Can Spam Be Legislated?

Karen L. Hamilton
Columbus State University

Robert A. Fleck, Jr.
Columbus State University

Spam, the unsolicited email that shows up in on-line mailboxes—both business and personal—costs business and individuals. Software and other spam-fighting measures are available that prevent spam from reaching email boxes. Various forms of legislation have also been proposed or enacted to address the problems with spam. This study examines current anti-spam laws at the state and federal levels in the United States and those laws enacted or being considered in other countries. The study also assesses the feasibility of each type of legislation in achieving the stated goals. The conclusions provide insights into the legislation that has the most merit in controlling the issues raised by spam.

INTRODUCTION

Spam, the unsolicited email that shows up in on-line mailboxes—both business and personal—costs business and individuals. Businesses lose employee productivity with time spent to delete spam, incur additional IT costs to fight it and face additional expenses to manage spam's effects, such as purchasing more bandwidth. Individuals spend time and money on their home systems to fight spam and to clean their mailboxes. Current estimates place the percent of emails that are spam at 50 to 80 percent of all emails. ("US Anti-Spam Law," 2004; Ward, 2004; The White House, 2003)

While many businesses and individuals around the world are fed up with spam, others support spam. Supporters claim that it is a legitimate business practice and is an extension of free speech with constitutional guarantees. Further, banning spam would put an end to otherwise successful businesses and hurt domestic employment.

Given the turmoil surrounding the issue of spam, federal and state governments in the United States (US) and national governments in other countries have enacted or have proposed legislation to address spam. These laws are generally grouped into two categories: 1) those allowing the recipients of unsolicited emails to choose to be removed from emailing lists, commonly referred to as opt-out laws, and 2) those that require potential recipients to choose to receive emails from commercial entities before they are sent, generally called opt-in laws.

The question remains, however, whether such legislation can successfully address the problems associated with spam. That is the question this study addresses. This study examines each of the current types of anti-spam laws. It also assesses the feasibility of each type of legislation in achieving the stated goals. The conclusions provide insights into the legislation that has the most merit in the controlling of the issues raised by spam.

ANTI-SPAM LEGISLATION

Many states and several national governments in addition to the US have enacted or are considering enacting laws to help control spam. These laws can be categorized as either opt-out laws or opt-in laws. Each of these laws place requirements on the senders of emails. The typical requirements of each are discussed below.

Opt-Out Laws

Most current legislation falls into the opt-out law category. Most of these laws apply to unsolicited commercial emails (UCE). The laws typically define UCE to mean emails 1) sent for the purpose of soliciting sales or promoting products and services, 2) to recipients whom are not current customers or clients and 3) to recipients whom have not asked to receive the emails. For example, Arizona's definition of UCE is as follows:

> "Unsolicited commercial electronic mail" means a commercial electronic mail message sent, without the consent of the recipient, by a person with whom the recipient does not have an established business relationship.
>
> Where,
>
> "Commercial electronic mail" means electronic mail sent for the purpose of encouraging the purchase or rental of, or investment in, property, goods or services. ("Subtitle 30," 2002, paragraph 14-3003)

Opt-out laws generally allow UCE to be sent to anyone with an email address unless recipients have notified the particular sender that they want to be removed from the emailing list. The typical requirements placed on the senders of these emails are:

- Provide valid sender contact information including at least the sender's name and email address. A street address and domain name may also be required.
- Provide instructions for opting-out. These may require only responding to the email with a certain subject line, such as "REMOVE" or may require that recipients also be allowed to call a toll-free number to be removed from the list. When opt-out requests are received, they generally must be honored.
- Use valid routing information and subject lines. The senders are not allowed to falsify the routing information in the email headers. They also must not use false or misleading subject lines. Furthermore, permission from third parties must be obtained before unsolicited emails can use their domain name in the email header.
- Use a label in the subject line. If an unsolicited email contains sexually explicit content, it generally is required to have "ADV: ADULT" or similar notation at the beginning of the subject line. For all other unsolicited commercial emails, "ADV:" or similar notation is often required.

