I just read a new White Paper from Montreal-based Vircom, developer of Modus secure messaging solutions, on recent international anti-spam legislation efforts. Entitled, “Can Laws Block Spam?” the paper uses interviews with five experts on spam:

* Lindsay Barton, Manager, Online Policy at the National Office for the Information Economy of Australia;
* Anne P. Mitchell, Esq., President/CEO, Institute for SPAM and Internet Public Policy and Professor of Law, Lincoln Law School of San Jose, California;
* Michael D. Osterman. President and Founder, Osterman Research
* Troy Rollo, Chairman of the Coalition Against Unsolicited Bulk Email in Australia and Executive Director of the International Coalition Against Unsolicited Commercial Email
* Neil Schwartzman, Editor & Publisher spamNEWS, Chair, Canadian Coalition Against Unsolicited Commercial Email

The paper analyzes the CAN-SPAM act in reasonable detail, but this column has already pointed readers to that legislation and analyses of its weaknesses. More interesting here is the analysis of the European Community Directive on Privacy and Electronic Communication Regulation 2003. This legislation provides for opt-in (not opt-out) restrictions on sending junk e-mail. Much as with fax messaging, no one may initiate e-mail marketing without prior permission or prior business relationship – and there must be an easy way to refuse future junk e-mail at the time of initial data collection about an individual. In addition to enforcement actions initiated by the Information Commissioner in law courts, victims of spam may also sue for damages of up to £5,000 in cases heard before a judge (unlimited if heard before a jury). However, critics point out that the law does not regulate business-to-business spam, including spam sent to employees via their business e-mail addresses.

Another section covers the Australian Spam Act of 2003, which includes not only e-mail spam but also SMS (Simple Message System) junk messages. This law also uses an opt-in strategy, in contrast with the US approaches that depend on opt-out methods. There are also clauses dealing with proper (accurate) origination addresses and restrictions on harvesting e-mail addresses automatically. Penalties are potentially much higher than in the US or in Europe: “Civil penalties under the Act will be assessed according to a sliding scale for repeat offenders. An individual could be liable for up to a total of A$44,000 … for contravention on a single day, while an organization could be fined up to $220,000 AUD in a day. Offenders with a prior record will be penalized up to a maximum of A$220,000 … for each day of spamming by an individual, and A$1.1 million … per day for organizations.”

Although the Australian law has many admirable features, it founders on the reef of international spam. As commentators note in the White Paper, national laws will inevitably fail to control spam sent from outside their borders. According to a UNCTAD (United Nations Conference on Trade and Development) report on the origins of spam in 2003, the sources were

- 58.4% USA
- 5.6% China
5.2% UK
4.9% Brazil
4.1% Canada
21.8% Other

[On a side note, I have been receiving the most amazing junk e-mail from China lately – ads in comically bad English for everything from inflatable dolls the size of buildings to industrial flooring components and chemicals. Given that China has one quarter of the world’s population and an economy that is growing at 9-11% per year, this trickle bodes very badly for the future of our inboxes.]

I think Michael Osterman summed up the situation well in his commentary: “Spam legislation, while well intended, will not control spam alone. The only answer is to fight spammers with the same weapon they use: technology. The problem with spam will be better faced by IT staff then by legislators. To control spam, it must be rendered economically non-viable. Now that is difficult to achieve because it costs virtually nothing to send; however, if we can increase the cost of sending a spam message, we can make it nonviable and the only way we can do that is through the increased use of anti-spam tools. . . . When anti-spam filters are effective they can eliminate 95% or more of the incoming spam, "...If an anti-spam filter can stop 95% of the spam that reaches an end user, the cost to the spammer of reaching that potential customer has risen by 20 times. Increasing the effectiveness of these filters to 97% increases the cost to the spammer by 33 times. The hope is that the potential revenue available to spammers drops by a corresponding amount, and equilibrium is reached.”

* * *

The Vircom White Paper is available through a simple registration process from <http://www.vircom.com/Products/Modus3/Whitepapers.asp>.

* * *


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 © 2004 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.