ARE YOU DOING E-MAIL MARKETING? LEGALLY?

Since so many small businesses now do a substantial part of their marketing on the Internet, it is not surprising that many have resorted to doing e-mail marketing to advertise their products or services, since it costs next to nothing to send out zillions of e-mail messages, other than the cost of acquiring the "mailing lists." You can't help be aware of this kind of marketing blitz, since everyone on the planet with an e-mail address seems to receive dozens of e-mail ads every day for such necessities of life as those wonderful herbal supplements that will supposedly enlarge certain critical parts of your anatomy.

In recent years, most of us are have grown tired of receiving these unwanted, unsolicited junk e-mail messages ("SPAM"), which now make up something like 80% of the e-mail volume we receive , even after SPAM filters have done their work. That has led to pressure on governments around the world to do something to stem the tide of SPAM. However, many of us who run small businesses may have privately thought about using such e-mail campaigns ourselves to market our own products or services. Or maybe we are doing it already, unaware of the possible legal consequences. Since we receive such a huge volume of SPAM in our e-mail inboxes every day, it isn't hard to jump to the conclusion that, since everyone does it, SPAM must be legal, as long as you aren't selling or promoting something like weapons-grade plutonium or some type of sleazy scam.

Right?

Wrong. In fact, most of the SPAM you receive on a daily basis (even "innocent," non-fraudulent SPAM) is illegal under U.S. laws, but since most of the illegal e-mail solicitations originate in places that don't crack down on SPAMmers, or even encourage them, there is very little most Western governments can do about it.

However, many small businesses who have heard about the new federal anti-SPAM law may be unnecessarily refraining from doing e-mail marketing, for fear of the legal consequences. Such caution is certainly warranted, but you should not assume that *all* e-mail marketing is illegal. It is still possible to legally send unsolicited e-mail to potential or existing customers -- but only if you meet a number of very specific federal guidelines.

Before embarking upon an e-mail marketing campaign, you need to be aware that, even though you and your business may be perfectly ethical and you may be advertising a

useful, legal product or service, you must be extremely careful to avoid both criminal prosecution and, even more of a realistic risk, being sued for private damages by Internet service providers (ISPs) that provide Internet access and who are now authorized to sue the pants off SPAMmers -- for statutory legal damages.

Thus, if or when you decide to do any e-mail solicitations for your business, you first need to know what the legal ground rules are, to avoid incurring fines or massive legal liability to ISPs, either of which penalties could put you out of business in a hurry. Those "ground rules" are all summarized in the remainder of this article, below, adapted from the author's e-book, **"Starting and Operating a Business in Colorado,"** part of his e-book series for each of the 50 states. (2008 Colorado edition and all other state editions available from www.roninsoft.com.)

Federal Government Comes Down Hard on (U.S.) SPAMmers

The U.S. Congress has enacted legislation, effective in 2004, in an attempt to stem the flow of unwanted, unsolicited junk e-mail ("SPAM") and "porn mail" on the Internet, by enacting the "CAN-SPAM" Act [15 U.S. Code Sec. 7701]. This law imposes hefty penalties of up to $250 per violation (limited to $2 million total) on SPAMmers who engage in any of these practices:

- Distributing "porn mail" -- commercial e-mail with sexual content, such as messages promoting pornographic web sites or sale of pornography;
- Sending out e-mail with deceptive "headers" or subject lines, which disguise the nature of the commercial message within;
- Sending e-mail with false return addresses ("spoofing") or false IP (Internet Protocol) addresses;
- E-mail solicitations sent to "harvested" addresses (gathered automatically from Internet web sites by special robot software) or to "dictionary lists" of e-mail addresses created by mechanically generating large numbers of target addresses, such as: abc1@xyz.com, abc2@xyz.com, abc3@xyz.com, etc.;
- Sending e-mail solicitations to recipients who have requested that the sender (or all senders) cease sending messages to that recipient, more than ten business days after such a request; or
- Sending fraudulent e-mail, such as chain letters, or promoting other fraudulent schemes such as the now famous Nigerian Scam, which has bilked gullible and greedy folks out of billions of dollars (making that particular scheme the second largest source of foreign exchange for the nation of Nigeria, second only to its oil exports).

The chances of your being prosecuted for minor technical violations of the CAN-SPAM act may not be that great, but there are other severe anti-SPAM penalties that can be enforced by private Internet service providers whose servers are being jammed with huge numbers of SPAM messages, costing them both time and energy to deal with it.

These provisions of the new law not only include harsh sanctions, but provide major incentives to ISPs to sue you for violations. Under the CAN-SPAM law, ISPs may seek statutory damages from a SPAMmer who uses their facilities or servers to send SPAM that violates the anti-SPAM rules. The liquidated damages are set at $25 per message and are increased to $100 per e-mail that uses a fake or "spoofed" return address or false header.

An ISP may collect up to $1 million of such statutory damages in an action against a violator.

Congress also ordered the Federal Trade Commission (FTC) to create, by July 1, 2004, a "Do-Not-E-Mail" Registry, where anyone who wished not to receive commercial e-mail solicitations could list their e-mail address. Mass e-mailers were supposed, in theory, to refrain from sending e-mail addresses listed on the Do-Not-E-Mail Registry. (Yeah, right.) It was to be similar to the Do-Not-Call Registry that has been established to prevent unwanted telephone solicitations, which has had some degree of success.

Luckily for us, reality soon set in at Foggy Bottom. Recognizing that illicit purveyors of SPAM would most likely use such a registry as just another handy list of e-mail addresses to send their SPAM to, the FTC told Congress on June 15, 2004 that the Do-Not-E-Mail Registry would fail to reduce SPAM, since there is currently no way to enforce the registry effectively against SPAMmers who are outside U.S. jurisdiction.

