

This article appeared in the March/April 2004 edition of the Canadian Bar Association magazine, the "National". It is reproduced with permission of the CBA & the author, Sheldon Gordon.

Copyright 2004. All rights reserved

DROWNING IN SPAM

The deluge of unwanted commercial e-mails has gone from amusing to irritating to downright dangerous for the continued viability of the Internet. Here's an overview of the legislative and technological weapons being deployed to fight spam, along with tips for how lawyers can stop from getting spammed themselves.

By Sheldon Gordon

In November, a California man was arrested on U.S. federal charges for allegedly making death threats against a group of Canadians whom he mistakenly believed were responsible for e-mailing him a large volume of advertisements for penis enlargement medication.

According to court documents, the American e-mailed back his perceived tormentors that he was "sending a package full of Anthrax spores to your address" and would "put a bullet in your head." Although no one would condone his action, many people could appreciate the frustration behind it.

The incident is one of the more bizarre to arise from the proliferation of junk e-mail (also known as spam), but it

DAVID CANTON
Harrison Pensa, London, Ontario

"We can't keep getting more and more spam, or it will become the majority of e-mail that we receive."

« Nous ne pouvons plus continuer à recevoir de plus en plus de pourriels puisque bientôt, ils constitueront la majorité des courriels que nous recevrons. »



STEPHEN GRIMES

DAVID EDINGER
Heenan Blaikie, Vancouver

The U.S. Can-Spam Law “allows unsolicited commercial e-mail, but it restricts both the method by which it is sent and the content.”

La législation fédérale américaine limite le contenu et les techniques par lesquelles les courriels à caractère commercial sont envoyés.

typifies growing public irritation and frustration over the unwanted side effect of what still remains must-have business and personal technology.

Spam overload

In 2001, the average Internet user received 3.7 spam messages per day; the total rose to 6.2 spam messages in 2002. By 2007, it is expected to reach an incredible 830 messages per day. “We can’t keep getting more and more spam, or it will become the majority of e-mail that we receive” warns David Canton, a technology lawyer with Harrison Pensa in London, Ontario. “And people just won’t tolerate it.”

In fact, Canton’s scenario may already be reality. Brightmail, the leading supplier of anti-spam software, reported that in 2003, spam actually exceeded legitimate e-mail, growing from 40% to more than 56% of all Internet e-mail in just one year.

Another recent study by the Pew Internet & American Life Project found that 60% of survey respondents have reduced their e-mail usage due to spam, while 73% now avoid giving out their e-mail addresses. The Internet is drowning in spam.

Spam drains productivity from businesses, including law firms, as employees spend anywhere from 15 minutes to an hour a day pressing the delete key. Consequently, the cost of Internet service rises, as providers have to spend more on filtering out the unwanted messages.

One New York technology industry research firm, Basex, blames unsolicited e-mail for nearly US\$20 billion in lost time and expenses worldwide. Within an enterprise, it reported in December, spam can cost between \$600 and \$1,000 per year for each user.

In Canada, where five billion junk e-mails were sent last year, the cost to the economy reaches \$1 billion annually, according to Senator Donald Oliver, who last September introduced a private member’s bill titled *An Act to Prevent Unsolicited Messages on the Internet* (Bill S-23). But Canada is a relative laggard in exploring anti-spam legislation.

Last December, the U.S. Congress passed the *Can-Spam Act of 2003*, empowering the Federal Trade Commission, state agencies, and Internet Service Providers (ISPs) to take legal action against spammers. The law’s primary targets are the 200 or so hard-core spammers who account for an estimated 90% of all unsolicited commercial e-mails.

“Clearly, the Act allows [unsolicited] commercial e-mail, but it restricts both the method by which it is sent and the content,” says David Edinger, a commercial litigator with Heenan Blaikie in Vancouver who advises clients on the U.S. law. He notes that s. 4 of *Can-Spam* prohibits the use of another person’s computer to send spam.



Other prohibitions cover the use of scripts or automated devices to harvest e-mail addresses and the use of false return addresses. Section 5 prohibits an e-mail from being “materially misleading” in its header, requires that the e-mail have a valid subject line indicating its advertising content, and mandates that the e-mail provide a “live” address to which the recipient can send a message opting out of further e-mails.

