



### **SPAMMING: USE AT YOUR OWN RISK!<sup>1</sup>**

While the Internet opens up exciting opportunities, it also allows entrepreneurs to send information to millions of users quickly, easily and inexpensively. The use of networks to transmit unsolicited, bulk, commercial e-mail, known as "spamming," can cost as little as \$500 to transmit 10 million messages.

Many recipients are less than pleased to receive these messages given the time wasted scanning the subject line and deleting the message. Worse still, these messages can clog the recipients' systems. Spamming can also be a nuisance to e-mail and Internet service providers ("ISPs"), whose reputations and goodwill are tarnished when their service fails because spam has jammed their systems.

While spamming has received much bad press lately, most commentators suggest that recipients really have no recourse. However, this is not the case. Many restrictions are in place to deter this marketing tactic, and the future will likely bring even more stringent regulation.

#### **CRIMINAL AND CIVIL LAW**

Currently, spamming is neither illegal nor subject to specific legislation in Canada. Nevertheless, Industry Canada confirms that computer mischief offences could apply where senders recklessly send spam understanding that the messages will likely interfere with the recipients' access to data or disrupt use of their computer systems.

What is more, a number of contractual and voluntary restrictions have been established to curtail spamming. Many ISPs try to restrict the distribution of unsolicited e-mail in their contracts with Internet users. If these provisions are breached, civil remedies that apply to damages resulting from wrongful actions or breach of contract would generally also apply to on-line activities.

In the only Canadian case on point, *1267623 Ontario Inc. et al. v. Nexx Online, Inc.* ("Nexx"), the defendant ISP cancelled the plaintiff's Internet service for sending spam. Although the ISP's standard contract did not specifically forbid bulk e-mail advertising, it did bind the user to follow generally accepted "netiquette" when sending e-mail. The court observed that while no written netiquette policy exists, a code of conduct for the orderly development of the Internet is evolving based on good neighbour principles. The court relied on American jurisprudence addressing spam in connection with the First Amendment and the tort of nuisance to find that spamming violates these informal rules of netiquette. Specifically, the court noted:

---

<sup>1</sup> This article by Ted Maduri appeared in the November 2001 edition of the Corporate Counsel Newsletter.

Unless a service provider specifically allows in the contract for unsolicited commercial bulk e-mail to be distributed, it appears clear that sending out unsolicited bulk e-mail for commercial advertising purposes is contrary to the emerging principles of Netiquette.

So, organizations planning to send bulk commercial e-mails would be wise to first check for possible provisions in their Internet service contracts that may prohibit the activity. While some contracts expressly prohibit spam, others (like the *Nexx* contract) simply require adherence to netiquette. Either way, businesses using spam as a marketing tool do so at their own peril.

#### **FEDERAL INITIATIVES AND VOLUNTARY CODES**

An Industry Canada working group has released the *Principles of Consumer Protection for Electronic Commerce: A Canadian Framework* (the "Framework") to promote consumer confidence in and facilitate the growth and acceptance of electronic commerce. The Framework's Principle Seven addresses unsolicited bulk e-mail, noting that vendors should not transmit commercial e-mail without the consent of consumers, unless the vendor has an existing relationship with the consumer. Like the Framework's other principles, Principle Seven is designed only to guide the actions of businesses, consumers and governments; the Framework provides no penalties for violation.

The Federal government also encourages independent industry associations to regulate the distribution of unsolicited bulk e-mail through industry-wide voluntary codes of practice. Failure to adhere to voluntary codes may lead to regulatory or civil liability, or disciplinary action by the responsible associations. For example, the Canadian Marketing Association's *Code of Ethics and Standards of Practice* (the "Code") contains an entire section (Section E4) describing the recommended conduct for marketing through electronic media. The provisions require industry members to obtain the recipient's consent and provide an opportunity to reply and unsubscribe before sending spam.

Part I of the Code (Protection of Personal Privacy) outlines seven principles for protecting consumer privacy. Under the first principle, consumers must be given a meaningful opportunity to decline the use of their name or other personal information for any third-party marketing. Violation of any part of the Code can lead to expulsion from the association accompanied by a "broad public announcement."

#### **THE PERSONAL INFORMATION AND ELECTRONIC DOCUMENTS ACT**

The *Personal Information and Electronic Documents Act* (the "PIPEDA"), which came into force on January 1, 2001, covers any organization that collects, uses or discloses personal information in the course of commercial activity. The PIPEDA applies to both the federally-regulated private sector (such as banking and broadcasting) and the inter-provincial exchange of personal information. By January 1, 2004, the PIPEDA (or its provincial equivalent) will apply to every organization that collects, uses or discloses personal information in the course of commercial activity within a province.

According to Canada's Privacy Commissioner, the PIPEDA:

specifies what information a web site can collect from you, and how. It also specifies how this information can be used. As

well, it gives you control over how your personal information, including your e-mail address, is used.

While the Commissioner's comments suggest that the PIPEDA will protect the public against Internet abuses like spamming, the PIPEDA's application to spamming remains largely undefined and untested by the Commissioner and the courts.

The PIPEDA deliberately defines "personal information" broadly as "information about an identifiable individual." The definition excludes the name, title or business address or telephone number of an employee of an organization. According to the Commissioner's PIPEDA Guidelines, the definition encompasses such information as name, age, weight, height, medical records, income, purchases, spending habits, race, ethnic origin, colour, blood type, DNA code, fingerprints, marital status, religion, education, home address and telephone number.

Note that "personal information" is not limited to information that can be used directly or indirectly to identify an individual. Rather, it includes any information *about* an identifiable individual. Thus, the PIPEDA most likely will also apply to personal identifying information, like e-mail addresses, that could be used in conjunction with other personal information to create detailed personal profiles of individuals.

#### **WHAT THE FUTURE HOLDS**

Recognizing the public policy reasons for prohibiting spam, some jurisdictions are taking action. In the U.S., for example, the highest court in Washington state has unanimously upheld the constitutionality of the state's anti-spam law, the *Unsolicited Commercial Electronic Mail Act*. According to the court, the law, which prohibits unsolicited, misleading, commercial e-mail, unauthorised use of third party domain names and misrepresented points of origin, facilitates rather than burdens commerce.

In addition to legislative developments, technological advances should also curb spamming. While spam undeniably is annoying and costly for the average Internet user, spamming does not appear to be overly burdensome at present. However, when spammers are someday able to easily configure bulk e-mail programs to send messages to all e-mail-equipped portable devices, spam will waste the more limited resources of these smaller screened devices with slower-speed connections. Recipients probably will not tolerate paying for airtime to receive and read spam text messages.

#### **CONCLUSION**

While spamming may be a cheap and effective way to market to a great many people, companies would be prudent to consider possible criminal sanctions (computer mischief offences), civil remedies, damage to goodwill, and statutory restrictions before using this marketing tactic. And, companies must realize that new, more stringent Canadian legislation is most likely on the horizon.