FCC GIVES TEETH TO THE CAN-SPAM ACT OF 2003

NEW RULES STRICTLY LIMIT COMMERCIAL EMAIL TO CELL PHONES

EDWIN N. LAVERGNE*

New rules adopted by the Federal Communications Commission ("FCC") significantly up the ante in the federal government's effort to curb spam.[1] The new rules are intended to be a preemptive strike to prevent cellular phones and other wireless devices from being deluged with unwanted commercial advertisements.[2] The rules prohibit companies from sending commercial messages, including email and text messages, to any address associated with a subscription to a wireless service unless the individual to whom the message is sent has given the sender express prior authorization to receive the message. Stated differently, the recipient must "opt-in" to receive such messages. Opt-out links, which are included in most commercial email, are insufficient to comply with the FCC's rules. Civil penalties of up to $11,000 per violation may be imposed on violators.[3]

---

* Edwin N. Lavergne is a principal in the Washington, D.C. office of Fish & Richardson P.C. He provides business, regulatory, and transactional advice to clients concerning wireless telecommunications services, telephone and Internet services, telemarketing, advertising, marketing and promotion law. Robert A. Silverman, an associate at Fish & Richardson P.C., provided substantial assistance in researching and drafting this article.

1. Controlling the Assault of the Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003), *codified at* 15 U.S.C. § 7701-7713, 18 U.S.C. § 1037 and 28 U.S.C. § 994 [*hereinafter* "CAN-SPAM Act"]. *See also In the Matter of Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, Order, CG Docket No. 04-53, FCC 04-194 (Aug. 12, 2004), 69 Fed. Reg. 55765 (September 16, 2004) [*hereinafter* "FCC CAN-SPAM Order"].

2. The new rules adopted pursuant to the FCC CAN-SPAM Order, codified at 47 C.F.R. § 64.3100, are sometimes referred to in this article as the "wireless spam rules."

3. 15 U.S.C. § 45(m)(1)(A); Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461; 16 C.F.R. § 1.98. Violations of the CAN-SPAM Act are treated as though they were violations of an FTC Trade Regulation Rule promulgated under Section 18(a)(1)(B) of the FTC Act, 15 U.S.C.§ 57a(a)(1)(B). *See also* 15 U.S.C. § 7706(a).

Most businesses need to take at least three steps to ensure compliance with the rules. First, internal procedures must be put into place to prevent commercial messages from being sent to wireless domains without proper authorization from the recipient. Second, privacy policies should be amended to reflect compliance with the FCC's requirements. Finally, agreements with affiliates and third party marketing partners may need to be amended to ensure that they are consistent with the FCC's rules.

This article discusses the basis and underpinning of the new rules, describes how existing business practices must change to comply with the rules, and considers challenges ahead in light of similar legislative and regulatory attempts to control commercial solicitations by telephone and facsimile.

I.
BASIS AND UNDERPINNINGS OF NEW RULES

The Problem with Spam

"Spam," the slang term for unsolicited commercial email, has become so ubiquitous it barely needs explanation. The official website of Hormel Food Corporation's SPAM® brand luncheon meat devotes an entire page to distinguishing its famous trademark, which has existed since 1937, from the Internet term, which was coined in recent years.[4]

Two years ago, Congress estimated that spam accounted for over half of all email traffic, and that the volume of spam was on the rise.[5] Congress found that spam was costly, inconvenient, and often fraudulent or deceptive.[6] It was on the basis of these and other findings that Congress passed the CAN-SPAM Act. Both the FCC and the Federal Trade Commission

4. *See Spam and the Internet, at* http://www.spam.com/ci/ci_in.htm (last visited Apr. 13, 2005) (indicating that the "[u]se of the term 'spam' was adopted as a result of the Monty Python skit in which [the] SPAM meat product was featured. In this skit, a group of Vikings sang a chorus of "spam, spam, spam . . . " in an increasing crescendo, drowning out other conversation. Hence, the analogy applied because [unsolicited commercial email] was drowning out normal discourse on the Internet."). *See also* CAN-SPAM Act, § 2(a), 15 U.S.C. § 7701(a)(2).

5. CAN-SPAM Act, § 2(a), 15 U.S.C. § 7701(a)(2).

6. *Id.*

("FTC") were directed to promulgate regulations implementing the Act.[7]

The Act does not prohibit the transmission of bulk commercial email messages. However, it attempts to restrict such messages by (1) establishing standards for compliant commercial email (*e.g.*, through identity disclosure and opt-out requirements);[8] (2) preempting state spam laws,[9] thereby providing uniform, national standards; and (3) adopting civil and criminal penalties for fraudulent and misleading practices.[10]

The Growing Problem with Mobile Spam

In adopting the Act, Congress was keenly aware of the growing threat of unsolicited commercial messages being sent to mobile wireless devices.[11] Such messages are widely considered to be far more intrusive and costly to consumers than other forms of spam. One industry insider observed that with "mobile spam, consumers have to pay for the delivery of annoying, unwanted messages to their personal phone. Even worse, some of the spammers will try to trick you into making an expensive call or will attempt to change the device settings on your own phone."[12]

---

7. *Id.* §§ 13(a), 14(b), 15 U.S.C. §§ 7711(a), 7712(b).

