



» canning the SPAM

BY JIM MOSS

This isn't a matter of "where's the beef?" If you want to fax or email a customer in 2005, you're going to need written permission ...OR ELSE.

How do I love thee?

Let me count the ways: by phone, by fax, by the U.S. Postal Service and through the Internet. But what if your love no longer wants to hear from you? You had better follow Elvis' advice and send her a letter by mail, because anything and everything else is going to get you in hot water.

Over the past 10 years, consumers have had it with unwanted contact offering sex, pills, mortgages and every other conceivable commodity or scam. This onslaught started by phone and mail, and moved quickly to fax before it leaped into email. Congress and several states have now passed laws to control how consumers can be contacted by advertisers and protect them from unwanted intrusions.

THE FACTS ON FAX

The Telephone Consumer Protection Act of 1991 (47 USCS § 227 (TCPA)) was the first law enacted by Congress to specifically address unwanted intrusions by marketers. The law makes it unlawful to send unsolicited faxes containing advertisements. The act requires an 800 number (by phone or fax) be included in the fax for the recipient to contact the advertiser and request to be removed from the list.

The TCPA is regulated by the Federal Communication Commission (FCC), which also regulates the Can-Spam Act and the Telemarketing Sales Rules. The FCC is amending the rules on faxing effective July 1, 2005, aligning the rules more closely with those on spamming. The new rules will require the sender to:

- » Have prior written permission of the recipient of the advertisement.
- » The business must identify itself in the top or bottom margin of each page or on the first page of the fax message and must include its telephone number and the date and time the fax was sent.
- » If a facsimile broadcaster demonstrates a "high degree of involvement" in the sender's facsimile messages, the facsimile broadcaster must provide its name on the fax.
- » Faxes sent to fax servers and personal computers are covered by the faxing rules.

The new regulations recognize that companies marketing their prod-

ucts are not the same ones sending the faxes. These commercial faxing operations or "facsimile broadcasters" may supply the fax list as part of their service and, as such, the regulations hold the sender, including the facsimile broadcaster, as a responsible party. The loophole that existed in faxing to fax servers and to computers has also been closed with both of those receiving machines now being covered in the definition of recipient. Complaints can be filed online at www.fcc.gov/cgb/complaints, and fines can reach a substantial \$500 per fax.

DIALING FOR DO NOT CALL

The next wave of laws was the "do not call" laws. People were tired of being contacted to buy items at inopportune times. There were also issues about unscrupulous salespeople selling swampland to unsuspecting consumers. Forty states enacted laws concerning telemarketing, and in 2003 the federal government enacted the Telemarketing Sales Rule (16 CFR Part 310). (For a list of those states with telemarketing laws, go to www.the-dma.org/government/donotcall-lists.) The law works by providing a federal or state website and 800 numbers con-



Deer
Creek
FABRICS, INC.



Deer Creek Fabrics has been supplying technical performance knitted fabrics for over 25 years. From the original warm and dry polypropylene constructions in the late '70s, to the latest energy enhancement Hologfiber collection, innovation has been both customer and technology driven.

Deer Creek has provided solutions for leading outdoor adventurers, top professional and Olympic athletes, and the brave men and women of our police and military.

See what Deer Creek can do for your products. Technologies include energy enhancement and recovery, odor control, sun protection, thermal regulation, flame protection, stretch and moisture management.

Join us at the Fabric Link Industry Panel Discussion on Sunday, January 30th, at 7:30 AM • Salt Lake City Marriott.



Please call (203) 964-0922 to schedule an appointment.

WORK WITH US AT OUTDOOR RETAILER BOOTH 6830



“opt out” provision in the email and requires that no further communication to the recipient be made 10 days after the consumer has notified the sender.

The Can-Spam Act sets up specific requirements when you are going to mass email recipients, even with their permission. There are prohibitions against emailing:

- » False or misleading transmission information.
- » Deceptive subject headings.
- » Emails that do not contain a functioning return electronic mail address, which must be active for 30 days after the email is sent.
- » A clear and conspicuous identification that the message is an advertisement or solicitation.
- » A clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender.
- » A valid physical postal address of the sender.

