In Defense of Spam

Neville Holmes, University of Tasmania

Denigrating spam has become a popular activity, if an ill-directed one. My experience with defending PowerPoint tells me that, before I begin defending spam, I should emphasize that by doing so I am not necessarily praising it.

In the letters column in *Computer*'s July 2004 issue, correspondent Davy Cheung concluded, "Does anyone really believe that anti-spam—or 'unsolicited communications,' to be exact—laws are not necessary?" In the October 2004 issue, Brian Whitworth and Elizabeth Whitworth spelled out why "passing laws in virtual worlds has several problems" ("Spam and the Social-Technical Gap," pp. 38-45). After describing four major problems, they observed that "the long arm of the law struggles to reach into cyberspace."

Indeed, it seems that antispam legislation has been largely ineffective. How can this impasse be broken?

Legislators' well-meaning attempts to eradicate spam are woefully misdirected.

DEFINING SPAM

The word *Spam* is a registered trademark (www.rsi.com/spam/) long owned by Hormel Foods LLC. Kenneth Daigneau, a New York actor and the brother of a Hormel executive, coined the trademarked term *Spam*, which came into successful commercial use in 1937. Some sources suggest that the term derived from a contraction of "spiced ham." During World War II, Spam—not being rationed as beef products were—was consumed widely, especially in the armed forces. Spam became so ubiquitous that the medal given by some governments to all those who served in that war at home or abroad was colloquially called "the spam medal." This sense of unlimited dispersal appropriately describes some varieties of the electronic messages now called spam.

Wikipedia (en.wikipedia.org/wiki/Spamming) defines spam as "the use of any electronic communications medium to send unsolicited messages in bulk" and refers to five different media: e-mail, messaging, newsgroups, mobile phones, and Internet telephony. Spam also refers to Web site interference that, for example, increases a product's search engine ranking through spamdexing. According to Wikipedia, blog, wiki, guestbook, and referer spam are all prevalent as well.

ANTISPAM LEGISLATION

Spam has been targeted by special legislation that seeks to control it, although legislators disagree about what it is and why it must be controlled. In the European Union, for example, the Privacy and Electronic Communications Directive 2002/58/EC is inclusive within the general scope of regulating the use of many kinds of personal data. Article 13(1), a minor exception aside, "prohibits the sending of unsolicited commercial communications by fax or e-mail or other electronic messaging systems such as SMS or MMS unless the prior consent of the addressee has been obtained…."

The US based its legislation—the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003—on the determination that commercial electronic mail should be regulated nationwide, that senders should not mislead recipients, and that recipients have a right to decline receiving further e-mail from a sender.

The Australian Spam Act of 2003 seeks to regulate *commercial* e-mail and other types of *commercial* electronic messages, forbids these when unsolicited (with exceptions), requires the sender to be identified and the receiver to be able to opt out, forbids address-harvesting programs and their output, and emphasizes that the main remedies are civil.

This legislation is typically voluminous and difficult to understand in full, which perhaps explains why there are many accompanying documents that, in particular, explain how businesses can continue their use of the Internet for marketing.

All of which makes it difficult to understand why—assuming lawmakers considered the existing legislation that relates to the control of marketing inadequate—they chose not to amend this legislation so that it would be adequate.

It's almost as though US and Australian legislators felt that the Internet itself, not the marketers, pose an extraordinary threat to users. After

Continued on page 86

Continued from page 88

all, the legislation carefully provides for Internet marketing to continue, proving that lawmakers do not consider marketing itself a problem.

JUSTIFICATION

The explanatory memorandum justifying the Australian legislation cites spam's effect on several aspects of Internet use:

- *User confidence.* "Today, the problem of spam has … a significantly negative effect on users' confidence in using e-mail." But why is this a government concern? Given that e-mail is a commercial service, user confidence should properly be the service provider's concern.
- *Network integrity.* "There are clear signs of a deleterious impact on the performance of the global e-mail network … [which] could mean the end of e-mail as an effective form of communication." But surely if the network fails to function satisfactorily, its commercial owners should use technologists to fix it from the inside, not the government to fix it from the outside.
- *Privacy.* "There are significant privacy issues surrounding the manner in which e-mail addresses and personal information are collected and handled." Is this peculiar to the Internet? Shouldn't the Internet's owners be responsible for that medium's methods of handling personal information? Certainly the European Union legislators think so.
- *Content.* "There are obvious … concerns with the illicit content of a considerable amount of spam—including those that promote pornography, illegal online gambling services, pyramid selling, get rich quick schemes or misleading and deceptive business practices." If such content is harmful, should it make a difference whether it appears on the Internet? If many are gullible enough to be taken in by spam, shouldn't the government be concerned about its constituents' gullibility rather than the bait? Shouldn't government ask instead why the education system has let society down?
- *Spoofing.* "Spammers may use spoofing to route spam through a reputable organization in an attempt to entice recipients to open and respond to their messages." Isn't this a technical problem that should be dealt with by having the Internet protocols prevent false addressing?
- *Financial costs.* "These [estimated to be huge] costs are usually borne by Internet users (and/or) employers … Spammers … bear relatively small costs in sending these messages." Surely, this amounts to saying that the business model is wrong. Why should the government try to cover up business problems? Won't this merely delay the development of a more viable and amenable Internet?