Penalties for violating these requirements vary. But, they generally allow civil lawsuits seeking damages. For example, the Maryland law allows lawsuits by the recipient, a third party whose name or domain was fraudulently used in the email and the ISP whose network was used

to send the UCE. The recipient and the third party can sue for actual damages or $500, whichever is greater. The ISP can sue for the greater of $1,000 or actual damages. (“Article 16,” 2003)

Opt-In Laws

Opt-in laws require that potential recipients choose to receive emails before they are sent any. No unsolicited commercial emails are allowed. These laws typically define commercial email as that sent to solicit sales or advertise products and services. For example the definition of commercial email that appears in the California law is as follows: ‘”Commercial e-mail advertisement" means any electronic mail message initiated for the purpose of advertising or promoting the lease, sale, rental, gift offer, or other disposition of any property, goods, services, or extension of credit.’ (“Article 1.8,” 2003, paragraph 14529.1)

The laws typically require that the consent to receive commercial emails be direct and informed. The potential recipient must recognize that he or she is giving consent and must be informed about what the results of the consent will be. However, the method of consent is typically not specified. Therefore, clicking a check box on a website or filling out a form received in the mail or on a website would both be appropriate means of consenting under most opt-in laws. The California law contains the following provision: ‘"Direct consent" means that the recipient has expressly consented to receive e-mail advertisements from the advertiser, either in response to a clear and conspicuous request for the consent or at the recipient's own initiative.’ (“Article 1.8,” 2003, paragraph 17529.1)

The Privacy Directive in the United Kingdom’s (UK) states that “consent may be given by any appropriate method enabling a freely specific and informed indication of the user’s wishes, including by ticking a box when visiting an internet website.” (Stokes and Bramwell, 2004)

Opt-in laws apply various penalties to violators. The offenders must stop sending commercial emails in violation of the law. In addition, civil lawsuits may be allowed against the offenders to recover damages and court costs. Under the California law, the damages be as high as $1,000 per unsolicited email, with a maximum of $1,000,000 per incident. (“Article 1.8,” 2003) The UK Privacy Directive makes failure to comply with the request to stop sending prohibited emails a criminal offense. (Stokes and Bramwell, 2004)

CURRENT LEGISLATION

Many states and the federal government in the US have enacted anti-spam legislation. Most of these laws are opt-out laws. Other countries have also enacted or proposed anti-spam legislation. In the European Union (EU) countries, under the guidance of an EU directive, countries have enacted or proposed opt-in and opt-out laws. Additionally, countries outside the EU, other than the US, have adopted or proposed legislation that address unsolicited emails. A review of the current legislation that has been enacted by states, the US federal government and other countries is provided in the following sections.

State Legislation

Thirty-seven states have enacted anti-spam legislation between 1998 and 2003. Two additional states have limited anti-spam provisions in other legislation that apply specifically to emails sent by attorneys for advertising purposes. The majority of state anti-spam laws are opt-out laws. Only 5 percent of states with any limits on commercial emails have opt-in laws.

Most of the laws apply to some form of UCE—either all UCE or that containing sexually explicit material. Some laws apply to all bulk commercial emails while others apply to all commercial or bulk emails. The definition of bulk varies—for example in Kansas, bulk means emails sent to 500 or more addresses while in Louisiana, bulk means sent to 1000 or more addresses.

The laws generally limit their enforcement to in-state entities. In some states, that could be either the sender, the receiver or the ISP or network used to send or deliver the UCE. In others both the receiver and the ISP need to be in-state for the law to apply. The most common requirement, for those states with specific provisions, is that the sender or receiver be in-state followed closely by just the receiver being in the state. (Sorkin, 2003b)

The state laws share certain provisions. Most states specify that the routing information must be valid. Many states also require that the subject line not be misleading and prohibit the sale of software that can create false routing information. Some states specify that fraudulent routing is a violation of the law only if the ISP policy is violated. Lastly, several states' laws indicate that personal jurisdiction will be established in cases where a non-resident of the state uses a computer within the state to send the offending email. For example, Oregon's law states that an ISP may bring suit against a sender in the circuit court in the county in which "that person … has sufficient contacts for the court to exercise personal jurisdiction over the person." ("SB 910," 2003)