8. *Id.* §§ 4-6, 15 U.S.C. at §§ 7703-7705.

9. *Id.* § 8(b), 15 U.S.C. § 7707(b).

10. *Id.* §§ 4(a), 5(d)(5), 7(d), 15 U.S.C. §§ 7703(a), 7704(d)(5), 7706(d).

11. Before Congress passed the CAN-SPAM Act, Rep. Rush D. Holt (D-NJ) commented in the proceedings and debates that he was "particularly pleased that [the CAN-SPAM Act] includes a provision intended to combat a related problem that has gotten out of hand in some countries and is growing ever worse in the United States—spam sent to wireless phones through text messaging. As many of my colleagues know, I introduced legislation intended to draw attention to this issue—the Wireless Telephone Spam Protection Act. This bill was intended to launch what could be called a preemptive attack against wireless spam before it spins out of control in the United States. Congress too often acts once the fire is already lit. This time, we can put the fire out before it gets out of control." 149 Cong. Rec. H12186-02 (daily ed. Nov. 21, 2003) (statement of Rep. Holt).

12. *Mobile Spam Volume Doubles to Forty-Three Percent*, Wireless Services Corporation Press Release (February 28, 2005) *available at* http://www.wirelesscorp.com/pressrelease_2_28_05_spam.htm. The quoted language is attributed to Rich Begert, President and CEO of Wireless Services Corporation, which provides value-added services to wireless carriers in North America. *Id.*

Rep. Edward J. Markey (D-Mass.), ranking member of the House Subcommittee on Telecommunications and Internet, led the successful effort to include a mobile spam amendment to the CAN-SPAM Act. In so doing, he conjured up the image of consumers being bombarded by hundreds of "unwanted rings on your phone, your cell phone, this zone of privacy which we all have as these marketers are calling into your cell phone all day long. . . . Wireless spam is even more intrusive [than spam to a desktop computer] because spam to wireless phones is the kind of spam that follows you wherever you go and according to U.S. wireless carriers, is already on the rise."[13]

Mobile spam already has plagued the international community. Rep. Markey described the situation in Europe, Japan and South Korea as a "full scale epidemic."[14] By way of example, a global study conducted in late 2004, found that over 80% of mobile phone users surveyed received unsolicited messages on their wireless devices.[15] The study also reported that both consumers and mobile operators expect mobile spam to become more of a problem in the future.[16] Eighty three percent of telecommunications industry respondents surveyed said they perceive mobile spam to be a critical issue today or within the next one to two years.[17]

As the next generation of wireless mobile devices are deployed in the United States, wireless Internet access and Short Message Service ("SMS") or "text messaging" will become increasingly commonplace. According to the Pew Internet and American Life Project, one quarter of American adults who have cellular phones have used the devices' SMS features, and of these SMS users, 63% were between 18 and 27, indicating a growing trend in mobile messaging and a growing

13. 149 Cong. Rec. H12186-02 (daily ed. Nov. 21, 2003) (statement of Rep. Markey).

14. *Id.*

15. *First Empirical Global Spam Study Indicates More Than 80 Percent of Mobile Phone Users Receive Spam*, Press Release, University of St. Gallen, Switzerland and BMD Wireless (February 9, 2005), *available at* http://mobilespam.org. The study was conducted in late 2004, and includes data from Germany, Switzerland, Austria, Canada, the United States, Singapore, China and Saudi Arabia. *Id.*

16. *Id.*

17. *Id.*

exposure to mobile spam.[18] More notably, 28% of people who sent text messages also reported receiving mobile spam.[19]

International Measures to Combat Mobile Spam

International efforts to curb mobile spam have had varying levels of success. In April 2002, Japan passed two pieces of legislation—The Law for Appropriate Transmission of Specified Emails (Law No. 26 of 2002)[20] and an Amendment to the 1976 Specific Commercial Transactions Law (Law No. 28 of 2002)[21]—that served essentially as a stopgap to the rapid growth of mobile spam by establishing, among other things, various opt-out and sender identity disclosure requirements and imposing civil and criminal penalties.[22] Following the passage of these legislative measures, however, an apparent loophole allowed for a sharp increase in mobile-to-mobile spam via SMS. As a result, mobile phone carriers took matters into their own hands by implementing strengthened service-based measures (*e.g.*, suspension of services, email traffic quotas, etc.), and within a year, mobile-to-mobile spam levels subsided.[23]