The U.S. federal statute follows, and overrides, anti-spam legislation in 30 American states, many of which had tougher curbs that have already produced results — in damages awards.

In 2003, an Atlanta-based ISP called Earthlink won a US\$16.4 million lawsuit against a spammer in Buffalo, N.Y., and a US\$25 million lawsuit against a spammer in Tennessee. More recently, Earthlink invoked a U.S. law normally used against organized crime to sue 25 unnamed spammers in Vancouver, whom it said were using stolen e-mail accounts to send spam.

Last July, as part of a larger action against 150 unnamed spammers, U.S. giant AOL sought a court order against Peer 1, a Vancouver-based ISP, to force it to provide information on clients who were allegedly sending millions of spam messages a day through AOL, marketing everything from pornography to online college degrees to penis enlargers.

“Peer 1 wasn’t about to consent voluntarily, but it did not object to the order,” says Edinger, who represented AOL before the B.C. Supreme Court. “The spammers were all offshore of Canada and the U.S.” AOL, which says spam is the number-one complaint of its customers, has to block over one billion unsolicited bulk e-mail messages every day.

The Canadian front

In Canada, there have been no legal actions pursued by private

citizens or ISPs against spammers, largely because few legal remedies are available. For spam that engages in outright fraud or misleading advertising, sanctions exist under the *Criminal Code* and the *Competition Act*.

Moreover, privacy legislation that took effect on January 1 across Canada provides remedies in certain circumstances. The

federal privacy law and substantially similar provincial statutes impose restrictions and obligations on firms that collect, use or disclose personal information, including non-commercial e-mail addresses, in the course of commercial activity.

But that isn't enough, say anti-spam advocates such as the Canadian Coalition Against Unsolicited Commercial E-mail

Vous pollupostez, ils pollupostent

Pourriels, polluriels ou pollupostage. Si l'équivalent français du terme « spam » ne fait pas l'unanimité, ce n'est définitivement pas le cas pour son impopularité.

En 2002, l'utilisateur moyen d'Internet recevait 6.2 pourriels par jour alors qu'il en recevait 3.7 en 2001. Si la tendance se maintient (comme dirait l'autre), en 2007, 307 messages par jour devraient envahir la boîte aux lettres électronique de ce même utilisateur. Ce qui fait dire à David Canton, un avocat en droit des technologies chez Harrison Pensa à London, Ontario que « nous ne pouvons plus continuer de recevoir de plus en plus de pourriels puisque bientôt, ils constitueront la majorité des courriels que nous recevrons. »

Initiative américaine

En décembre dernier, le Congrès américain entérinait la *Can-Spam Act of 2003*, permettant à la *Federal Trade Commission*, aux organes étatiques et aux fournisseurs Internet d'avoir recours à des moyens légaux pour calmer les ardeurs des polluposteurs. Cette loi a pour principale cible les quelques deux cent polluposters à grand volume qui produisent environ 90% des courriels à caractère commercial non désirés.

« Cette loi permet l'envoi de courriels à caractère commercial [non désirés] mais elle limite les techniques par lesquelles ils sont envoyés ainsi que leur contenu », explique David Edinger, un avocat en litige commercial du cabinet Lavery de Billy à Vancouver. L'article 4 du *Can-Spam* interdit l'usage de l'ordinateur d'une tierce personne pour expédier des pourriels. D'autres articles portent sur l'utilisation de dispositifs automatisés pour produire des adresses électroniques ou l'utilisation d'adresses de retour erronées.

Un impact chez-nous

La nouvelle législation fédérale américaine vise à créer un régime uniforme pour tous les états car certains disposaient déjà de leur propre législation parfois plus sévère. Certaines de ces lois ont déjà donné lieu à des poursuites judiciaires ayant eu des répercussions jusque chez-nous.

En juillet dernier, le géant des communications AOL demandait aux tribunaux d'ordonner à Peer 1, un fournisseur de services Internet de Vancouver, de dévoiler des informations sur certains de ses clients accusés d'expédier des millions de messages par jour faisant la promotion d'un nombre varié de services par l'intermédiaire d'AOL.

« Peer 1 n'allait pas se soumettre volontairement à cette demande mais n'a pas contesté l'ordonnance de la Cour », explique Me Edinger qui était chargé de représenter AOL devant la Cour suprême de la Colombie-Britannique.