State opt-out laws also have common provisions. The majority of states require that the contact information about the sender—such as the reply email address and sender's name—be valid. The same number of states require that opt-out instructions be included in the UCE. Most states also require that all UCE have a subject line that indicates it is commercial in nature. For non-sexually explicit UCE, the subject line often is required to start with "ADV:" or a similar indication. For sexually-explicit UCE, the required start to the subject line is usually "ADV:ADULT" or a similar phrase. Only about 1/3 of the states with opt-out laws specify that the opt-out requests must be honored. Several states require only sexually-explicit UCE have subject lines that indicate their contents are advertisements of a sexually-explicit nature. When this provision is included, it requires a subject line similar to that referred to above, "ADV:ADULT."

The state laws contain similar provisions concerning the penalties for violations of their anti-spam acts. Violators will be required to stop sending the inappropriate emails and follow the guidelines established by the laws. The violators can also be sued in civil court by recipients and ISPs. Actual or liquidated damages can be sought, with the maximum set at usually $500 to $1,000 or actual damages per email. Daily dollar limits, such as $25,000, are also generally included. (Sorkin, 2003b)

The United States Can-Spam Act

The "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (Can-Spam Act) was signed into law in the US by President Bush in December 2003. The act is an opt-out law that became effective January 1, 2004. Under this act, commercial emails sent to promote or advertise an organization's products or services must satisfy the following requirements:

- Indicate that they are advertisements or solicitations, or that they include sexually explicit content
- Provide a valid and clear means for opting out of receiving additional similar emails

- Include a valid email address (for at least 30 days) and physical postal address for contacting the sender
- Use accurate header information, including truthful and non-misleading routing information and subject lines

Fraud is deemed to be a criminal action and is punishable by fines and imprisonment. It also may result in forfeiture of equipment and other property used to commit the fraud. Failing to comply with the requirements listed for unsolicited commercial emails can result in civil litigation with damages up to $250 per violation (i.e., separately addressed email) to a maximum of $2 million. Courts are given discretionary powers to increase these fines within certain guidelines.

The act is to primarily be enforced by the Federal Trade Commission. Other federal and state agencies may be given enforcement powers as well. States, individuals and private parties may not sue violators. However, ISPs have limited rights to bring civil action. The White House, 2003; Hoffman, 2003)

Legislation in European Union Countries

The EU adopted an anti-spam directive in 2002. The Privacy and Communications Directive includes provisions for an opt-in system for addressing UCE in member countries. Member countries were supposed to have implemented their own opt-in anti-spam legislation by October 31, 2003. Several member countries have already enacted anti-spam legislation, including Austria, Belgium, Denmark, Finland, Greece, France, Italy, Norway, Portugal, Spain, Sweden and the United Kingdom (UK). (Stokes and Bramwell, 2004) However, not all of the member countries chose to use the opt-in system in the EU directive. Belgium and Portugal enacted opt-out systems that apply to emails sent to individuals and organizations. Finland enacted an opt-in system for individuals and an opt-out system for organizations. Furthermore, Luxemburg issued an opinion on the EU directive that supports an opt-out system, although the country has not yet enacted its own legislation. Several other EU countries have not yet enacted legislation as required by the EU directives.(Sorkin, 2003a; EuroCAUCE, n.d. a-n)

The laws in the EU countries that have enacted opt-in anti-spam legislation are generally similar to that espoused in the EU directive. For example, the UK's Privacy & Electronic Communications (EC Directive) Regulations 2003 became effective in December 2003. It has an opt-in provision that applies to direct marketing via emails. No direct marketing emails can be sent without prior consent of the intended recipients. However, prior consent is deemed to be given when the recipient's contact information was made available during the sale or negotiations for sale of products or services, similar products and services are being offered in the email and an opt-out provision is provided in the email. The UK's law also does not allow use of fraudulent or misleading identification information and requires the valid email addresses be provided for recipients to choose not to receive additional emails. The UK's regulations are enforced by the Information Commissioner (ICO) and apply only to UK emails. Violations of the regulations may result in civil liability. (Stokes and Bramwell, 2004)