In Europe, where mobile spam is less problematic than in Japan, stricter measures have been taken. In July 2002, the European Parliament and the Council of the European Union adopted for the European Community Member States a "directive concerning the processing of personal data and the protection of privacy in the electronic communications sec-

18. Pew Internet, *Pew Internet & American Life Project Press Release* (March 14, 2005), *available at* http://www.pewinternet.org/press.asp ("34 million American adults send text messages on their cell phones").

19. *Id.*

20. *See* Evan Cramer, The *Future of Wireless Spam*, 2002 DUKE L. & TECH. REV. 0021 (2002), *available at* http://www.law.duke.edu/journals/dltr/articles/PDF/2002DLTR0021.pdf *citing* Japan Computer Industry Scan, *Law Enacted to Regulate Unsolicited E-mail Ads*, at LEXIS, IAC Japan (April 15, 2002).

21. *See id.*, citing Yomiuri Shimbun, DAILY YOMIURI (July 1, 2002), *available at* 2002 WL 19074087.

22. *See* Cramer, *supra* note 22.

23. MINISTRY OF PUBLIC MANAGEMENT, HOME AFFAIRS, POSTS AND TELECOMMUNICATIONS (MPHPT), JAPAN, ANTI-SPAM ACTIVITIES IN JAPAN 2-3 (March 2004) (on file with New York University Journal of Law and Business).

tor"[24] (the "Directive"). Unlike Japan's initiatives, which provided only an opt-out mechanism to control mobile spam, the Directive established an opt-in requirement, whereby "prior explicit consent of the recipients" must be obtained before "unsolicited communications for direct marketing" may be sent to mobile phone devices.[25] In addition, the Directive regulates messages that use "automated calling machines, telefaxes, and e-mails, including SMS messages,"[26] thereby closing the loophole on mobile-to-mobile spam.[27]

II.
ANALYSIS OF WIRELESS SPAM RULES

Definitions and Exemptions

The FCC's wireless spam rules are similar to those adopted in Europe in that they require recipients to "opt-in" to receive commercial messages on cell phones and other wireless devices. More precisely, the wireless spam rules provide that in the absence of the express prior authorization of the recipient, a Mobile Service Commercial Message ("MSCM") may not be sent to any email address that includes a reference to an Internet domain name found on the FCC's official list of wireless domain names.[28] The list was released to the public in February 2005, and now is updated on a regular basis.[29]

An MSCM is defined as a "commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service. . . . in connection with that service."[30] The term "'commercial electronic mail message' encompasses 'any electronic mail mes-

24. Directive 2002/58/EC of the European Parliament and of the Council, OFFICIAL J. OF EUR. CMTIES. L 201/37 (July 7, 2002).

25. *Id.* ¶ 40

26. *Id.*

27. *Id.* art. 13 ¶ 1.

28. The FCC's wireless domain name list was created by requiring all commercial mobile radio service ("CMRS") providers to provide the agency with all domain names used to offer subscribers messaging for mobile devices. FCC CAN-SPAM Order ¶ 29, at 55,768. The FCC's list can be downloaded at http://www.fcc.gov/cgb/policy/DomainNameDownload.html. CMRS providers are sometimes referred to in this article as "wireless carriers" or "carriers."

29. *See* FCC CAN-SPAM Order ¶ 30, at 55,768.

30. CAN-SPAM Act, § 14(d), 15 U.S.C. § 7712(d).

sage the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet Web site operated for a commercial purpose).'"[31] The definition of an MSCM includes any commercial electronic mail message as long as the address to which it is sent or transmitted includes a reference to the Internet and is for a wireless device. This holds true regardless of the format of the message.[32] Therefore, messages sent using Internet-to-phone SMS technology are among messages covered when they include an Internet reference in the address to which the message is sent or delivered.[33]

Consistent with the general framework of the CAN-SPAM Act, the FCC's rules exempt a broad array of "transactional or relationship messages" whose primary purpose is non-commercial. Examples of transactional or relationship messages include warranty information, product recall notices, health and safety information, and customer service information.[34]

---

31. Definitions and Implementation Under the CAN-SPAM Act, 70 Fed. Reg. 3110, 3111 (January 19, 2005) [*hereinafter* "FTC Final Rule"]. The FTC has delineated certain categories and criteria to determine a message's "primary purpose" so as to know what types of messages should be considered "commercial." *Id.* at 3127-28 (to be codified at 16 C.F.R. § 316.3).