Solutions canadiennes

Au Canada, le peu de recours possibles expliquerait pourquoi aucun fournisseur de services Internet ou simple citoyen n'aurait entrepris de procédures judiciaires pour s'attaquer aux polluposters. Le *Code Criminel* ou la *Loi sur la concurrence* offrent des recours uniquement dans les circonstances de fraude ou d'information trompeuse. La nouvelle *Loi sur la protection des renseignements personnels et sur les documents électroniques* et ses équivalents provinciaux offriraient peut-être une certaine protection.

Ce n'est pas suffisant, prétendent les groupes militant contre la prolifération des pourriels. Selon le *Canadian Coalition Against Unsolicited Email* (CAUCE Canada), « le Canada pourrait bientôt devenir le seul pays industrialisé ne disposant pas d'une législation [fédérale ciblant spécifiquement les pourriels] ce qui pourrait en faire une terre d'accueil pour les polluposters [...] »

Me Canton, pour sa part, exprime un certain scepticisme face au recours à des mesures législatives exclusivement canadiennes pour prévenir la propagation des pourriels, les concepts étant limités. « S'agit-il simplement de recevoir un courriel non désiré d'une personne avec qui on entretient aucun lien? », s'interroge-t-il quant à la définition du pourriel. « Si, par exemple, un avocat obtient une liste de courriels et expédie, à des gens qu'il ne connaît pas, un résumé des services qu'il offre,

s'adonne-t-il au pollupostage? La réponse est probablement oui mais cette situation démontre qu'il est parfois difficile de tracer la ligne. » Qui plus est, la plupart des pourriels proviennent de l'extérieur de nos frontières.

Bien qu'il reconnaisse qu'une approche internationale du problème serait préférable, Me Canton fonde plutôt ses espoirs sur l'amélioration des procédés technologiques pour mieux filtrer les indésirables.

Une vision globale

Pour sa part, Me Kirsten Embree, une avocate spécialisée en télécommunications chez Osler, Hoskin & Halcourt à Ottawa estime que le remède idéal serait constitué « de mesures coercitives juridiques réciproques entre diverses juridictions. »

Dans l'interim, Me Embree est d'avis qu'une meilleure utilisation de la *Loi sur les télécommunications* pourrait s'avérer être une bonne solution. Le libellé de l'article 41 de la loi qui énonce que « le Conseil peut, par ordonnance, interdire ou réglementer, dans la mesure qu'il juge nécessaire — compte tenu de la liberté d'expression — pour prévenir tous inconvénients anormaux, l'utilisation par qui que ce soit des installations de télécommunication de l'entreprise canadienne en vue de la fourniture de télécommunications non sollicitées » serait suffisamment large pour permettre au Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) d'intervenir contre les courriels non désirés.

Car au delà de la prohibition, on doit aussi s'assurer d'octroyer des pouvoirs coercitifs aux instances concernées, avance Me Philippa Lawson, directrice exécutive de la Clinique d'intérêt public et de politique d'Internet du Canada de l'Université d'Ottawa. « Il ne sert à rien de créer tous ces interdits sans s'assurer de mettre en place un système pour les faire respecter. » Elle suggère l'instauration d'amendes sévères (par exemple, 25\$ pour chaque courriel illégal) et la possibilité d'intenter des poursuites civiles contre les polluposteurs.

Me Lawson concède toutefois qu'il ne s'agit pas d'une panacée. « Je ne veux pas transmettre l'idée que de permettre aux gens de poursuivre et de créer de fortes amendes feront en sorte de résoudre [tous] les problèmes », souligne-t-elle. « Nous avons besoin de coopération au niveau international et de percées technologiques. » N

(CAUCE Canada) and the Canadian Marketing Association. These groups want to see federal legislation that specifically targets the junk e-mail plague.

"Indeed," warns CAUCE, "Canada may soon be the only industrialized country without such legislation in place, a shortcoming which is likely to lead to spammers regarding Canada as a 'spam-friendly' environment in which to set up shop, given our relatively lenient banking laws and advanced Internet infrastructure."

Under pressure from these anti-spam campaigners, Industry Canada published a discussion paper in January 2003 titled *E-mail Marketing: Consumer Choices and Business Opportunities*. It raised many questions but made no recommendations.