Some countries have enacted their own forms of opt-in anti-spam legislation. For example, Italy has three laws that address spam, all of which were enacted prior to the EU directive. Under DL 171/1998 all advertising expenses are to be borne by the company conducting the advertising, which essentially bans mass emails that create processing costs for the recipients. Under DL 185/1999, a company must have prior approval to solicit sales outside of a commercial building. Therefore, UCE for advertising purposes is illegal. Italy's laws makes

sending unsolicited emails for the purposes of profit a criminal offense, punishable be fines and possible jail time. In addition, the burden is placed on the sender to justify its actions. Anyone who receives a UCE can request such an explanation, and if the explanation is not satisfactory, can request that the governmental agency regulating UCE investigate. (EuroCAUCE n.d.i)

Legislation in Other Countries

Argentina, Australia and Canada have enacted legislation that addresses UCE. Japan has proposed anti-spam legislation. The laws in Australia and Canada are opt-in laws while the legislation in Argentina and Japan includes opt-out provisions. In addition, Brazilian Internet and direct advertising companies have banded together to self-regulate spam.

Australia's Spam Act of 2003 and Canada's Personal Information Protection and Electronic Documents Act are notably different, with Canada's law being similar to the legislation passed by EU countries. Australia makes it illegal to even send one UCE to any individual or organization or from any individual or organization in Australia. The penalties for violating the law in Australia are set at a maximum of $1.1 million per day for organizations and $220,000 per day for individuals. (CAUCE, n.d.) Canada requires that bulk commercial emailers ensure that people and organizations on the list of email addresses have consented to receiving commercial bulk emails. ("Personal Information," 2005)

The opt-out laws in Argentina and Japan contain provisions similar to the opt-out laws discussed above. Argentina's 2000 Argentine Data Protection Law prohibits sending UCE that does not contain opt-out instructions. It also requires that opt-out requests be honored. Violators are subject to civil lawsuits. Japan's legislation requires that UCE contain a subject line that indicates it is an advertisement. It also requires that opt-out requests be honored. Additionally, the Japanese law allows telecommunication carriers to refuse email from spammers when the quantity of email can cause problems for the network systems. (Palazzi, 2003; Miyake, 2001)

The guiding principle of Brazil's Self-Regulation Anti-Spam Campaign is that industry can address the spam issue on its own. The campaign proposes a code of ethics for advertisers using UCE. The code provisions require emailers to tell customers the truth about the company sending the email and about the products and services being advertised. The code also contains opt-out provisions for recipients and encourages senders to honor such requests. (Bolin, 2005)

EFFECTIVENESS OF CURRENT LEGISLATION

The current spam legislation does not seem to be having much affect on the amount and cost of spam. Following the enactment of the US Can Spam Act, various observations were made. One study indicated that the amount of email that was spam was reduced by 1 percent—from 80 percent to 79 percent. Another study noted that a February 2004 survey of home and work email users found that the majority of respondents (53 percent) had observed no change in the volume of spam they received. In that spam survey, only 11 percent of work email users indicated a reduction in the amount of email while 19 percent indicated an increase in the amount of spam. (Seda, 2004; "U.S. Anti-Spam Law," 2004)

State laws were superseded by the federal law for emails crossing state lines. Before the federal law was enacted, several state laws were found to be unconstitutional because they attempted to regulate interstate commerce by applying to emails sent from other states or through ISPs based in other states. (McCullagh, 2004)

The EU legislation has had similar results. Those countries with legislation in place apply their laws' requirements only to email in their countries. If different countries have different laws, the end result is that spammers will locate the country with the most lenient or nonexistent regulation from which to operate. And, outside the EU, Australia's law is most aggressive but it has not yet been tested. Australia will run into the same issues: how to enforce its provisions across territorial boundaries.