32. *See* FCC CAN-SPAM Order ¶ 17, at 55,767.

33. *See* FCC CAN-SPAM Order ¶ 16 and n. 74, at 55,767. Technologies that use other types of addresses or numbers to deliver messages to wireless devices are not covered by the FCC's rules adopted pursuant to the CAN-SPAM Act. For example, phone-to-phone SMS messages are not covered because such messages do not have references to Internet domains. However, the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 [*hereinafter* "TCPA"] prohibits using autodialers to make calls to wireless phone numbers, including phone-to-phone SMS messages and voice calls. *See* TCPA, 47 C.F.R. § 64.1200(a)(1)(iii). *See also In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, CG Docket No. 02-278, FCC 03-153 at ¶ 165 (July 3, 2003), 68 Fed. Reg. 44,144 (July 25, 2003) [*hereinafter* "FCC TCPA Order"].

34. "Transactional or relationship messages" are defined as messages the primary purpose of which is (1) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; (2) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient; (3) to provide (i) notification concerning a change in the terms or features of; (ii) notification of a change in the recipient's standing or status with respect to; or (iii) at regular periodic intervals, account balance information or other type of account statement with respect to a subscription, membership, account, loan, or

The FCC's Wireless Domain List

In order to comply with the FCC's rules, businesses that market via email need to download the list of wireless domain names from the FCC's website. Then they must cross-check their internal list of email addresses against the FCC's list. If a domain on the FCC's list matches a domain on the business's list, the business must stop sending commercial email to the affected address until it has obtained express authorization from the recipient. By way of example, the FCC list includes the domain name *cingularme.com.* This means that a company is prohibited from sending an MSCM to any address including that domain name (*e.g.,* John.Doe@cingularme.com) absent the recipient's express prior authorization. Opt-out procedures alone are insufficient; the recipient must expressly opt-in to receive such messages.

The FCC has established a "safe harbor" defense to liability in situations where an MSCM is sent to a domain name that was not on the FCC's list more than 30 days before the offending message was sent.[35] Thus, although the FCC's wireless domain name list is expected to remain relatively static, businesses should check the list at least once every 30 days to take advantage of this safe harbor.[36]

Methods of Obtaining Express Consent

Under the FCC's rules, express consent may be obtained by oral or written means, including electronic methods.[37] However, whether given orally or in writing, prior authoriza-

---

comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender; (4) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or (5) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender. 15 U.S.C. § 7702(17)(A) (2003).

35. FCC CAN-SPAM Order ¶ 32, at 55,769. *See also* 47 C.F.R. § 64.3100(a)(4).

36. *Id.* This safe harbor defense does not protect against willful violations, *i.e.,* if the sender has actual knowledge that the email address is otherwise protected.

37. FCC CAN-SPAM Order ¶ 43, at 55,770. *See also* 47 C.F.R. § 64.3100(d).

tion must be express, must be given prior to sending an MSCM, and must include the email address to which the MSCM may be sent.[38]

Significantly, businesses may not ask for express prior authorization by sending an email to an address which has been matched to the FCC's wireless domain name list. This is because the FCC requires that a consumer not bear any additional cost to receive a request for authorization, and must be able to reply to such a request without incurring any additional cost.[39] As a result, express consent must be obtained by other means such as a postcard, a telephone call, or though a web site.

In cases where an authorization is given through a website, the website must allow the subscriber to input the specific email address to which MSCMs may be sent.[40] The authorization must also include an affirmative action on the part of the subscriber, such as checking an "I Accept" button, accompanied by appropriate disclosures.[41] If authorization is obtained in paper form, it must include the subscriber's signature and the email address to which MSCMs may be sent.[42] If authorization is obtained electronically, it must include an electronic or digital form of signature recognized as valid under federal or state law.[43] If authorization is obtained orally, businesses are expected to take reasonable steps to ensure that such authorization can be verified.[44] This might include, for example, tape recording a telephone conversation with a consumer.[45]

---

38. FCC CAN-SPAM Order. ¶ 45, at 55,770. *See also* 47 C.F.R. § 64.3100(d).

39. FCC CAN-SPAM Order ¶ 45, at 55,770. *See also* 47 C.F.R. § 64.3100(d).

40. FCC CAN-SPAM Order ¶ 46, at 55,771. *See also* 47 C.F.R. § 64.3100(d)(2).

41. FCC CAN-SPAM Order ¶ 46, at 55,771. Authorization may not be obtained using "negative options" where authorization is presumed by the sender unless advised otherwise. *See id.*

42. *Id.* ¶ 43, at 55,770. *See also* 47 C.F.R. § 64.3100(d)(1).