Canton is skeptical about a legislative approach to fighting spam, especially if the legislation is limited to Canada. "First, you have to define what spam is, and it's hard to put into words.

"Is it just unsolicited e-mail from someone who doesn't have a relationship with you?" he asks. "If, for example, a [law firm] obtains an e-mail list and sends out a pitch about their practice to a bunch of people they have no existing relationship with, is that spam? It probably is, but where do you draw the line?"

Even if Canada added a clearly defined prohibition in the *Criminal Code*, adds Canton, the majority of spam is probably foreign in origin. "I don't think it would put more than a small dent in the problem if the Canadian component were eliminated. How do you deal with a cross-border sender?"

"If there's an international approach," he notes, "it would

be much more successful. But if it's only the U.S. and Canada, a spammer could set up offshore, or make it look like it's offshore even though it's just down the street."

Rather than looking to a made-in-Canada legislative solution, or even to an international dragnet, Canton pins his hopes on improved technology to filter out a greater volume of spam. "If you have to mail something to people, you have paper, printing and postage costs. It's expensive to mail things to a lot of people," he says.

"But if you have an e-mail list, you can send to hundreds of thousands of people, and your costs on a per-person basis are incredibly low, so your response rate doesn't have to be high to make it worthwhile. I'm hoping that improved technology will drive down the rewards of sending it."

Searching for solutions

Kirsten Embree, a telecommunications lawyer with Fraser Milner in Ottawa, believes that because so much spam is of foreign origin, the ultimate remedy has to be "reciprocal law enforcement solutions with other jurisdictions." While Ottawa dithers on enacting a comprehensive domestic statute, however, she points to the availability of an "interim measure" in an overlooked section of the *Telecommunications Act*.

Under s. 41 of the Act, she says, the CRTC "may prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications, to the extent that the Commission

STOPPING SPAM

Sick and tired of spam? Consider buying software that will greatly reduce the flow, or adopt these seven steps towards better anti-spam behaviour.

A few months ago, Patterson Palmer's offices across Atlantic Canada were awash in spam. "It was identified as a serious problem," recalls Doug Wright, a partner in the St. John's office and Chair of the Newfoundland Branch of the CBA's Law Practice Management & Technology Section.

The firm's 155 lawyers were receiving "upwards of 60 to 70 junk e-mails a day, in the worst-case scenarios," says Wright. As much of 60% of the messages received by the firm had to be deleted. "In addition to the volume," says Wright, "there were technical consequences, such as viruses that were difficult to eliminate."

So last autumn, several of the firm's lawyers, tired of devoting an hour a day to removing spam from their digital in-boxes, approached the firm's I.T. personnel and asked them to devise a solution.

Their answer, on a region-wide basis, was to acquire and install a software program called Brightmail, whose "Anti-Spam 5.1" was *PC Magazine's* Editor's Choice (along with Postini Perimeter Manager) last November as the best anti-spam products on the market.

Brightmail now filters some 30,000 messages a week at Patterson Palmer's offices.

"It cost in the thousands of dollars, but people here have noticed the difference, and think the expense is worthwhile," says Wright.

Brightmail isn't perfect: it allows 11% of junk e-mail to sneak through, according to *PC Magazine's* tests. But Wright is willing to endure one or two pieces of spam a day rather than risk having legitimate e-mails mistaken for spam.

"False positives are a big issue," he says. "It's not a matter of quantity, but of the importance of what you miss." Brightmail rarely blunders on that score, producing less than one false positive in every million messages.

Buying expensive anti-spam software, however, is not the only way to combat the plague of junk e-mail. Here are seven low-cost alternatives.

1. Keep separate e-mail addresses for different purposes — one for your business, one for corresponding with friends and family, and another (perhaps a Web-based account like Yahoo or Hotmail) for the rest of your online activity. Only the third one likely will be deluged with spam, and you can change it as often as you like.

2. Never respond to unsolicited e-mails from unknown sources, even to request that they

stop sending you messages. That just tells them that you're a live address to which they can send more spam. Don't even open e-mail messages that are obviously spam.

3. Don't give out your e-mail address to any commercial entity without first ascertaining that they have a privacy policy that includes not sharing addresses with third parties.

4. If you have your e-mail address on your Website, don't write it with the @ symbol; write "at" instead; this will thwart "spider programs" that look for the @ symbol in order to harvest addresses off the Internet.