Thus, the Do-Not-E-Mail Registry will apparently not be implemented by the FTC until technological improvements and international cooperation make it possible to effectively enforce the anti-SPAM laws. That may take a while. Quite a while.

You have probably noticed, if you have an e-mail account, that the anti-SPAM laws have so far had zilch effect on the ever-growing volume of SPAM and "porn mail" we receive daily, since most of the SPAMmers are either outside the United States or are using servers in foreign countries, where U.S. laws cannot reach them or find out who is behind them. One expert recently estimated that, since the anti-SPAM laws have made it riskier to send SPAM from within the U.S., some 70% of the SPAM we receive is now sourced from SPAMmers in China or Taiwan, nations that have shown little if any interest in cracking down on SPAMmers.

FACTOID: Postini, Inc., the world's largest SPAM-filtering company, reports that the volume of unsolicited e-mail increased by 147 percent in one recent year alone, and they estimate that 14 of every 15 e-mails that show up are junk. Interestingly, Postini estimates that almost 75% of all SPAM emanates from computers in the United States, mostly due to hackers who implant sophisticated viruses in computers that are connected to the Internet, using your computer or mine as a “slave” to spew out the junk e-mails, thus making it extremely difficult to trace the SPAM back to its ultimate source.

The Ground Rules for Sending E-Mail Solicitations

Although anti-SPAM laws have not been able to stem the tide of unwanted e-mail clogging your in-box, the laws do have significant teeth in them, as noted above, for anyone based in the United States who sends out SPAM e-mails. Thus, if you are using e-mail as an advertising or marketing tool, you need to know what is, and is not, allowed.

These are the basic rules:

WHAT YOU CAN DO

- Not surprisingly, you can send e-mail solicitations to anyone who has affirmatively consented to receive such messages from you.
- You can send e-mails to a customer or former customer in the process of facilitating or completing a transaction or when responding to questions or service requests from the customer.
- You can also send information to a customer with whom you have an ongoing relationship, such as subscribers to a publication or service you offer, or to notify a customer of product updates or upgrades to which they may be entitled.
- You do not have to first check the "Do-Not-E-Mail Registry" before sending out solicitations, since, as noted above, the FTC decided not to create such a registry.

Otherwise, you can only send out SPAM if it meets all of the following legal requirements:

WHAT YOU CANNOT DO (UNLESS YOU HAVE THE AFFIRMATIVE CONSENT OF THE RECIPIENT)

- Do not send advertising e-mail with false or misleading headers or subject lines (a tactic commonly used to trick recipients into opening a junk mail message, such as "Lucky you! You have won the Irish Sweepstakes!").
- Do not use false or inaccurate routing information: "From" and "To" routing information must be accurate and must identify the sender. "Spoofing" (using fake return e-mail addresses) carries quadrupled civil penalties!
- Do not promote fraudulent schemes, such as chain letters, pyramid schemes, or variations on the "Nigerian Scam" described above. That types of solicitations are illegal under numerous other federal and state laws, never mind the anti-SPAM laws.
- Don not send e-mail solicitations to "dictionary lists" of e-mail addresses that are created by mechanically generating large numbers of target addresses, such as: abc1@xyz.com, abc2@xyz.com, abc3@xyz.com, etc.
- Do not send e-mail solicitations to addresses that have been mechanically "harvested" (gathered automatically from Internet web sites by robot software).
- Do not send advertising to anyone who has asked you not to e-mail them.
- Do not send advertising solicitations unless you do all of the following in the e-mail:

    - Clearly identify the message as advertising, and advise the user how to opt out of receiving further solicitations, using an e-mail or other Internet-based mechanism by which the recipient can opt out. You must process the recipient's request within ten business days of receipt and must not provide that recipient's e-mail address to another party;
    - Include a valid e-mail return address;
    - Identify your company; and
    - Include your physical postal address.
- Do not send solicitations with sexual content unless the recipient has affirmatively consented to receive such messages from you, or unless the header or subject line provides a warning that the e-mail contains sexually explicit material or is promoting such material.

WARNING:

It is not illegal for you to send out unsolicited commercial e-mail, or SPAM. But you MUST heed all of the foregoing rules. Any failure to toe the line can subject you to heavy criminal penalties and fines, as well as potentially disastrous statutory damages from the private lawsuits that can be brought against you by ISPs.

EUROPE HAS ANTI-SPAM LAWS, TOO:

While unsolicited SPAM is illegal in the U.S., you may be thinking, "OK, I'll just send my SPAM solicitations to e-mail addresses in Europe, instead of to U.S. recipients." Forget that. The 2002 EU Directive on Privacy and Telecommunications gives everyone in EU countries the right to seek legal damages against the senders of unwanted e-mail, fax, or text messages.

[Footnotes deleted]

About the Author: Author Michael D. Jenkins, is a graduate of the Harvard Law School and has practiced as a tax attorney and a CPA with major California law and CPA firms and with a major national management and economics consulting firm in Washington, D.C.. Since 1981, he has authored the **"Starting and Operating a Business"** series of small business guidebooks for each of the 50 states and D.C., all of which are now published only in electronic format (e-books with included Windows software that customizes the book for the user's specific business). Each 2007 or 2008 state edition is roughly 500 to 600 pages, if printed out. For ordering or more information on these guidebooks, see: http://www.roninsoft.com/advisor.htm

Note to editors/writers: A Microsoft Word file version of this article is also available on the author's web site, at:

http://www.roninsoft.com/_nonpublic/SPAM_law.doc

...and an HTML file (web page) version is also available at:

http://www.roninsoft.com/_nonpublic/SPAM_law.htm