No electronic communication can occur after the sender has received an objection from the consumer:

The Act does not set up a “do not email” registry, despite widespread Internet myth.

In fact, a quick search for “do not email” registries identifies several Federal Trade Commission articles about these scams and an equal number of fake registries attempting to collect your email address and actually spam you if you register. The only actual consumer service that is available is an email address to forward spam to the FTC so it can take action against the spammer: spam@uce.gov.

Why is the act considered unsuccessful? Because most spam is coming to you from outside of the United States. Consequently, spammers who hide their identities are not going to be found or extradited from foreign countries.

Another problem is we have given permission thousands of times for spammers to contact us in the past, we just did not know that we had done so. Most software that you install, especially something you download from the Internet, such as free-ware or shareware, includes the right to contact you by email. Many of these programs include the right to sell your information to spammers. Although the law now requires a conspicuous notice of their intent to spam and to sell your email address, it will take a while for this to be weeded out of the system.

SIGH, SO NOW WHAT?

In sum, email marketing is cheap, but you must make sure you conform to all the laws.

1. You need permission from the consumer (recipient) to contact him or her, not just a good email address. Consequently, you need the consumer’s name to identify the permission provider.
2. That permission must have been obtained in a clear and conspicuous manner.
3. Your intentions must be clear to the consumer, and you must make it clear whether you are going to share the information with third parties.
4. You must allow consumers a free way to get off your list, and you must follow up with the decisions to be removed immediately.

Marketing has taken a turn back to the 19th century with the advent of this 21st century technology. It’s ironic that the U.S. Postal Service has a monopoly on the ability to mass contact consumers without first receiving their permission.

» SNEWS® has launched a new section with legal advice and case reviews at www.snewsnet.com/lawreview. Direct legal questions to LawReview@snewsnet.com.

Red Ledge—Your window on Mountaineering

- Waterproof and Breathable T-Core LX
- Insulated Liner Jacket
- Welded Sleeve Pocket

**Men's Paladin Parka*

- Waterproof Zipper Pockets
- Fully Taped Seams
- Roomy Hood

**Women's Kali Parka*

Affordable never came with so many features

SIA BOOTH D229
OR BOOTH 3383

thermionAg™
the science of silver

LAYERS

www.layers-outdoor.com
919-834-5007



sumers can use to place their phone numbers on a do-not-call registry. The federal do-not-call website is www.donotcall.gov. Once your phone numbers, including cell phones, are on the list, telemarketers cannot call you. The federal listing is effective for five years.

The do-not-call laws have been quite effective because various state attorney generals have jumped on the act as a way to garner consumer support. Many attorney generals have negotiated large payments from telemarketers who ignored the law.

WHERE'S THE SPAM?

The latest and broadest laws concerning marketing (and, in many people's minds, the least effective) are state and federal anti-spam laws. Spam is the name applied to unsolicited email attempts to sell us such oh-so-useful things as mortgages, pills and access to websites of people doing things we can't see anywhere else.

Thirty-six states have enacted anti-spam laws. Alaska's spam law only applies to material of a "sexual nature." Seven states have made violation of the laws a criminal act. The remaining 29 states have certain requirements when sending spam.

Seventeen states require the email have a label in the subject line and an "opt out" provision in the email. Most of the subject line labels require the letters "ADV" or "ALT" or a combination of both "ADV: ADULT" in the subject line based on the material being sent. The "opt out" requirements are to be fairly immediate and free to the consumer. Five states require only an "opt out" provision, and five states require only a label identifying the message in the subject line as an ad or as sexual material. All of the states allow a recipient to sue the sender.

A great website to stay current with each state's spam laws is www.spamlaws.com. This site lists each state's spam laws and a summary, as well as the federal Can-Spam Act. In addition, the site lists the laws of all other countries and the European Union, which are extremely strict. If you are thinking about emailing people in Europe, a long look at the EU laws is in order.

Another requirement is the sender (spammer) of the message must be easily identified in the message. Hidden headers, email that is bounced through different domains, or ones that do not contain correct routing information are illegal, just as is using another persons' email address without permission.

The states allow either the State Attorney General or the individual to sue the spammer for violation of the act. Most of the laws are in addition to consumer protection acts which allow consumers not only

to recover their damages but also to recover attorney fees, costs, interest and in some cases up to three times the amount of damages for violations.

