LOS ANGELES
Daily Journal
— SINCE 1888 —
Vol. 116 No. 123 **THURSDAY,** JUNE 26, 2003

Companies Using Unsolicited E-Mail Must Be Careful to Avoid Spam Laws

By Frank J. Johnson Jr.

On June 16, Microsoft filed a series of complaints alleging that professional spammers sent millions of unsolicited e-mails over Microsoft's e-mail servers by abusing Microsoft's MSN Hotmail and MSN Internet Access services.

Microsoft alleges common-law claims for trespass to chattels and conversion and statutory claims for violations of the Washington Commercial Electronic Mail Act, the Washington Consumer Protection Act and the federal Computer Fraud and Abuse Act. The software company is seeking an injunction and damages.

According to Hormel Foods, the name "Spam" originated at a New Year's Eve party thrown by Jay Hormel in 1936, when Kenneth Daigneau won $100 for suggesting the now-famous name to describe the well-known canned meat product manufactured by Hormel Foods. Spam is a registered trademark of Hormel Foods in 111 countries.

Not to be confused with Hormel Foods' Spam, the term "spam" today has come to mean unsolicited commercial e-mail. The Internet community widely condemns the transmission of spam, a practice referred to as "spamming," by people known as "spammers."

But how did the phrase catch on in the Internet community? The prevailing theory, adopted by Hormel Foods in a statement about the difference between its Spam and Internet spam, is that the new definition originated with a Monty Python skit about Spam-loving Vikings, who were sitting in a restaurant that served all its food with Spam.

The Vikings would sing over and over, with increasing volume, "Spam, Spam, Spam ... lovely Spam! Wonderful Spam!" It became impossible for the other patrons to converse, because they were inundated with annoying repetitive phrases of "Spam." Thus, the analogy to unsolicited e-mail is that it can overwhelm and drown out normal discourse on the Internet and via e-mail.

With the push of a button, an unsolicited commercial advertisement can be sent to millions, if not billions, of recipients, at a relatively inexpensive cost to the spammer. However, while spammers obtain significant cost savings, they impose significant economic burdens on Internet service providers and recipients.

In its complaints, Microsoft alleges that spam demands storage space and processing capacity from Microsoft's computers and computer systems, making those resources unavailable to serve the legitimate needs of Microsoft's customers. The diversion of these resources impairs the normal operation of the computers and computer systems. Therefore, spamming diminishes the value of that equipment.

Individuals who receive spam must take the time to sort through larger volumes of received e-mail, attempt to distinguish spam from legitimate e-mail and discard unsolicited material. In an effort to mislead e-mail recipients and make it more difficult for them to identify and discard these unsolicited advertisements, spammers frequently use deceptive methods, such as using false or misleading information in the e-mail subject lines.

Spammers also have become sophisticated in trying to cover their tracks and shift greater burdens to Internet service providers. They know that their bulk e-mailing practices inevitably result in a significant amount of e-mail being undeliverable because there is no such e-mail address or because a server is down. When an e-mail message is undeliverable, additional e-mail messages (known as "bounce-back messages") are generated to advise the sender and the provider.

To lessen the burden on their own computer equipment from voluminous bounce-back messages, spammers create the original message so that any reply or bounce-back message is sent to others. Thus, as Microsoft alleges, a spammer who sends spam using a MSN or MSN Hotmail return address can be assured that the inevitable, innumerable bounce-back messages will be returned to that address, not to the spammer's own system. Microsoft alleges that this practice adds to its burdens because its computers must process and store the bounce-back messages from these spam mailings.

Microsoft filed 15 complaints in Washington and California, alleging that its MSN Hotmail service has received millions of unsolicited e-mail messages from the defendants. In some cases, when recipients open the e-mail, they see graphic sexual photographs, invitations to subscribe to adult Web sites and advertisements for additional adult material.

