Vi@gr@ $old h^r^:
Is your annoyance our problem?

Chris Berg

By the end of the year, the number of emails sent worldwide is predicted to reach 136 billion per day. An estimated 64 per cent of these, however, are spam—unsolicited emails sent in bulk, usually of a commercial nature.

The question is how to deal with the spam—should it be left to internet entrepreneurs and innovators, or to government regulators?

Spam is popularly derided for a myriad of reasons.

Like most technological developments in communication, spam marketing has been pioneered by the porn industry. Most people with email addresses will now be intimately familiar with the benefits that Viagra has on 'performance', often graphically illustrated.

Spam is said to have a negative impact on productivity. A survey in the US, the 2004 National Technology Readiness Survey, found that workers spend 2.8 minutes per day deleting spam, at a total cost to US businesses of $21.58 billion annually in lost productivity. While the survey's results, which relied on self-reporting, implied that workers spent more than 9 seconds deleting each spam message they received, the findings reflected a broad social belief that spam does not merely annoy, it harms.

As well as being detrimental to productivity and offensive, spam has also become a tool of the fraudster—Nigerian royalty are looking for investment partners right now.

Chris Berg is Editor of the IPA Review

Spam is not restricted to email—spambots (automated robots which crawl the Internet looking for places to put spam, in part to raise their Google rankings) are now a common curse of the comments section on blogs, and a burden on website administration.

In response, governments around the world have stepped in to try to curb the evil of spam. The US *CAN-SPAM Act* 2003 requires email solicitations to provide details such as opt-out information, warnings about adult content, and a valid physical address of the business.

The Australian *Spam Act* 2003 goes much further—making it illegal to send 'unsolicited commercial electronic messages' that have an Australian link, with the usual exemptions for charities, political parties, and the government. The penalty for doing so can be as high as $1.1 million a day.

Despite the well-publicised efforts outlined above, spam continues to grow in quantity. While the Australian Government may be able to punish businesses with Australian links or physical addresses, there is absolutely nothing they can do to punish Russian—or Nigerian—spammers. While the legislation stops at the border, in a networked world, the spam does not.

Given that the problem is worldwide, it was perhaps inevitable that the United Nations would come to consider spam as a matter of utmost importance. Combating spam has become a central plank in the UN's push to take over regulation of the internet.

None of these legislative remedies works. In fact, spammers don't tend to obey laws. No legislation, no matter how draconian or restrictive, would be able to stop spam.

As one of the founders of the internet's architecture, Vince Cerf, says, 'if all you have is a hammer, everything looks like a nail. If we are not careful, we may fall into that trap by trying to develop overly simple definitions for what is really a very complex question'.

It is much wiser to leave anti-spam measures to the private sector, to place the responsibility for removing spam from mailboxes on the owners of those mailboxes, rather than a Canberra-based spam taskforce. Anti-spam technology is one which the private sector is well equipped to develop. Sensible protection measures on individual machines, as well as responsible handling of spam messages (never respond to spam) reduce vulnerability. Email filters, available at all levels of ISP-user interaction, are able to reduce spam by a variety of methods—searching for commonly used spam words, statistical analysis, authentication, checksum-based filtering, and a whole host of others.

The back and forth between spammers and anti-spam developers has forced spammers to innovate and produce what will likely be remembered as a cultural artefact of the period—replacing 'viagra' with '|/@g^ra'.

There are clear indications that the anti-spammers are winning. Google's web-based mail service, Gmail, has a spam filter which is remarkable in its capacity to identify dodgy messages accurately. Existing filters are highly effective in screening for malicious attachments—the only real danger that spam poses.

We haven't been introduced... :)
Want to increasee your pleasure?
Boost your sexual perrformance?
Ci@@liis SOFT
Vii@grr@ SOFT

DO-NOT-CALL OR DO NOT ANSWER?

Governments' efforts to protect us from spam are indicative of an approach to modern communications which is expensive, symbolic and useless. Rather than allowing communications technologies to develop at the pace at which the market dictates, governments are intervening whenever it sees a 'threat'—even if it is undefined and merely an annoyance.

Does the mere fact that people are annoyed require government action? Is it the government's role to encourage the productivity of individual workers? These seem to be the rationale behind the *Spam Act*, and the rationales behind the increasing amount of anti-annoyance legislation.

The Do-Not-Call list is another example. Modelled on the US system, the proposed Australian Do-Not-Call list is an opt-in list for those who do not wish to receive commercial telemarketing on their home phone.

On the grounds that unsolicited commercial phone calls are intrusive, the do-not-call list would fine companies who called people who had registered. Similar exemptions apply here as with spam: charities, political parties and research institutions—as if these groups do not make intrusive calls seeking money!

With no apparent irony, the Consumer's Telecommunications Network's executive director, Teresa Corbin, stated in October that telemarketing 'is a huge issue for consumers. It should be dealt with the way spam has been dealt with—effectively and by the Government'.

Although Corbin draws the parallel for the wrong reason, spam and telemarketing are clearly similar—and have similar, free-market solutions.

Individuals are free to hang up the phone, and even to disconnect it when they do not wish to be disturbed. For those who don't want to miss important calls, using answering machines to screen calls is not exactly a new development. And the market has come up with numerous other technological solutions—various products are available on the market that can screen telemarketers' calls specifically, detecting the telltale signs of a call centre autodialer and hanging up the call.

MALICIOUS CONTENT: SPYWARE AND ZOMBIES

While telemarketers and (in most cases) spam emails are not malicious, some unsolicited communications material can be. Spyware, roughly understood, is software that installs itself on your computer without your knowledge, desire or approval. Not only can it render the machine unusable if it is allowed to build up, but it can also report private information on it to another party. The challenge of making even a working definition of 'spyware' illustrates the haphazard approach any legislative solution to the problem would present.

As the danger of spyware is greater, so is the response from the software community. The anti-spyware market is highly competitive—AdAware and Spybot Search & Destroy, two programs which are considered essential to keep a Windows computer clean, have been joined by a Microsoft anti-spyware system.

Any legislation to tackle spyware would have little effect on the major sources of the problem—the software markets operating out of Russia and Asia which constitute the bulk of nefarious activity. As Andrew Grossman of the Heritage Foundation says, 'no set of regulations, no matter how finely detailed, would have much of an effect'.

The Australian Communications and Media Authority has recently announced its intention to intervene when computers have been hijacked by spyware or other users and are broadcasting unintentionally over the Internet—a phenomenon known as 'zombies'. A worthy cause, but again, one in which government's involvement is unnecessary and ill-advised.

Responsibility for the Internet and the computers connected to it has to remain with those who have a stake in them—that is, users and internet service providers. If, as it seems clear, the government cannot keep up with the pace of innovation in spam, spyware, and telemarketing, then its input is at best unnecessary and, at worst, counter-productive. A government insisting that it is tackling the problem of spyware would rob users of an understanding that they have to protect their machines themselves.

Depending on who you listen to, the first act of spam occurred either in 1978 or in 1994. The first *Spam Act* was passed in 2003. The decade-long lag between the invention of spam and the legislation to protect against it is a perfect illustration of the futility of government action in protecting people against the horrors of the internet.

IPA