Canning the spam

By Alan Pedersen

GROWING AT EPIDEMIC PROPORTIONS, Internet spam is stifling industry's efforts to develop e-commerce. But a new e-mail seal programme developed in the US could help to inject some consumer confidence back into the e-mail marketing industry.

E-marketers are in dire need of distancing themselves from fraudulent e-mailers. The "Trusted Sender" seal programme aims to help them do just that, by separating out the good guys from the bad. The project is a joint initiative between technology and consultancy group e-Privacy and not-for-profit privacy organisation TRUSTe.

Based on the principles of TRUSTe's website seal programme, the scheme works by embedding a digital seal in the body of an outgoing marketing message. The recipient can click on the seal to verify the sender's identity, the details of their privacy policy, and gain access a dispute resolution service should they question the validity of the message. Companies who sign up to the scheme are required to adhere to TRUSTe's privacy rules, but will in theory reap the benefits of greater response rates from consumers. The theory is that sealed e-mails promote greater confidence, leading to more consumer spending.

Initial reactions have been positive, with groups such as the Association of Interactive Marketing (AIM) and the International Association of Privacy Officers (IAPO) backing the scheme. However, if it is to be successful, Trusted Sender will need to persuade both industry and consumers alike, that it is a worthwhile project.

A SOLUTION NEEDED

E-mail spam is a pain to just about everyone concerned. It's irritating, time consuming, and often extremely offensive. Unsolicited mailing is not just an annoyance to the general public, it is also having a significant impact on the business community. According to an EU study conducted in 2001, the global cost to business of handling spam was estimated at around $8.6 billion. Companies are losing money as employees devote more and more time to deleting unwanted messages. Computer Mail Services, who have developed a free spam calculator, demonstrate that a company with 1,000 employees could be losing up to 90 thousand dollars and over 400 working days a year, just through processing junk mail.

And as the sheer size and volume increases, industry is having to pay out for more bandwidth and storage space. According to a number of analysts, the cost is likely to rise between 100-150 per cent over the next year.

So significant is the problem, that companies are now starting to take action. Last month, law firm Morrison & Foerster LLP announced it was suing Etracks.com, a Californian-based company that delivers untargeted e-mail advertising. Even after complaints, Etracks.com reportedly sent through at least 6,500 unsolicited e-mails. The law firm is now seeking damages of up to $50 per day for each e-mail delivered in violation of Californian state law.

The main threat that spam poses, is to the respectability of e-commerce and the profitability of using e-mail channels for marketing purposes. Legitimate marketers are drowning in a sea of fraudulent and deceptive messaging, which is creating a sceptical and distrustful public. IT analyst firm Gartner estimates that commercial mail from "honest e-mail advertisers constitutes just 20 per cent of the total." This, they say, "dilutes the effectiveness of legitimate commercial e-mail." Research by IMT Strategies last year, backs up this claim by revealing that 77 per cent of its respondents delete unsolicited e-mail without even reading it.

The one ray of light for industry is that consumers are willing to use new media channels if their doubts can be put to rest. A recent survey by US pollsters Harris Interactive showed that nine out of ten consumers are willing to do business with firms that have their privacy policies verified by a third party. Dr Alan Westin, founder of *Privacy & American Business* and the survey's academic advisor, says: "These results offer powerful evidence that if American business wants to affect the attitudes and activities of today's consumer, independent verification is the single most preferred action to accomplish a rise in trust."

ALTERNATIVES ARE FLAWED

Steven Cobb, senior vice president of research and education at the ePrivacy Group, says the Trusted Sender programme is a valuable tool that can help marketers to tackle this problem of consumer mistrust. However, he does stress that it is not "the answer" to eradicating spam. There are other methods for tackling the problem, but Cobb suggests they can be both ineffective and restrictive to business practices.

E-mail filters, employed by some Internet Service Providers, can stop

junk mail from reaching consumers' mailboxes. However, Cobb says that this "black hole" approach can lead to perfectly legitimate mail being lost. Last month in the UK, some corporate users of BT's broadband service found out that legitimate mailings to clients were being blocked by its filter systems.