5. Use spam management systems provided by your e-mail program, such as blocking e-mails that originate with certain senders or that contain certain words.

6. Choose your ISP on the basis of how effectively it filters out spam. Read industry magazines or reports to get a sense of a potential ISP's track record in this regard.

7. Report spam to the U.S. Federal Trade Commission and/or to software firms that develop anti-spam applications; many of these firms offer a reporting service that helps them to refine their blocking capabilities. It's a small but satisfying way in which you can help stop spam. **N**

KIRSTEN EMBREE
Fraser Milner, Ottawa

An overlooked section of the *Telecommunications Act* could hold the key to stopping spam in Canada.

« Le remède idéal serait constitué de mesures coercitives réciproques entre diverses juridictions ».

considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression.”

The Act’s language, says Embree, is sufficiently broad to cover unsolicited e-mail messages. Although it’s often assumed that the Act applies only to telecom utilities and not ISPs, she says that the CRTC has recourse against the latter. “The CRTC can go after an ISP [such as Bell Sympatico or Telus] that owns and operates its own telecom network and say, ‘Disconnect this person who is spamming the system.’”

Or, since most ISPs rent the network of a telecom carrier, “it can ask the underlying carrier to disconnect someone who is spamming, simply because that carrier provides the link that runs from the spammer’s premises to the connection to the Internet.”

That said, Embree opposes any federal statute that would make ISPs liable for spam that does not originate with its customers but arrives over its system. “It would be difficult to place onerous burdens on ISPs to monitor spam,” she says.

“They are a natural control point, but they range in size. I’m concerned that we don’t put our smaller ISPs out of business because we impose too great a burden on them to filter spam. Before we talk about imposing obligations on ISPs, let’s talk about voluntary steps to reduce spam on their systems.”

On the other hand, Philippa Lawson, Executive Director of the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa Faculty of Law, advocates a stringent federal law that would ban all unsolicited commercial e-mail without prior, explicit consent from the recipient.

Under such a statute, marketers would have to seek an explicit “opt-in” from consumers, rather than being allowed to target anyone who has not deliberately opted out. Sending an “opt-out” message doesn’t work, she says, because spammers “treat that as a signal that it’s a live address.”

Lawson’s proposed law would also include a standardized labeling requirement for all advertising e-mail, so that it could easily be recognized as spam. The statute would specifically prohibit false, misleading or invalid information in e-mail messages, as well as disguised paths of transmission. It would further ban software products used to harvest e-mail addresses from the Net that falsify return addresses or disguise transmission paths.

“But there’s no point having all of these prohibitions without an enforcement mechanism,” Lawson emphasizes. Her “teeth” would be significant penalties for violation of the law (e.g., fines of \$25 for each illegal e-mail) and statutory provision for civil suits against spammers. “Why not empower governments, ISPs and individual consumers to go after them?” she asks. “The penalties have to be large enough to be an incentive for individuals and ISPs to take spammers to court.”



MIKE PINDER

The U.S. *Can-Spam Act* does not give a private right of action to individuals, instead mandating the Federal Trade Commission, state agencies and ISPs to enforce the Act. Lawson concedes that “a civil right of action hasn’t yet proven to be tremendously effective in stopping spam [when used at the American state level], but I think it’s an important component, and we’re still in the early days of using those kinds of tools.”

“The effective actions are going to be when you get the government or the ISPs and a fair amount of resources behind a large-scale suit,” she adds.

Yet Lawson, too, realizes the limitations of a made-in-Canada legal remedy. “I don’t want to give the impression that legislation giving people the right to sue and setting heavy penalties will solve the problem,” she says. “We need international co-operation and technological advances.”

Today, a solution to the scourge of unwanted e-mail seems out of reach. The spammers always seem to be several steps ahead of the best efforts of both governments and businesses to combat their activities. But according to the experts, there is hope for the future.

Between continuing advances in technology, a rising legislative response to the threat, and perhaps most importantly, better spam-prevention activity by e-mail users themselves, it seems reasonable to think that ten years from now, we may look back on the spam problem as just another developmental phase in the wildly successful growth of the Internet. ■

Sheldon Gordon is a Toronto freelance writer. His last article for *National*, “Fathers’ Day,” was the cover story of the December 2003 issue.