Critics of legislation applying to unsolicited emails point out just this: when federal laws are different (opt-in versus opt-out), they will not help to control the growth of spam. Just as the states ran into territorial issues when trying to prosecute out-of-state spammers, nations will be unable to prosecute or even locate senders from other countries. Because much spam comes from other countries, such legislation cannot do much about spam. (Stokes and Bramwell, 2004)

DISCUSSION

Opt-in laws, if enacted and enforced on a global level, might help control the volume of spam. Requiring prior permission before emails can be sent to recipients automatically reduces the amount of unsolicited emails. It thereby reduces the volume and the costs of spam.

Opt-out laws will not reduce initial unsolicited emails. Furthermore, they still require recipients to respond—using time and incurring technology costs to transmit their responses. As the number of business using UCE increases, the amount of email that arrives in a email box will also increase.

While opt-in laws appear to better address the costs involved with spam for businesses and individuals, both types of laws are affected by the jurisdictional issues involved in enforcing legislative provisions. States in the US cannot enforce their provisions on emails sent from other states because of the US Constitutional prohibition of states regulating interstate commerce. Federal governments in different countries are likely to have the same difficulty regulating emails sent from other countries. In addition, senders can hide their locations—whether they are sending spam from inside countries with anti-spam legislation or not. Even if false routing information is illegal, it will be difficult to find senders using it.

Enforcement of the laws may result in higher costs for businesses and individuals, at least initially. The remedies provided by the current legislation involve civil lawsuits. Thus, to recoup damages, businesses and individuals must incur the costs of filing the lawsuit, gathering the supporting information and spending time in court or in legal proceedings. This involves attorneys' fees, lost time from work, lost productivity and court costs; the sum of these costs may exceed the costs associated with simply deleting the unwanted email and paying for the additional transmission costs.

Based on the current legislative and global Internet environment, even opt-in laws in only some states and countries are not going to prevent spam from being sent. To fully eliminate spam through legislation will take a joint effort and the same or very similar legislation in all countries. Given the experience in the US and in the EU, it is unlikely that all countries will enact similar anti-spam laws. Therefore, the legislative solution is likely not the best answer to preventing spam and reducing its costs for businesses and individuals.

RECOMMENDATIONS AND CONCLUSIONS

Legislation does not appear to be the most effective answer. However, alternative solutions already exist. Spam-fighting software is available and prevents a large amount of spam from reaching employee and individual email boxes. In a related study, the authors found that because of the spam software filters, governmental agencies do not find spam to be a major concern. The costs of the anti-spam software are a business expense and businesses are finding ways to make it work most effectively for their organizations (for example, having employees help identify which emails are spam and which are not). The software is so effective, the costs of spam related to employee time and productivity have become minimal. (Fleck and Hamilton, 2004)

The Brazilian answer—the Self-Regulation Anti-Spam Campaign—provides additional opportunities to prevent spam from occurring in the first place. By having industry take the initiative to be truthful in advertising and better listen to the requests of customers, UCE will not be sent as often. This will result in lower transmission and email box management costs.

The software and industry-driven initiatives are likely to have more effect on reducing the costs of spam for businesses and individuals than the laws currently in place. However, further study of spam-fighting measures—both the legislative and industry-based—is needed. Spam may not be as much of an issue as it once was because software solutions continue to be improved. However, as these techniques become more effective and spam is increasingly kept from entering the email boxes of its intended recipients, senders are likely to seek alternative routes for getting their commercial messages out. Measures to fight the new routes will have to be developed and can be based on those that are most effective in fighting spam today.

ENDNOTES

Article 1.8, Restrictions On Unsolicited Commercial E-mail Advertisers. (2003). California Business And Professions Code Division 7, Part 3, Chapter 1, paragraph 17529.1.

Article 16, Commercial Electronic Mail. (2003). Arizona Revised Statutes Title 44 Trade And Commerce Chapter 9. Trade Practices Generally, paragraph 44-1372.

Bolin, R. (2005, March 4). Spam Laws Worldwide: Brazil. Lawmeme. Retrieved March 10, 2005, from http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1366.