Software cannot undermine society, although _people_ can use it to do so.

After some discussion of spam statistics, the Australian report eventually tackles the basic issue: Why is antispam legislation necessary? The report gives the following reasons:

- most spammers are not subject to codes of practice,
- applying present content laws to spam could be expensive, and
- technical solutions are imperfect and can't relieve the overload on the Internet.

These reasons raise more questions than the report answers. What is the law but a code of practice? How will the spammers be constrained to obey the law anyway?

If this is all primarily about unsolicited broadcast commercial electronic messages, and the government seeks to protect me from them, why won't it try to protect me from the unsolicited broadcast of commercial electronic messages that overwhelm television, particularly around seven in the evening and during major sporting events? Government makes the commercial television stations responsible for the advertising they accept. Why don't they put the same responsibility on the Internet owners?

If applying present content laws to spam would be expensive, why not improve the present laws rather than come up with new law specific to the Internet? After all, the Internet isn't the only game in town. Will there be new laws regulating content over mobile phone transmissions? What happens if RFID technology gets extended to sending messages to mobile phones in the neighborhood—will the spam laws then need further expansion?

Surely the focus should be on the content itself rather than on the particular medium.

Technical solutions are always imperfect—at least to some degree, as Bob Colwell will tell you. This provides a compelling reason to improve the technology, not to resort to legislation.

I'm puzzled by the talk of overload on the Internet backbone. How could e-mail overwhelm dense wavelength division multiplexed optical fiber? Doesn't the repetitive downloading of the complex and largely pointless graphics that adorn most Web pages place a far greater burden on the Internet, not to mention on the user's patience? What's going to happen when the browsers start interleaving fancy commercials with their browsings?

Perhaps these questions explain why antispam legislation doesn't seem to be having much effect and why spam filtering and blocking remain the primary tools for countering spam. Even these measures don't stop the spam from being sent, and spammers can usually work around the countermeasures. They can also have side effects, such as contributing to the digital divide

(www-staff.it.uts.edu.au/~lueg/papers/asistam04.pdf).

SYMPTOM OR DISEASE?

In treating diseases, a physician might succeed in alleviating the symptoms but will always realize professionally that eradicating the illness requires seeking the cause. If the cause is a continuing one, the disease can only be conquered by removing that cause. If it's not, merely knowing what caused the illness can help to more quickly and thoroughly restore the patient's health.

Much the same principles apply to alleviating malfunctions in the use of digital technology. In a thoughtful and prescient article, "Copy Protection Technology Is Doomed" (*Computer*, Oct. 2001, pp. 48-49), Dan S. Wallach argued that copyright violations constitute a commercial disease and that the "only way to prevent teenage girls from freely sharing boy-band MP3s will be to provide reasonably priced service that's irresistibly better than free file sharing." This seems to be the direction the recorded music industry is finally moving in, albeit reluctantly and ponderously.

The disease behind illegally copying digital entertainment or software is, however, in contrast to that behind spam, spim, viruses, and hacking. The first is theft, because legislators have seen fit to create monopolistic property rights over intangibles. The second is intangible assault even if, as in the case of phishing, it's with a view to theft. Someone sends the spam to someone else or damages or abuses someone else's computer without permission. The first is impersonal, the second personal; the first is a commercial disease, the second a social one.

Computing professionals are not responsible for diagnosing the social disease behind digital assault. This problem is arguably only one symptom of a disease that includes everything from telemarketing and littering to massacre and terrorism. However, digital assault is easier to study than other social malaises, and computing professionals should team with social scientists to help investigate social phenomena.

It is proper, even mandatory, for computing professionals to design and implement systems that make digital assault more difficult to commit. The Whitworths focused on fairness and legitimacy as aims that digital technology can support to discourage such assault. They concluded that "If software is to support society, not undermine it, legitimacy concepts must be taught in core information system design courses, as a social-technical requirement."

Nevertheless, at the social level, digital systems serve merely as intermediaries in digital interaction, and designing them to make digital assault more difficult would only treat the symptom. *Software* cannot undermine society, although *people* can use it to do so. Digital technology supports people, and people, in turn, can support or attack society.

Sending someone an unsolicited commercial electronic message is illegitimate only if done with malicious intent. Digital systems can be designed to deter certain kinds of digital communication, but this does nothing to deter malice and could even amplify it.

If all professionals learned about social actualities as well as concepts, they would be better placed to choose, design, and implement procedures and systems that lessen the causes of malice in society. ■

Neville Holmes *is an honorary research associate at the University of Tasmania's School of Computing. Contact him at neville.holmes@utas.edu.au. Details of citations in this essay, and links to further material, are at www.comp.utas.edu.au/users/nholmes/prfsn.*

Editor: Neville Holmes, School of Computing, University of Tasmania; neville.holmes@utas.edu.au. Links to further material are at www.comp.utas.edu.au/users/nholmes/prfsn.