43. FCC CAN-SPAM Order ¶ 43 n. 129, at 55,770 . *See also* 47 C.F.R. § 64.3100(d)(1); 15 U.S.C. § 7001 (E-Sign Act).

44. FCC CAN-SPAM Order ¶ 43, at 55,770.

45. *Id.* ¶ 44 n. 130, at 55,770.

Required Consumer Disclosures

At the time express authorization is obtained, three disclosures must be made to the consumer. First, the consumer must affirmatively agree to receive MSCMs from a particular sender. This disclosure must include the electronic mail address to which MSCMs can be sent. It also must state clearly the identity of the business, individual, or other entity that will be sending the messages (or the person or entity whose product or service is advertised or promoted in the MSCMs if different from the sender).[46] Second, the consumer must be told that he or she may be charged by their wireless service provider in connection with the receipt of such messages.[47] Third, the consumer must be told that his or her authorization to receive MSCMs may be revoked at any time.[48]

All notices containing the required disclosures must be clearly legible, use sufficiently large type or, if audio, be of sufficiently loud volume, and be placed so as to be readily apparent to a wireless subscriber. In addition, such disclosures must be presented separately from any other authorizations in the document or oral presentation. If any portion of the notice is translated into another language, then all portions of the notice must be translated into the same language.[49]

Burden of Proof and Documentation

Careful recordkeeping is warranted because if there is a dispute as to whether appropriate consent was obtained from a consumer, the burden of proof rests squarely on the sender. In this regard, the FCC has emphasized that senders must be prepared to provide "clear and convincing" evidence of express prior authorization.[50]

---

46. FCC CAN-SPAM Order ¶ 50, at 55,771. *See also* 47 C.F.R. § 64.3100(c)(5)(i).

47. FCC CAN-SPAM Order ¶ 50, at 55,771. *See also* 47 C.F.R. § 64.3100(c)(5)(ii).

48. FCC CAN-SPAM Order ¶ 50, at 55,771. *See also* 47 C.F.R. § 64.3100(c)(5)(iii).

49. FCC CAN-SPAM Order ¶ 50, at 55,771. *See also* 47 C.F.R. § 64.3100(c)(6).

50. FCC CAN-SPAM Order ¶ 52, at 55,771.

The FCC suggests that businesses document promptly that they received authorization from a consumer.[51] For example, such documentation might include an affirmative message from a consumer sent in response to a confirmatory message from a business stating that the consumer had previously asked to receive MSCMs from that business.[52] The FCC cautions that "by itself, a message from the sender purporting to be a confirmatory message does not show that prior express authorization has been given."[53]

Third Parties and Affiliates

Authorization provided by a consumer to a particular company will not entitle that company to send MSCMs on behalf of third parties, including on behalf of affiliated entities and marketing partners.[54] Likewise, authorization to one company will not permit affiliated entities and marketing partners to send their own MSCMs to the consumer absent specific authorization from the consumer.[55] Accordingly, businesses should consider whether they need to amend agreements with affiliates and third party marketing partners to ensure that such affiliates and marketing partners conduct business in accordance with the FCC's new rules.

Content of MSCMs

Businesses that send MSCMs must abide by several FCC requirements. First, such messages must include a functioning return email address or other Internet-based mechanism that is clearly and conspicuously displayed for the purpose of receiving requests to cease the initiating of MSCMs,[56] and that does not require the consumer to view or hear further commercial content other than institutional identification (*i.e.*, an email or other Internet-based opt-out mechanism must be offered) .[57]

---

51. *Id.* ¶ 44, at 55,770.
52. *Id.*
53. *Id.* ¶ 44 n. 130, at 55,770.
54. *Id.* ¶ 49, at 55,771.
55. *Id.*
56. CAN-SPAM Act § 5(a)(3). *See also* 15 U.S.C. § 7704(a)(3); FCC CAN-SPAM Order ¶ 55, at 55,771; 47 C.F.R. § 64.3100(4)(b)(2).
57. FCC CAN-SPAM Order ¶ 58 n. 162, at 55,772.

Second, in cases where authorization to receive MSCMs is granted electronically, a functioning option and clear and conspicuous instructions to opt-out of receiving further messages by the *same electronic means* that was used to obtain authorization in the first place must be provided to the consumer.[58] For example, if a consumer grants authorization by means of a short code, such as 12345,[59] the consumer must also be provided with a way to send a short code to the sender to reject future MSCMs from that sender.[60]

Third, senders must ensure that the use of at least one of the opt-out options made available to the consumer does not result in additional charges to the consumer.[61] Using the above example, at least one of the opt-out mechanisms described (*i.e.*, a return e-mail address or other Internet-based mechanism, or a short code) must be free to the consumer.