Some of the defendants also allegedly sell spam software that explains basic methods for obscuring the origin of spam. Microsoft alleges that this software describes how the would-be spammer can insert a "bulk-friendly" or "throw-away e-mail address" in the "From:" line of the spam, rather than the spammer's real e-mail address. In addition, Microsoft alleges that the software allows spammers

to make it look like the mail originated from the falsified address, making it difficult or impossible for the spam recipient to contact the real sender.

In its claims, Microsoft first relies on the 19th century common-law concept of trespass to chattel, alleging that the defendants have trespassed onto Microsoft's personal property (its computers and computer networks). Courts have embraced this concept in cases brought by CompuServe (to justify blocking spam sent to CompuServe customers), Intel Corp. (to uphold an injunction against a former employee sending e-mail to current employees) and eBay (to prevent another Internet company from accessing and copying parts of its Web site).

In addition to relying on common law, Microsoft alleges claims for violations of state laws designed to reduce spam and the federal Computer Fraud and Abuse Act, designed to prevent unauthorized access to protected computer systems.

Many states have passed laws restricting unsolicited e-mail. Under the Washington state law at issue in Microsoft's complaints, it is unlawful to send commercial e-mail to an address that the sender knows, or has reason to know, is held by a Washington resident and that uses a third party's Internet domain name without permission, misrepresents or obscures any information in identifying the sender or contains false or misleading information in the subject line. The statute provides for minimum statutory damages of $500 to $1000, unless actual damages are greater.

Comparing Washington's anti-spam law with California's anti-spam law demonstrates the varying requirements in different jurisdictions. Under California's law, unsolicited advertising e-mail may be sent, so long as it includes unsubscribe instructions in the first line of the text of the message in the same size as the majority of the remaining text. In addition, the subject line must begin with "ADV:" for advertising materials or "ADV:ADLT" for adult materials. The law applies to e-mail that is delivered to a California resident by any person or entity doing business in California. It provides for statutory damages of $50 for each e-mail received, with a maximum daily amount of $25,000.

Congress is considering various proposed federal anti-spam laws. For example, in May 2003, Silicon Valley Rep. Zoe Lofgren, D-Calif., introduced the Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of 2003. This legislation has labeling requirements similar to those found in the state statute that would apply to messages sent in the same or similar form to 1,000 or more e-mail addresses within a two-day period. In addition, it would prohibit all false or misleading headers and deceptive subject lines in unsolicited e-mail, regardless of whether the e-mail was sent in bulk.

Also in May 2003, Sen. Bill Nelson, D-Fla., introduced the Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003, which would prohibit the inclusion of false information in message headers in unsolicited bulk commercial e-mail. It also would prohibit spammers from harvesting e-mail addresses of potential recipients from Web pages and other sources. Violations could be prosecuted under the Racketeer Influenced and Corrupt Organizations Act.

In June 2003, Sen. Charles Schumer, D-N.Y., proposed a national "do not spam" registry, similar to a Federal Trade Commission service that is to begin blocking unwanted telemarketing calls.

Many companies and individuals, not just spammers, use mass e-mail as a marketing tool. Offering goods and services, or simply communicating on a mass level via the Internet, can be inexpensive but fraught with risk.

For example, what seems to be a harmless few keystrokes involved in sending a general announcement to a company contact list may be troublesome if the sender is not familiar with how the list was compiled and the identity of each recipient. Such a message may be construed as an "advertisement" or other unsolicited commercial e-mail, subjecting the sender to requirements under various state, federal and even foreign statutes. The possibility of having to defend a lawsuit in a faraway jurisdiction can make it even more troublesome.

If anything, the varying state laws, the pending federal legislation and the recent Microsoft lawsuits should send a wake-up call to companies and individuals involved in sending any type of mass e-mail. If not to lessen the risks associated with commercial e-mail, then to be good "netizens," such companies and people should implement and strictly follow a well-considered e-mail policy.

Frank J. Johnson Jr., a partner in the Del Mar Heights office of Sheppard, Mullin, Richter & Hampton, is a trial lawyer and member of the firm's intellectual property group. He has represented clients in complex business disputes and on issues relating to intellectual property and the Internet.