Over the last several weeks, I’ve been looking at spam and some of the ways companies are fighting back in courts of law. In this, my final article on the topic for a while, I’ll review some of the antispam laws already on the books and some of the laws being considered to fight the problem.

Before we get into real laws, a word of warning about a widespread fraud: “S. one thousand six hundred eighteen.” Many spammers put a note at the bottom of their junk messages claiming that they are complying with such a US law and that it makes their spam legal. Rubbish: the Senate of the US did indeed pass S. 1-6-1-8 (without the hyphens) in 1998, but it never became law because it was not ratified by the House of Representatives [1]. Ironically, any reference to this number in an e-mail message may activate antispam filters, which is why I’m going to such lengths to avoid putting it in its usual form. I hope its inclusion in the URL won’t trigger readers’ blocking software.

The most comprehensive list of antispam laws I have found is provided by emaildaddy.com [2]. It provides links not only for US federal and state laws and proposed bills but also for 15 European countries plus the European Union, Australia, Brazil, Canada, Czech Republic, India and Russia. The Federal laws show none enacted, 10 bills from the 106th Congress (1999-2000) and five from the 107th Congress (2001-2002). Twenty-four state laws are summarized and linked in the list.

The 108th Congress currently in session has a number of bills pending [3]. The CAN-SPAM Act (S. 877) is widely touted as a major advance, but according to the “spamlaws.com” site, “It would pre-empt any state laws that prohibit unsolicited commercial e-mail outright, but would not affect the majority of state spam laws.” The Anti-Spam Act of 2003 is apparently even weaker, since it would preempt most state laws. The REDUCE Spam Act of 2003 (HR 1933) is even worse, with a definition of spam that limits its applicability to people sending out more than 1,000 junk messages in any two-day period. The Stop Pornography and Abuse Marketing Act (S. 1231) sponsored by Sen. Charles Schumer (D-NY) would establish a no-spam registry administered by the FTC (much to that agency’s horror) [4]. The registry would work for people who choose to use it, but it could equally well be used to harvest all the e-mail addresses for use by criminal spammers. To fight this kind of abuse, Schumer’s bill also calls for strict penalties including imprisonment for repeat offenders.

Most of these laws and bills are relatively weak. They generally require identification of the spam – many by having “ADV:” in the subject line – and demand that the junk include accurate postal addresses and working unsubscribe links or instructions. They thus use the opt-out concept to regulate spam, ignoring the possibility that even a single junk message per business may flood e-mail recipients with millions of messages over years of annoyance. Worse, they don’t take into account the possibility that the creeps who send junk e-mail can simply sell the
confirmed e-mail addresses received through the opt-out process to new spammers who are thus not bound by the specific opt-out demand. Finally, none of these bills seems to take into account the strong likelihood that overseas spammers will pick up where domestic spammers leave off. Recall that international regulations on extradition require “dual criminality;” equivalent severity of the crime in both the jurisdiction of residence and in that requesting extradition [5]. Since most countries have nothing equivalent to antispam laws, it’s unlikely that prosecutors from those places with such laws will successfully interfere with international spammers.

In addition to allowing government officials in the US to file charges under state and federal laws governing spam, these statutes also allow private citizens to launch class-action lawsuits. For example, a Utah law firm has filed a class action lawsuit against Sprint Corp. alleging violation of that state’s spam law because the company is accused of having used a fraudulent FROM address, failed to put the ADV: prefix in the subject line, failed to include the sender’s company name and street address in the message, and failed to include an opt-out method [6]. I hope that many other law firms will take advantage of local laws to sue prominent spammers.

In conclusion, this problem is global and will probably be with us for several more years until we collectively come up with solutions spanning the spectrum from artificial intelligence tools through IPv6 to authenticate all Internet packets through individual lawsuits by deep-pocket victims, class-action lawsuits on behalf of shallow-pocket victims.

My own favorite antispam fantasy solution? Dunking convicted spammers in large vats of melted SPAM® before asking them if they’d like to opt out. And then doing it again. And again. And again. And . . .

* * *

References


* * *

MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.
Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.