Many websites have sprung up to assist consumers in suing spammers. The necessary paperwork is available for download so all a consumer has to do is identify the sender and fill in the blanks and off to court everyone goes.

In November 2003, Congress passed "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003," or the CAN-SPAM Act of 2003. The act supersedes but does not eliminate state laws for violation of the federal and state acts. This means a spammer can be sued or criminally prosecuted by the federal government, a state's attorney general and the consumer at the same time.

The Can-Spam act is written very broadly. The definitions close loopholes before they are exploited. The first definition is the most descriptive and helpful in understanding the act—the definition of what is a contact. That is defined as "affirmative consent." Affirmative consent requires that you not only must have permission to contact someone, but also that failing to have permission is a violation of the act. The agreement or consent to contact must be clear and conspicuous so consumers understand what they are agreeing to.

If your intention is to sell the consumer's contact information, the definition of Affirmative Consent also requires you give the consumer: (1) notice of the intent to contact them, and (2) notice of the intent that their email address would be "communicated" to others. Communicated seems to be broadly defined to include every possible way that one person is giving the consumer's information to another, including selling that information. This definition has promoted the check boxes seen on websites and other registration forms that require you to agree to receive mail, whereas in the past you would have agreed to the terms of the website or subscription.

A LOAD OF EMAIL

The next important term is "recipient," the person to whom the information is communicated, or more precisely defined, the person using the email address. Affirmative consent must be received for each email address of the recipient. One final point is if the email address is reassigned to a new person, you must receive consent from the new person. The consent you have from the old person is not sufficient. This places a horrendous burden on the sender to somehow make sure that mail sent, for example, to Snewsbox@snewsnet.com is always sent to Michael or Therese, and if

one of those two are replaced by Jim, then you have to get Jim's consent to email him at Snewsbox@snewsnet.com. Permission is not granted by the email address, but by the person using the email address.

There is no safe harbor for communication to commercial or business entities that exist in many other acts such as the Telephone Consumer Protection Act of 1991. Consequently, every email address being contacted must have consent from the reader, not just the email address. If a commercial operation has multiple email addresses, consent must be received for each email address of the business.

For manufacturers and distributors, or business in general, there are some safe harbors. You can:

- » Continue a transaction the recipient has agreed to or has started.
- » Notify someone of warranty information or product changes.
- » Inform someone of product recalls.
- » Send product safety information.
- » Announce security information.
- » Notify someone of delivery of goods or services or product updates or upgrades if the recipient has previously agreed to be notified of this.

Even though these safe harbors exist, the shoals are still lined with rocks. Notifying someone of a product upgrade probably does not fall within the safe harbor if the notification of the upgrade requires that you buy it. That will probably be defined as selling and, as such, a violation of the act. The safest way to go is to have the recipient agree to receive the information.

Section 4(a)(1)(B) of the act sets forth the penalties for violating the act which start at a fine and imprisonment for up to one year and increase up to five years based on the number of previous convictions, whether you were engaged in another felony at the time, or how many and how often you violated the act.

Section 4(c) of the act also requires forfeiture of:

(A) Any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

(B) Any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

The forfeiture provision is based on the forfeiture provisions of the federal drug laws so any money received by the illegal acts can be traced to the proceeds. That means if you received \$10,000 by the illegal act and used the money to buy a car, the car is also subject to forfeiture.

The act requires businesses that use email to contact recipients to provide an

TAKING Activewear Performance to another level



Sewfree[®] Adhesive Films Seam Tape

- Bonds almost any combination of fabrics
- Eliminates stitching
- Truly waterproof, permanent bonds
- Seamless, sleek garment design
- Great wash resistance, extends garment life
- Weight reduction & performance improvement

THE DESIGN
possibilities
are endless

Corporate Headquarters

One Bemis Way
Shirley, MA 01464 U.S.A.
Tel: 1-800-543-1324
Fax: 1-978-425-2278
email: info@bemisworldwide.com

Outside the continental U.S.

Tel: 1-978-425-6761

www.bemisworldwide.com



BEMIS



www.ispo.com



together
we are outdoor_ispo



outdoor  05 ispo 3-5 july 05