CPSC 457: Sensitive Information in a Wired World

The Enforceability of Current Anti-Spam Legislation

Jeannie Wong

In July 2003, 50 percent of all electronic messsages sent through the Internet was unsolicited bulk email, according to Brightmail, a San Francisco spam-filtering company, and the Radicati Group has predicted that by the end of this year, 4.9 trillion pieces of spam will have been sent. Under pressure from angry Internet users, the United States, the United Kingdom, the European Union, Australia, Japan, and South Korea have or will enact legislation intended to control the onslaught of spam. In the United States, President Bush is expected to sign the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 into law by the end of this year and on October 31, 2003 European Union member countries began implementing a strict opt-in anti-spam law. South Korea has had anti-spam laws since 1999. Focusing on the enforceability of current anti-spam laws and at the risk of using a flawed analogy, I'd venture that anti-spam legislation will be about as effective as anti-prostitution legislation.

Cost of spam to consumers

Internet users tend to agree that junk email apart from being an annoyance, consumes valuable resources such as bandwidth and server processing time. Ferris Research estimates that in 2002, spam cost U.S. corporations $8.9 billion in lost worker productivity while the Federal Trade Commission believes that consumers spend an additional $10 billion to $87 billion per year on Internet fees because of spam. Spam takes up server disk space and its sheer volume drains bandwidth. Internet Service Providers then pass this cost along to customers. Spam-filtering products and services meanwhile make up a $65.2 million industry.[1]

Spam is hard to define

However, as evidenced by the high percentage of consumers who have made purchases after receiving commercial spam sent by established firms—anywhere from 5 to 7 percent for

[1] Spam by Numbers, 2003.

general email marketing campaigns, to 10 to 15 percent for targeted marketing campaigns[2] —the definition of junk email varies from individual to individual. Organizations such as the American Association of Advertising Agencies and the Direct Marketing Association therefore lobby actively to protect their members' rights to send bulk email advertisements. And this, critics charge, led to the dilution of the CAN-SPAM Act.

The CAN-SPAM Act of 2003

The CAN-SPAM Act has nevertheless been approved by Congress and has received the support of the NetChoice coalition, which includes eBay, Orbitz, and the Information Technology Association of America, the Direct Marketing Association, AOL, Yahoo, and other technology trade organizations. As with most anti-spam legislation the CAN-SPAM Act defines spam as unsolicited bulk commercial email.

Reintroduced by Senators Conrad R. Burns (Republican-Minnesota) and Ron Wyden (Democrat-Oregon) in April 2003, the CAN-SPAM Act restricts the definition of a commercial email to an email whose primary purpose is to advertise a commercial product or service. The bill increases the penalties that may be imposed on spammers who send deceptive electronic messages and effectively legalizes the sending of all truthful bulk email with opt-out mechanisms.

Under the CAN-SPAM Act, sending bulk commercial email using fraudulent transmission information—whether by illegally accessing another person's computer, by falsifying or intentionally excluding header information in emails, or by using fake email accounts or falsified domain name registrations—to hide the identity of the sender will be punishable by a fine and up to five years in prison depending on the severity of the offense.

[2] According to the Radicati Group, "Legitimate email advertisers typically see a 5 to 7 percent success rate in their email marketing campaigns, compared to 1 to 3 percent for traditional, offline direct-marketing methods." (Elkin, 2003)

Header information is defined as information that identifies the sender, destination, and routing of an email. The bill additionally prohibits false, misleading or nonexistent subject headings in all emails, both commercial and otherwise.

Anyone convicted of sending commercial email containing sexually oriented material that does not include a standard label, that still needs to be specified by a commission appointed by Congress, may be fined or jailed for up to 5 years. The CAN-SPAM Act will pre-empt more stringent state laws that prohibit spam outright, or require standard labels which facilitate spam filtering such as the "ADV: " label in the subject lines of unsolicited commercial email, although it will not override provisions that address falsity.

Opt-out mechanism

All commercial email must include an opt-out mechanism such as the sender's email address, and the sender's postal address. Consumer advocates however note that even if only one percent of America's 24.7 million small businesses send an electronic message to an email address per year, this will still add up to 658 unsolicited emails per day. Moreover, by responding to or even by just opening an email, Internet users could in effect be informing unscrupulous spammers that an address is valid, leading to more spam, not necessarily from the same address. The F.T.C. in fact advises consumers to completely ignore spam.

