The CAN-SPAM Act and Its Applicability Today

by Kyle St. James

I. What is CAN-SPAM and why should I care?

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 sets out requirements for sending commercial/advertising electronic messages and is enforced by the Federal Trade Commission (FTC).[1] The purpose of the Act is to restrict the number of unsolicited and unwanted emails consumers receive from companies that are advertising products or services. Even a single violation of the CAN-SPAM Act may result in hefty financial penalties.

What messages are covered?

The CAN-SPAM Act regulates "commercial electronic mail messages," defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."[2] The Act applies to electronic mail and other electronic messages, including social media. Although CAN-SPAM does not regulate the *content* of emails whose primary purpose is to facilitate an already agreed-upon transaction or to update a customer about an ongoing transaction (otherwise known as "transactional" emails), the Act requires that transactional emails recite truthful sender identification. [3] Without violating the ACT, transactional emails may also include content pertaining to warranties or recalls, account balances, memberships or subscriptions, or provides employment relationship information.[4]

To determine whether an email is covered by the CAN-SPAM Act, look to the content of the email – does the email include advertising content, transactional content or a combination? The Act distinguishes between the following situations:

(1) if the email contains only advertising content, it is covered by the CAN-SPAM Act;

(2) if the email includes both advertising and transactional content, the email has a commercial primary purpose if: (i) the subject line would be interpreted as an email that includes advertising content, or (ii) a substantial part of the transactional content does not appear at the beginning of the email;

(3) if the email includes both advertising content and content that is not transactional in nature, the email has a commercial primary purpose if: (i) a recipient reasonably interpreting the subject line of the email would likely conclude that the email contains an advertisement, or (ii) a recipient reasonably interpreting the body of the email would likely conclude that the primary purpose of the message is advertising; and

(4) an email that contains only transactional content is not a commercial email and is not regulated by the CAN-SPAM Act beyond requiring truthful routing information.[5]

Because the line that distinguishes between commercial emails and transactional emails is often unclear, we recommend ensuring every email you send complies with the CAN-SPAM Act.

Why should I care about the requirements of CAN-SPAM?

The CAN-SPAM Act affects nearly every business. If you – as an individual, business entity or non-profit association – send commercial emails, you must abide by the Act's requirements. A single violation of the Act may result in a monetary penalty of up to $16,000.[6] Recognizing that advertising emails are typically sent to a large mailing list, violations can get very expensive because each email that does not meet the Act's requirements is considered a violation.[7]

II. General Overview of CAN-SPAM Requirements

The CAN-SPAM Act can be broken down into a list of do's and don'ts. Abiding by the following list will help you avoid violating the Act.

Do's

1. **Do identify the email as an advertisement or a solicitation**. The law gives you a lot of leeway on how to do this, but you must disclose clearly and conspicuously that your email is an advertisement.

2. **Do include your physical address in the email**. Your email must include your valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've registered with a commercial mail receiving agency established under Postal Service regulations.

3. **Do include an opt-out mechanism in the email**. Your email must include a clear and conspicuous explanation of how the recipient can opt out of getting email from you in the future. Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. Give a return email address or

another easy Internet-based way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt out of certain types of emails, but you must include the option to stop all commercial emails from you. Make sure your spam filter doesn't block these opt-out requests.

4. **Do honor opt-out requests within 10 days**. Any opt-out mechanism you offer must enable processing of opt-out requests for at least 30 days after you send your email. You must honor a recipient's opt-out request within 10 business days. You cannot charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once a customer has told you no more emails are wanted from you, you cannot sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the Act. To comply with the opt-out requirements of the Act, we recommend establishing email accounts with various email providers to test your opt-out mechanism. Specifically, testing of the opt-out mechanism should be performed periodically to ensure that opt-out requests are honored within 10 days, the opt-out mechanism is enabled for at least 30 days after the email is sent and the email from which the opt-out request was received is not repopulated onto your mailing list.

5. **Do review emails sent on your behalf**. The law makes clear that even if you hire another company to handle your email marketing, you cannot contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the email and the company that actually sends the email may be held legally responsible.

Don'ts

1. **Don't use false or misleading header information**. Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the email.

2. **Don't use deceptive subject lines**. The subject line must accurately reflect the content of the email.

In addition to reviewing emails sent on your behalf, be careful with emails you send that request the recipient to forward to a friend. You, as the initial sender, are liable for CAN-SPAM compliance for the forwarded email if you offered the initial recipient a reward or benefit for forwarding to a friend. For this reason, many emails that include forward to a friend language raise a violation under the CAN-SPAM Act; we recommend you seek guidance from counsel before utilizing such language.

III. Opt-out mechanisms are required, what about opt-in?

a. Commercial electronic mail messages under the CAN-SPAM Act

As discussed above, the CAN-SPAM Act covers "commercial electronic mail messages," and requires that commercial emails provide an opt-out mechanism. The Act is silent, however, on requiring a recipient to give consent (e.g. opt-in) prior to receiving commercial emails. Thus, the CAN-SPAM Act does not require that recipients opt-in.

In that emails are often and easily transmitted across national borders, you should be aware of requirements in other jurisdictions, such as the European Union (EU) and Canada. In contrast to the US, the EU Opt-In Directive explicitly requires that consumers receiving electronic communications give consent prior to receiving direct marketing emails.[8] In the EU, the exchange of contact information in a business relationship qualifies as consent. Similarly, Canada's Anti-Spam Legislation (CASL) requires that consumers receiving emails have previously given consent.[9] Canada has extremely hefty financial penalties with each violation of CASL potentially costing between one million and ten million dollars.[10] Like the US, the EU and Canada also require that all commercial emails sent to consumers include an opt out mechanism.[11]

IV. Based on the CAN-SPAM Act's lack of an opt-in requirement, is it safe to buy lists of email addresses?

Although not as commonplace today, buying lists of email addresses still occurs. Purchasing a list of email addresses presents the following question – will sending a commercial email to any of the email addresses included in the purchased list result in a violation of the CAN-SPAM Act?

As discussed above, if the owner of an email address opts out of receiving your commercial emails, you cannot send a commercial email to the email address within 30 days. Blindly sending commercial emails to a purchased list may result in sending a commercial email to someone that has opted out of your emails within the past 30 days resulting in a CAN-SPAM violation. Therefore, it is not wise to purchase a list of email addresses and blindly send commercial emails to that list.

---

[1] *See* 16 C.F.R. § 316
[2] *See* 16 C.F.R. § 316
[3] *See* https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business
[4] *See* https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business
[5] *See* 16 C.F.R. § 316.3

[6] *See* https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

[7] In 2008, the FTC brought charges against an online advertiser, the press release of the settlement stating, "Online advertiser ValueClick, Inc., will pay a record $2.9 million to settle Federal Trade Commission charges that its advertising claims and e-mails were deceptive and violated federal law. The agency also charged that ValueClick and its subsidiaries, Hi-Speed Media and E-Babylon failed to secure consumers' sensitive financial information, despite their claims to do so."

[8] *See* EU directive 2002_58_ec - https://www.privacycommission.be/sites/privacycommission/files/documents/directive_2002_58_ec.pdf

[9] *See* CASL - http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html#q6

[10] *See* CASL - http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html#q6

[11] *See* https://www.privacycommission.be/sites/privacycommission/files/documents/directive_2002_58_ec.pdf and http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html#q6

Kyle St. James
(714) 338-1805
kstjames@rutan.com

To see related articles, please click here.