Fourth, for a period of no less than 30 days after the transmission of an MSCM, the sender must remain capable of receiving messages or communications made to the electronic mail address, other Internet-based mechanism or, if applicable, other electronic means provided by the sender.[62] If the sender is notified by the consumer that he or she does not wish to receive MSCMs, the sender must cease sending such messages within 10 days of receipt of such request.[63]

Finally, businesses must ensure that they are properly identified in MSCMs sent to consumers who have opted-in to receive such messages. Specifically, the FCC's rules require that a company with express prior authorization from a recipient must identify itself in a form that will allow the recipient to reasonably determine that the sender is the company authorized to send MSCMs.[64] For example, in obtaining authoriza-

58. *Id.* ¶ 56, at 55,772.

59. "A short code is a number to which an SMS or text message can be sent. A short code is fewer digits than a 10-digit telephone number." COMMON SHORT CODE ADMINISTRATION, FAQS: THE BASICS OF CSCS, *available at* http://www.usshortcodes.com/content/csc_faq_csc.html (last visited Apr. 13, 2005).

60. FCC CAN-SPAM Order ¶ 57, at 55,772.

61. *See* 47 C.F.R. § 64.3100(b)(4).

62. FCC CAN-SPAM Order ¶ 59, at 55,772.

63. The FCC has followed the FTC's interpretation of "10 days" to mean 10 business days. *See* FCC CAN-SPAM Order ¶ 48 n. 139, at 55,771.

64. *See id.* ¶ 49, at 55,771.

tion from a consumer, it is not sufficient to state simply that a company will be sending messages from its "partners and subsidiaries."[65]

Applicability of Rules to Non-Profit Entities

Following adoption of the CAN-SPAM Act, there was substantial discussion as to the applicability of the Act to non-profit entities.[66] The FTC, which has overlapping jurisdiction with the FCC in regulating spam, ultimately found that the CAN-SPAM Act is applicable to non-profit entities.[67] However, as a practical matter, many emails sent by non-profits are likely to fall outside the scope of the Act or within the "transactional or relationship message" exemption to the Act.[68]

For example, emails soliciting charitable contributions would fall outside of the CAN-SPAM Act because such solicitations do not promote a commercial product or service.[69] Other types of messages may or may not fall within the purview

65. *See id.* ¶ 57 n. 147, at 55,771.

66. *FTC Final Rule, supra* note 33, at 3111-12. The American Association for Marriage and Family Therapy ("AAMFT") suggested that "email transmitted by a . . . nonprofit organization primarily related to one or more of the organization's duly authorized tax exempt nonprofit purposes . . . be specifically exempt from regulation under the Act." Letter from David Bergman, Director, Legal and Government Affairs, AAMFT, to the FTC (August 18, 2004), *available at* http://www.ftc.gov/os/comments/canspam2/OL-100030.htm. The National Automobile Dealers Association ("NADA") went further suggesting not only that email from trade associations be excluded "based on the non-profit purpose of these organizations," but that emails from for-profit subsidiaries of nonprofit organizations "that are consistent with the organization's purpose, should be similarly excluded . . . ." Letter from Smith Koppuzka, Staff Attorney, NADA, to the FTC (September 13, 2004), *available at* http://www.ftc.gov/os/comments/canspam2/04-18565-29507-ATT-1.pdf. *See also FTC Final Rule, supra* note 33, at 3112.

67. The FTC concluded, for example, that "a message from a nonprofit could meet the definition of 'commercial electronic mail message' (*e.g.*, an email message sent by a nonprofit hospital offering medical screening in exchange for a fee.)." *FTC Final Rule, supra* note 33, at 3112. At the same time, the FTC observed that "it is possible—or even likely—that messages between a nonprofit and its members could constitute 'transactional or relationship messages' under [S]ection 7702(17)(A)(v) [of the CAN-SPAM Act]." *Id.*

68. *See infra* note 71 and accompanying text.

69. FTC Final Rule, *supra* note 33, at 3125 n. 165 *citing* 149 Con. Rec. H 12186 (daily ed. Nov. 21, 2003) (statement of Rep. Sensenbrenner) (the Act "concerns only commercial and sexually explicit email and is not intended

of the Act depending on the "primary purpose" of such messages. In this regard, the FTC has stated that messages from a nonprofit to its members "will only be considered 'commercial electronic mail messages,' and thus subject to greater regulation than transactional or relationship messages, if (1) a recipient reasonably interpreting the subject line of the message would likely conclude that the message advertises or promotes a commercial product or service; or (2) the transactional or relationship content does not appear, in whole or substantial part, at the beginning of the body of the message."[70] Nonetheless, if the primary purpose of a message sent by a nonprofit entity is commercial, the non-profit entity is subject to the same requirements that are applicable to other senders of MSCMs.[71]