Do-not-spam list

Additionally, although the CAN-SPAM Act stipulates that the Federal Trade Commission must study the feasibility of setting up the do-not-spam registry proposed by Senator Charles Schumer (Democrat-New York) the F.T.C.'s chairman Timothy J. Muris has said that he does not think that the F.T.C. can enforce a do-not-spam list. Spammers are much harder to track down than telemarketers, sending spam consumes a much lower overhead, and

the marginal cost of sending out a million emails is not much higher than the marginal cost of sending out a hundred emails. Worse still, spammers who are already sending out illegal junk mail may very well use the do-not-spam registry to get working email addresses.

Enforcement of existing anti-fraud laws

In any event, the F.T.C. is already devoting significant resources to stemming the flow of the 70 percent of spam that is fraudulent. MessageLabs, a British spam-filtering company, estimates that the Nigerian advance fee scam, also known as 419 after the section in the Nigerian Criminal Code that pertains to it, will net $2 billion in 2003, ranking it as one of the nation's top five major sources of income while using bulk email to hawk pornography nets U.K. spammers approximately $3.2 billion worldwide annually[3]. Besides being used to peddle everything from fraudulent business opportunities to bogus weight-loss plans, spam is used to spread computer worms and viruses such as the SoBig worm and Mimail virus.

In 2002, the F.T.C. reported that it had trained 1,700 American and Canadian law enforcement agents to investigate fraudulent emails and other Internet-based scams, and the F.T.C. has played an active role in the creation of "netforces," which facilitate inter-agency cooperation at the local, state, federal, and international levels. In April 2002, the Northwest Netforce, which is made up of the F.T.C., eight U.S. state law enforcement agencies, and four Canadian organizations filed 63 criminal charges and issued more than 500 warning letters to online conmen.[4]

There is little indication however that law enforcement has significantly lowered Internet crime rates. At a cybercrime conference in Germany on December 3, David Finn, Microsoft's director of digital integrity for Europe, the Middle East, and Africa conceded that computer

[3] Spam by Numbers. 2003
[4] Putting a Lid on Deceptive Spam. 2003

viruses will cost the global economy about $13 billion this year. Companies worldwide spend about $3.8 billion a year protecting their networks against virus attacks but creators of computer viruses appear to be staying a step ahead of both the companies taking preventive measures and law enforcement agents.[5]

In the U.S., as part of a series of steps taken under the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act, the Secret Service is expanding their e-crimes task force to cities nationwide starting with Boston, Charlotte, Chicago, Los Angeles, Miami, San Francisco, Washington D.C., and Las Vegas. Modeled upon the Secret Service's New York Electronic Crimes Task Force, these task forces will foster close public and private sector cooperation in preventing and solving electronic crimes. The New York task force is made up of over 250 people, including officials from 50 federal, state, and local law enforcement agencies, 100 private corporations such as AT&T, Citibank, Intel, Microsoft, and Morgan Stanley Dean Witter, and 12 universities. Formed in 1995, it has to date arrested over 800 individuals who committed e-crimes that cost over $425 million, resolved about 2.1 thousand identity thefts, and trained more than 11 thousand law enforcers, prosecutors, and corporate executives in the recognition and prevention of e-crimes. [6] So law enforcement may yet win the war against cyber-criminals.

Suing spammers

Many spammers however are more annoying than they are dangerous and law enforcers may not deem them a sufficient enough threat to justify the time and effort required to find and build a case against them. Anti-spam activists consequently believe strongly that consumers should be given the right to sue, which is currently allowed in many U.S. states such as

[5] Virus Writers Winning the War, Says Microsoft. 2003
[6] http://www.ectaskforce.org

Connecticut, Colorado, Ohio, Rhode Island, Washington, and Virginia. It is easy enough to track down amateurs and anti-spammers often use websites like Suespammers.org, SamSpade.org, which searches the Whois database for domain name registrars, and Whew.com, which can be used to locate the physical address of a spammer, to identify spammers.[7]