CAUCE. (n.d.). Spam Act of 2003. Retrieved February 7, 2005, from http://www.cauce.org.au.

EuroCAUCE. (n.d. a). Austria. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_at.html.

EuroCAUCE. (n.d. b). Belgium. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_be.html.

EuroCAUCE. (n.d. c). Denmark. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_dk.html.

EuroCAUCE. (n.d. d). Finland. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_fi.html.

EuroCAUCE. (n.d. e). France. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_fr.html.

EuroCAUCE. (n.d. f). Germany. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_dt.html.

EuroCAUCE. (n.d. g). Greece. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_gr.html.

EuroCAUCE. (n.d. h). Ireland. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_ie.html.

EuroCAUCE. (n.d. i). Italy. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_it.html.

EuroCAUCE. (n.d. j). Luxemburg. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_lu.html.

EuroCAUCE. (n.d. k). Netherlands. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_nl.html.

EuroCAUCE. (n.d. l). Portugal. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_pt.html.

EuroCAUCE. (n.d. m). Spain. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_es.html.

EuroCAUCE. (n.d. n). Sweden. Retrieved February 7, 2005, from http://www.euro.cauce.org/en/countries/c_se.html.

Fleck, R. A. and Hamilton, K. L. (2004). Managing the Total Cost of Spam. Proceedings of the Academy of Information and Management Sciences, pp. 11-16.

Hoffman, I. (2003) The Federal Can Spam Law. Retrieved February 7, 2005, from http://www.ivanhoffman.com/federalspam.html.

McCullagh, D. (2004, December 15). Antispam Law Ruled Unconstitutional. News.com. Retrieved February 7, 2005, from http://www. news.com.com/2102-1030_3-5491683.html.

Miyake, K. (2001, November 9). Spam-Blocking Law Proposed In Japan. ITWorld.com. Retrieved February 7, 2005, from http://www.ITWorld.com.

Palazzi, P. (2003, November 19). Data Protection Law and Spam: First Case in Argentina. Message posted to http://dataprotection.blogspot.com/2003_11_01_dataprotection_archive.html. Retrieved February 7, 2005.

Personal Information Protection and Electronic Documents Act (2005) Retrieved February 7, 2005, from http://e-com.icga.ca/epic/internet/inecic-ceac.nsf/en/h-gv00246e.html#existing.

SB 910. (2003). 72nd Oregon Legislative Assembly, 2003 Regular Session, ORS 646.607 Section 6 5 (b). Retrieved March 4, 2005, from http://www.spamlaws.com/state/or.html.

Seda, C. (2004, July). Spam Uncanned. Entrepreneur, p. 72;

Sorkin, D. E. (2003a). Laws from Other Countries: European Union. Spam Laws. Retrieved February 7, 2005, from http://www.spamlaws.com/othercountries/europeanunion.

Sorkin, D. E. (2003b). State Laws Summary. Spam Laws. Retrieved February 7, 2005, from http://www.spamlwas.com/state/summary.html.

Stokes, S. and Bramwell, A. (2004, February). The Push To Can Spam. Managing Intellectual Property, Issue 136. Retrieved January 27, 2005, from Academic Search Premier Database.

Subtitle 30, Commercial Electronic Mail. (2002). Maryland Commercial Law Code Title 14. Miscellaneous Consumer Protection Provisions, Paragraph 14-3003.

The White House. (2003, December 16). Fact Sheet: President Bush Signs Anti-Spam Law. Retrieved February 7, 2005, from http://www.whitehouse.gov/news/releases/2003/12/print/20031216-4.html.

US Anti-Spam Law Fails To Bite. (2004, February 9). BBC News World Edition. Retrieved February 7, 2005, from http://news.bbc.co.uk/2/hi/technology/3465307.stm.

Ward, M. (2004, February 4). How To Make Spam Unstoppable. BBC News World Edition. Retrieved February 7, 2005, from http://news.bbc.co.uk/2/hi/technology/34458457.stm.