III.
CHALLENGES AHEAD

It remains to be seen whether the FCC's rules adopted pursuant to the CAN-SPAM Act will be successful in curbing the proliferation of mobile spam in the United States. However, what *is* clear is that many businesses will find compliance with the new rules to be burdensome and costly. Consider, for example, that a business which only has an email address for a customer is prohibited from further email marketing to that customer if it turns out that the customer's email address includes a domain on the FCC's wireless domain name list. Even more troubling, the business cannot contact the customer by email for the purpose of obtaining the necessary opt-in consent.[72] Other means of obtaining opt-in consent must be found.

In this respect, the FCC's wireless spam rules are significantly more stringent than the federal government's Do-Not-Call ("DNC") rules, which were the subject of significant de-

---

to intrude on the burgeoning use of email to communicate for political, news, personal, and charitable purposes").

70. *FTC Final Rule, supra* note 33, at 3112 n.29.

71. *In the Matter of Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, CG Docket No. 04-53, DA 05-692, ¶ 9 and n. 22 (March 25, 2005).

72. *See supra* footnote 37 and accompanying text.

bate.[73] The DNC rules require businesses periodically to download a list of telephone numbers provided by consumers who choose not to receive sales-related calls from telemarketers.[74] Businesses must avoid making sales-related calls to telephone numbers included on the DNC list.[75] But, the DNC rules include an exemption which permits calls to persons with whom the caller has an "established business relationship."[76] This is an important exemption which balances the legitimate desire of businesses to stay in touch their customers against the equally legitimate desire of consumers to avoid unwanted intrusions into their privacy.

By contrast, there is no "established business relationship" exemption in the FCC's wireless spam rules. The wireless spam rules are more analogous to rules prohibiting marketers from sending unsolicited fax advertisements.[77] In July 2003, the FCC adopted a rule which reversed an earlier interpreta-

---

73. *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, 68 Fed. Reg. 44144 (July 25, 2003) *codified at* 27 C.F.R. §§ 64, 68 [*hereinafter* "FCC TCPA Rules"], and *Telemarketing Sales Rule*, 68 Fed. Reg. 4580 (January 20, 2003) *codified at* 16 C.F.R. 310 [*hereinafter* "FTC TCPA Rules"]. Numerous legal challenges followed the implementation of the DNC rules. *See, e.g.*, *'Do not call' list unplugged*, CNN MONEY (September 24, 2003), *available at* http://money.cnn.com/2003/09/24/technology/ftc_donotcall; Paul Davidson, *Supreme Court lets do-not-call list stand*, USA TODAY (October 4, 2004), *available at* http://www.usatoday.com/news/washington/judicial/2004-10-04-donotcall-upheld_x.htm.

74. The term "sales-related calls" refers to calls regulated by the FCC and the FTC pursuant to the TCPA. The FTC regulates a "plan, program, or campaign which is conducted to induce the purchase of goods or services." *FTC TCPA Rules*, *supra* note 75, 68 Fed. Reg. at 4655; 16 C.F.R. § 310.2(cc). The FCC regulates calls made "for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services." 47 C.F.R. § 64.1200(g).

75. *FCC TCPA Rules*, *supra* note 75, 68 Fed. Reg. at 44145. There is an exception for calls made to persons who have given their prior express consent to receive such calls. *Id.*, 68 Fed. Reg at 44,163.

76. *Id.*, 68 Fed. Reg. at 44,148. An "established business relationship" is defined as "a relationship between a seller and a consumer based on (1) the consumer's purchase, rental, or lease of the seller's goods or services or a financial transaction between the consumer and seller, within eighteen (18) months immediately preceding the date of the telemarketing call; or (2) the consumer's inquiry or application regarding a product or service offered by the seller, within three (3) months immediately preceding the date of a telemarketing call." 16 C.F.R. § 310.2(n).

77. An "unsolicited advertisement" is defined as "any material advertising the commercial availability or quality of any property, goods, or services

tion of the law by requiring consumers to opt-in to receive unsolicited fax advertisements.[78] Industry resistance to the rule change was fierce.[79] Hundreds of associations and businesses banded together claiming that compliance with the new fax restriction would cause irreparable injury to businesses and trade associations and negatively impact the nation's economy.[80] Ultimately, the FCC bowed to industry and political pressure by delaying the effective date of the rule until June 30, 2005.[81]

Not surprisingly, pockets of resistance are already beginning to emerge in opposition to the wireless spam rules. In March 2005, the Direct Marketing Association and the E-Mail Service Provider Coalition filed a joint petition requesting a limited waiver of the rules so as to permit additional time for companies to determine (1) which individuals with whom they communicate via email have email addresses associated with domain names on the FCC's wireless domain name list, and (2) whether the existing authorizations they have on file for these individuals satisfy the requirements of the FCC's wireless spam rules.[82] The petitioners note that, in many cases, consumers have provided opt-in consent to receive commercial

---

which is transmitted to any person without that person's prior express invitation or permission." 47 U.S.C. § 227(a)(4); 47 C.F.R. § 64.1200(f)(5).