Legislators and legitimate firms that rely on bulk email advertising however worry that laws that allow individuals to sue spammers will result in frivolous lawsuits and add to the backlog of cases in many courts. Once the CAN-SPAM Act is signed into law, the individual's right to sue currently guaranteed under several state anti-spam laws will be eliminated. Only state attorneys general and ISPs will be able to bring civil actions against law-breaking spammers. State attorneys general may sue to obtain compensation on behalf of state residents equal to their actual financial loss, or $250 per email received up to $2 million. This limit doesn't apply if false header (transmission) information was used. ISPs may sue a spammer who uses false transmission information to recover their actual financial loss or for up to $100 per email sent through the ISP. For violation of all the other rules, ISPs are allowed to sue to recover the actual loss or for up to $25 per email, with a cap of $1 million. In addition, ISPs may sue spammers who commit what the bill defines as aggravated violations: sending bulk commercial email to addresses that were obtained via automated harvesting and dictionary attacks, or from email accounts that were created automatically or by illegally accessing some other computer to reroute spam.

ISPs have in the past successfully sued spammers for trespass-to-chattel and under existing state anti-spam laws. A Radicati Group study, "Anti-Spam Market Trends, 2003-2007" states that by the end of 2003, the added toll on servers caused by spam will have cost companies

[7] Can Spam be Canned. 2000

worldwide an estimated $20.5 billion. This figure is projected to rise to $41.6 billion in 2004[8]. The Gartner Group found that in 1999, ISPs spent an annual median amount of $387 thousand to process and delete spam, which averaged out to $1 of each user's monthly fee[9].

In 1997, CompuServe won a settlement of $2 million from Sanford Wallace's company Cyber Promotions for trespass-to-chattel, arguing that the millions of junk mail sent to CompuServe accounts had illegally tied up CompuServe's servers[10]. In 2002 Earthlink, which spends over $1 million a year fighting spam, was awarded compensatory damages of $24.8 million in a lawsuit brought against Khan Smith who had fraudulently obtained personal information and credit card numbers from Earthlink users he had spammed by selling them non-existent credit reports and by using Trojan horse viruses that allowed him to steal information from users' computer[11]. More recently, the ISP won a $16 million lawsuit in May 2003 against Howard Carmack, the Buffalo Spammer who sent his bulk emails from Internet accounts opened using stolen personal information[12]. Unfortunately it is unclear whether these high-profile lawsuits have or will sufficiently deter spammers.

Sanford Wallace the self-styled Spam King remains unrepentant and has announced that he plans to create a backbone ISP network that spammers can use to send bulk email. Both Smith and Carmack were absent from their trials and neither had legal counsel. Carmack however is facing criminal charges brought against him by the New York State Attorney General, Eliot Spitzer, which may result in a maximum sentence of seven years in jail upon conviction.[13]

[8] Spam by Numbers. 2003
[9] Can Spam be Canned. 2000
[10] Spam King Retreats. 1998
[11] Earthlink Wins $25 Million in Spam Suit. 2002
[12] Earthlink Wins $16 Million Settlement in Spam Case. 2003
[13] Geeky Legal Beagles Nail Spammers. 2003

Moreover, it is estimated that some 80 to 90 percent of all spam originates from only 10 percent of all spammers, and these professionals are much harder to catch and convict. Carmack's own brother testified against him in the Earthlink lawsuit. Alan Ralsky, who some believe to be the world's premier spammer, on the other hand, simply settled his case for an undisclosed sum after losing a lawsuit brought against him by Verizon Internet Services in 2002 under Virginia state law, and then began routing his emails through bandwidth provided by foreign ISPs.[14]

Given how complicated it is to trace spammers and collect enough evidence to justify a lawsuit, the cost of litigation remains too high for many ISPs, regardless of the potential payoffs. Smaller ISPs find that it is still cheaper to ban spammers than to take them to court.[15]

CAN-SPAM's proof of knowledge requirements

When prosecuting or suing spammers, CAN-SPAM will require that state attorneys general and ISPs prove that spammers or their affiliates willfully and knowingly continued sending emails to a recipient ten days after the person had opted-out. In addition, businesses can only be held liable for damages if it can be shown that they were aware that spam sent on their behalf was illegal. This will impose an additional burden on lawyers and law enforcement officials.

