WILMERHALE

Spammers Face Increasing Legal Obstacles

2003-07-07

As the volume of unsolicited commercial email, or "spam," continues to increase, state and federal authorities are still trying to regulate it. Now, with spam accounting for up to half of all email by some estimates, new legislative and regulatory initiatives are gaining momentum.

The importance of anti-spamming legislation at both the federal and state levels is likely to increase as common law remedies against spam are rejected by the courts. In a significant decision last week, the California Supreme Court overturned a lower court ruling that the transmission of thousands of unwanted email messages to Intel's corporate network was held to constitute trespass to chattels or, as it has come to be known, "cyber-trespass" (see our July 26, 1999 and May 9, 2002 Internet Alerts). In *Intel v. Hamidi*, the California Supreme Court overturned the cyber-trespass ruling, holding that trespass would not be found in California when an electronic communication neither damaged the recipient computer system nor impaired its functioning.

Effective July 1, 2003, Virginia, the home of numerous Internet Service Providers (ISPs), amended its Computer Crimes Act to create what is probably the nation's most powerful anti-spamming legislation. Under Virginia's new law, spammers will now be faced with the possibility of criminal prosecution. If convicted, a spammer can face up to five years imprisonment. The law also allows authorities to seize the assets and profits that spammers earn as a result of their spamming activities. The law makes it a crime to:

1. use a computer or computer network in Virginia with the intent to falsify an email header or other routing information, or use a tool that automates spam; and

2. intentionally send or attempt to send either 10,000 messages within a twenty-four hour period or 100,000 messages in a thirty-day period; or generate $1,000 in revenue from a specific transmission, or $50,000 from total transmissions.

Virginia's spam law is important because much of the global Internet traffic passes through Virginia-based ISPs, such as America Online and WorldCom, and the Virginia law may be applied against nonresidents who use computer networks located in Virginia. Therefore, spammers who send the requisite amounts of spam to America Online subscribers may be prosecuted in Virginia even if they are operating out of a state or foreign jurisdiction with less severe anti-spamming penalties.

Most states with anti-spam laws impose civil, rather than criminal, penalties. For example, states such as Maryland and Washington prohibit spammers from inserting fraudulent information in an email header, and may require violators to pay $500 to each recipient of the email as well as $1,000 to the ISP that handles the spam. In these states, ISPs can take direct actions against the spammers to obtain monetary damages. For example, on June 17, 2003, Microsoft filed fifteen lawsuits in Washington which accuse the defendants of sending unsolicited spam to users of its MSN and Hotmail services. Microsoft is seeking both monetary damages and various court orders to stop the more than two billion spam emails its members and customers receive.

Other anti-spam laws, such as those enacted in Arizona, California and Colorado (see our October 26, 1999 Internet Alert), require advertisers to insert "ADV" or "ADV-ADLT" in spam email headers unless consumers give their permission, or "opt-in," to receive such email. As we discussed in our December 11, 2002 Internet Alert, a bill recently proposed by Massachusetts Attorney General Thomas F. Reilly would allow ISPs, the state and consumers to sue spammers for up to $500 for sending spam. The Massachusetts bill would also require advertisers to include an "opt-out" mechanism, prohibit fraudulent information from being inserted into email headers, and prevent advertisers from garnering other potential email addresses.

Other states that do not have anti-spam legislation, such as New York, have fought spammers using other laws. In May 2002, Eliot Spitzer, the Attorney General for the State of New York, filed a lawsuit against MonsterHut, Inc. alleging that the company sent more than 500 million fraudulent unsolicited commercial emails in violation of New York's deceptive business practice laws. *New York v. MonsterHut, Inc.*, Index No. 402140/02 (N.Y. Sup. Ct., January 6, 2003). MonsterHut had fraudulently advertised that its email marketing services were permission—based or "opt-in." In January 2003, a New York lower court held that MonsterHut had fraudulently represented its email marketing services as opt-in, as shown by the fact that the company failed to remove more 750,000 consumers who asked to "opt out" of the service.

To date, no federal anti-spam legislation has been enacted, although several bills are pending in Congress. Two examples are the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) and the Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003. The CAN-SPAM Act would require, among other things, unsolicited commercial emails to be appropriately labeled, without the use of deceptive email headers, and include opt-out instructions. The Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003 would prohibit spammers from inserting fraudulent information in email headers, from garnering email addresses of potential recipients from other sources, and require opt-out instructions.

Just recently, the Federal Trade Commission (FTC) petitioned Congress for more authority to secretly investigate spammers who inundate consumers with unwanted spam. Since spammers have been known to hide their assets during FTC investigations, the notification requirements have hindered such investigations targeting the spammers. The FTC proposal provides for effective measures to conduct these investigations and broadens the FTC's powers to target the spammers. Modeled after the disclosure requirements in telemarketing laws, the FTC's proposal requires spammers to disclose their identity and what they are advertising for sale.

The European Union has also adopted new restrictions which ban the use of spam, except in certain situations. For a discussion of those restrictions, see our August 12, 2002 Internet Alert.

This new wave of anti-spamming legislation is intended to minimize the amount of spam sent to consumers and prevent spammers from using fraudulent and deceptive practices. As we have seen, however, different jurisdictions have taken different approaches intended to address the same problem. While Virginia threatens spammers with the possibility of incarceration, other state laws have threatened spammers with high fines and lawsuits by ISPs. What is the best approach, and will any of this be effective? Only time will tell.

Authors

John C. Christie Jr.

RETIRED PARTNER

+1 202 663 6000