Deceptive companies, meanwhile, are managing to stay one step ahead, and are constantly finding ways to avoid these filters. "It's very difficult to filter spam by identifying e-mails simply as spam," says Cobb. "It's far easier to identify legitimate e-mails, then remove the rest."

Legislation is another method showing mixed results. In the US, there are a number of state laws that deal with unsolicited e-mail. The Federal Trade Commission (FTC) has also stepped up efforts by launching an anti-spam campaign. It recently announced that it had made settlements on seven cases of unsolicited e-mailing. But legislation misses a large proportion of fraudulent companies. The most serious offenders are often those which operate overseas, or simply avoid detection and prosecution through anonymous e-mailing.

Self-regulation is the best approach for industry if it wishes to avoid the introduction of more stringent legislation. According to Cobb, "there are US state attorney generals who are keen to build careers on action against privacy violation." But, he argues that the business community does not "want a bunch of politicians writing laws on how to use e-mail." Introducing opt-in policies for electronic marketing could have a serious impact on e-commerce. Cobb argues that Trusted Sender could be a way for business to employ effective self-regulation and keep overzealous regulators off their backs.

PERSUASION PROBLEMS

The impact that Trusted Sender will have on industry profit margins will be the most persuasive argument in getting businesses to invest in the scheme. The problem is in convincing industry that consumers will use the seal. One US-based privacy expert says it is a "chicken & egg situation". He

suggests businesses will not sign up if unconvinced that consumers will make use of the seal, or even be aware of it. By the same token, consumers will not see the value of the scheme if only one or two companies have signed up.

One IT analyst told *PL&B International* that whilst the TRUSTe seal programmes may be well known within marketing circles, it has not made a great impact among consumers. Charles Prescott, vice president of international business development and government affairs at the Direct Marketing Association (DMA), draws a parallel with his organisation's efforts. "Try as we might," he says, "the DMA is not all that well known in the consumer community."

He says the success will depend upon "brand confidence". "Most people deal with a brand they trust" he says. "And if the brand isn't known, they don't trust it." Therefore, the Trusted Sender scheme is going to have to build its reputation and raise its profile among consumers. In order to achieve that, a significant number companies will have to take an investment risk and sign up.
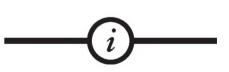
Some high profile companies – including Microsoft Doubleclick, Topica – have already recognised this and agreed to support the programme. Jules Polentsky, chief privacy officer at Doubleclick – an organisation which offers e-mail outsourcing for companies' marketing campaigns – is confident businesses will sign up. He says that the seal is something "desperately needed by industry". As part of its support, Doubleclick recently announced that it will help to raise the profile of Trusted Sender and promote the scheme to its clients.

The fact that Doubleclick is covering the cost of building the seal software into its servers is not just down to some altruistic wish to enhance consumer trust. Polentsky recognises the potential business benefits of Trusted Sender. Aside from the cutting down on staff time devoted to handling complaints, he believes a successful seal programme will lead to more legitimate businesses using e-

mail marketing channels; hopefully through Doubleclick's servers.

A CAUTIONARY NOTE

There is, however, the danger that Trusted Sender could become the sole preserve of richer organisations which have the marketing budgets to pay for the scheme. Joyce Graf, analyst at Gartner, says that whilst large legitimate senders will probably join the scheme, smaller senders will not go to the trouble if it is too expensive. They then "run the risk of being labelled a spammer," she says.

Even if Trusted Sender manages to pull in a sufficient number of members, there is no guarantee that consumers will be any more receptive to legitimate offers. An e-mail to one person may be regarded as a bargain offer, whilst another will view it as nothing more than an annoying piece of junk. If the seal is used for too many unsolicited marketing campaigns – even if the opt-out rules are respected – there is a danger that the seal's integrity could be compromised.

For details on IMT Strategies paper, see: www.nua.ie/surveys/index.cgi? f=VS&art_id=905357231&rel=true

For more information on the Harris Interactive survey, contact Privacy & American Business at www.pandab.org or Tel: +1 201 996 1154

Find out how much money spam is costing your company at: www.cmsconnect.com/ Marketing/spamcalc.htm

Privacy Laws & Business is holding a one day conference, entitled Website Privacy: How to attract and legally use personal data, in London on May 22nd.