California's S.B. 186

Among the stricter state laws that CAN-SPAM will pre-empt is California's S.B. 186 that was due to take effect on January 1, 2004. S.B. 186 is an opt-in law would have banned the mailing of all unsolicited commercial spam and would have held both the spammer and the entity whose product is being advertised liable for damages. The law recognizes that "the true

[14] Spam King Lives Large Off Others' Email Troubles. 2002
[15] Can Spam be Canned. 2000.

beneficiaries of spam are the advertisers who benefit from the marketing derived from the advertisements." And since in most cases it is easier to track down the advertiser, this would have resulted in easier enforcement of the law. It would also have allowed all recipients of spam, ISPs, and state attorneys general to sue spammers.

CAN-SPAM at least sets a nationwide standard

Weak as the CAN-SPAM Act is, it does represent significant legislative progress in the fight against spam. A federal law will facilitate prosecution of spammers particularly those who sent email to or from states without anti-spam legislation. It will also prevent spammers who live outside the state that they're being sued in from arguing that state anti-spam laws limit interstate commerce in violation of the Constitution's Commerce Clause that gives only Congress the power to regulate interstate commerce. On March 10, 2000, a Washington state court ruled that in prohibiting spammers from sending emails with deceptive subject headers to Washington state residents and thereby requiring spammers to verify each recipient's state of residency, Washington's "unduly restrictive and burdensome" anti-spam law violated the Commerce Clause. On June 7, 2000, the San Francisco Superior Court ruled that in mandating that all unsolicited commercial email contain the prefix "ADV:" in the subject line and include an opt-out mechanism, California law violated the Constitution because as a result Internet users were forced to follow different rules when sending mail to different states[16]. Apart from observing the Constitution's Commerce Clause, lawmakers also have to ensure that any federal or state anti-spam law does not unfairly discriminate against small businesses or infringe upon freedom of speech rights.

[16] Courts Declare Two State Anti-Spam Laws Unconstitutional. 2000.

South Korean anti-spam legislation

The South Korean government has had some success in limiting the amount of unsolicited commercial spam in Korean inboxes since amending South Korean anti-spam legislation to include criminal penalties and increasing the maximum fine to $835 thousand in December 2002. South Korean law prohibits the automated generation and harvesting of email addresses, requires standard labels on all commercial email and mandates that South Korean marketers provide a toll free number that consumers can call to opt-out of all future mailings. With no free-speech protection laws comparable to the American First Amendment, South Korea has faced little difficulty in passing anti-spam legislation since 1999[17]. Even so, the anti-spam task force at the Korea Information Security Agency (KISA) found that in July 2003, Koreans were still receiving an average of 41 pieces of commercial spam per day and that pornographic spam has only just recently begun to decline. In addition, KISA found that although the percentage of commercial email that was unsolicited dropped from 90 percent in March 2003 to about 70 percent in July 2003, the total sum for all commercial email increased[18].

European Union anti-spam legislation

In the E.U., under Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, also known as the Directive on Privacy and Electronic Communications, member states were required to enact national legislation by October 31, 2003 that either bans unsolicited direct marketing emails sent without the consent of the recipient or prohibits marketers from emailing Internet users who have stated explicitly that they do not want to receive unsolicited commercial email. E.U. nations that have chosen to implement the second option will in effect be setting up and enforcing a do-not-spam list.

[17] No Slap on the Wrist for Spam in South Korea. 2003
[18] Spam Falls after South Korea Strengthens Email Law. 2003

At the moment, it is unclear how countries with anti-spam laws will be able to enforce their laws with regards to spammers who send their emails from abroad. As reported by messagecare, the Australian company that sells SpamTrap, most spam currently originates from the United States (33 percent), China (18 percent), Korea (9 percent), Brazil (4 percent), Canada (3 percent), the United Kingdom, Italy, Mexico, and Germany (2 percent each), and Taiwan (1 percent). These proportions however are bound to shift over time as spammers move their base of operations to countries with non-existent or weak anti-spam laws.

Odds are in spammers' favor

With current Internet infrastructure the way it is, spammers are at a distinct advantage. ISPs and anti-spam activists have created blacklists, which individuals and ISPs can refer to, to block all mail coming from ISPs that have allowed spammers to use their networks. Spammers therefore send millions of emails from one address, and then shut the address down quickly before it is blacklisted. ISPs in places like Finland and Hong Kong let users sign up from anywhere, often with little proof of identity. Spammers also steal email addresses by hacking into individual accounts and ISP databases, among other techniques. The British anti-virus company, Sophos estimates that one third of all spam is sent from computers that have been infected by Trojan horse viruses. Trojan horses exploit software vulnerabilities in operating systems, usually Windows, and allow hackers to install Remote Access Tools (RATs) in the compromised computers[19].

Spam is an outgrowth of the basic structure of the Internet, which aims for quick and cheap dissemination of information and there will be spam as long as there is an economic incentive to send spam. Law enforcers, privacy advocates, and anti-spam activists generally agree that spammers can only be stopped through a combination of legislative enforcement,

[19] Sobig-F Wins 2003 War of the Worms. 2003

technology tools and consumer awareness. And even if laws that ban unsolicited commercial emails were completely effective, Internet users would still be fair game for religious, non-profit, political, and other types of non-commercial spam that governments in nations where freedom of speech is protected will find difficult to ban outright.

Legislation can be used to further empower law enforcement officials to hunt down spammers who do serious harm. But it should also be the responsibility of each Internet user to protect himself or herself from the worse excesses of spam such as fraud and computer viruses by exercising good judgment and enlisting the help of decent spam filters.

References

- Bureau of Consumer Protection, Federal Trade Commission. 2002. Putting a Lid on Deceptive Spam. *ftc consumer feature*, July 2002. *http://www.ftc.gov/bcp/conline/features/spam.htm.*
- California Business and Professions Code: Division 7, Part 3, Chapter 1. Article 1.8. Restrictions on Unsolicited Commercial Email Advertisers (added by S.B. 186 (2003), approved September 23, 2003)
- Cave, Damien. 2000. Can Spam be Canned? *www.salon.com*, April 19, 2000. *http://www.salon.com/tech/feature/2000/04/19/spam_legislation*
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. November 25, 2003.
- Delio, Michelle. 2003. Geeky Legal Beagles Nail Spammers. *Wired News*, May 26, 2003. *http://www.wired.com/news/politics/0,1283,58939,00.html*
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal of the European Communities. 31.7.2002. L 201/37-47.
- Electronic Crimes Task Force About Us *http://www.ectaskforce.org/About_Us.htm*
- Electronic Crimes Task Force Regional Locations *http://www.ectaskforce.org/Regional_Locations.htm*
- Elkin, Tobi. 2003. Spam: Annoying but effective. *Advertising Age*, September 22, 2003. Vol. 74. Issue 38, p41.

- ePrivacy Group. 2003. Spam by Numbers: June 2003. *http://www.eprivacygroup.com/pdfs/SpamByTheNumbers.pdf*.
- Kornblum, Janet. 1998. Spam King Retreats. *CNET News.com*, March 12, 1998. *https://news.com.com/2100-1023-209035.html*
- Lemke, Tim. 2003. No Slap on the Wrist for Spam in South Korea. *The Washington Times*, September 2, 2003. *http://www.washtimes.com/business/20030901-102352-8411r.htm*
- Morgan, Jeffrey and Hurewitz, Barry. 2000. Courts Declare Two State Anti-Spam Laws Unconstitutional. *Hale and Dorr LLP*, November 29, 2000.
- Roberts, Paul. 2003. Earthlink Wins $16 Million Settlement in Spam Case. *IDG News Service*, May 8, 2003.
- Saunders, Christopher. 2002. Earthlink Wins $25 Million in Spam Suit. *InternetNews.com*, 2002. *http://www.internetnews.com/IAR/article.php/1430591*
- Sophos. Sobig-F Wins 2003 War of the Worms. 4 December 2003 *http://www.sophos.com/pressoffice/pressrel/au/20031204yeartopten.html*
- Trevelyan, Mark. 2003. Web Virus Authors 'Winning Battle'—Microsoft. *Reuters*, December 3, 2003. *http://www.washingtonpost.com/ac2/wp-dyn/A31818-2003Dec3*
- Wendland, Mike. 2002. Spam King Lives Large Off Others' Email Troubles: West Bloomfield computer empire helped by foreign Internet servers. *Free Press*, November 22, 2002. *http://www.freep.com/money/tech/mwend22_20021122.htm*
- Williams, Martyn. 2003. Spam Falls After South Korea Strengthens Email Law. IDG News Service, September 15, 2003.

http://www.idg.com.sg/idgwww.nsf/0/D0130F55C8E59E1A48256DA300271F3C?OpenDocument