78. *See FCC TCPA Rules, supra* note 75, 68 Fed. Reg. at 44168.

79. The several hundred business and organizations of the Fax Ban Coalition, as well as other groups such as the American Bar Association, joined in an intense lobbying and publicity campaign. *See, e.g.*, Letter from Robert D. Evans, American Bar Association Governmental Affairs Office, to The Honorable Fred Upton, Chair, Subcommittee on Telecommunications and the Intent, Committee on Energy and Commerce (June 18, 2004), *available at* http://www.abanet.org/poladv/letters/108th/fcc061804.pdf. *See also* The Fax Ban Coalition, Open Letter to All Members of the House of Representatives (June 21, 2004), *available at* http://www.astanet.com/govaffairs/docs/FaxLettertoHouse062104.doc.

80. *Fax Ban Coalition Petition for Extension of Stay*, CG Docket No. 02-278 (August 10, 2004) at 6.

81. In addition to opposing the new fax restrictions at the FCC, the Fax Ban Coalition made their case on Capitol Hill. These efforts led to the passage of legislation in the U.S. House of Representatives on July 20, 2004, which would have reinstated the established business relationship exemption for facsimiles. *See* Junk Fax Prevention Act of 2004, H.R. 4600, 108th Cong. (2d Sess. 2004). Similar legislation was introduced in the Senate. *See* Junk Fax Prevention Act of 2004, S. 2603, 108th Cong. (2d Sess. 2004).

82. *See* Joint Petition for Limited Waiver, *In re* Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and

email messages from consumers, but such consents may not meet the precise opt-in requirements set forth in the FCC's wireless spam rules.[83] According to the petitioners, "the effect of strict adherence to the MSCMS rules will be to limit the sending of [commercial email messages] to millions of recipients that have not provided express prior authorization in the manner required in the rules."[84]

Commercial wireless carriers have gone even further. Cingular Wireless LLC ("Cingular"), for example, has requested that the FCC reconsider its refusal to grant a blanket exemption for wireless service carriers from the mobile spam opt-in requirement.[85] Cingular's argument is rooted in language included in the CAN-SPAM Act, which provides the FCC with discretion to exempt wireless carriers from the opt-in requirement, as long as consumers can opt-out of receiving future MSCMs.[86] Cingular asserts that the FCC's failure to adopt this exemption upset the "careful balance of provider and consumer interests that the Commission and Congress previously have adopted" by failing to fully analyze the carrier/customer relationship.[87]

Thus far, the FCC steadfastly has resisted efforts to create exceptions to the wireless spam rules. As of this writing, the FCC has not acted on the waiver request filed by the Direct Marketing Association and E-Mail Service Provider Coalition. Moreover, in rejecting earlier arguments made by wireless carriers, the Commission stated that it was persuaded that safeguarding consumers "undiluted with an exemption" for wireless providers would best serve the public interest.[88] The FCC said that MSCMs sent by wireless carriers "are not fundamentally different from those sent by other senders, other than

---

Marketing Act of 2003, CG Docket No. 04-53, at 1 (March 1, 2005) (on file with New York University Journal of Law and Business).

83. *See id.* at 6.

84. *Id.*

85. *See* Petition for Reconsideration, *In re* Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, CG Docket No. 04-53, at 1 (October 18, 2004) (on file with New York University Journal of Law and Business) [*hereinafter* "Petition for Reconsideration"].

86. *See* 15 U.S.C. § 7712(b)(3).

87. *See* Petition for Reconsideration, *supra* note 87, at 4.

88. FCC CAN-SPAM Order ¶ 70, at 55,773.

that they may be provided without additional cost to subscribers."[89] The Commission's position, no doubt, is influenced by the controversy surrounding the agency's efforts to change the facsimile advertising rule, where the Commission saw how difficult it can be to change well-settled business practices once exemptions are created.

IV.
CONCLUSION

Congress wants to protect consumers from intrusive assaults of privacy, especially with respect to mobile wireless devices. Federal agencies are working diligently to protect and serve the public through rulemaking and enforcement. In the long term, however, legislative and regulatory initiatives *alone* are not likely to be effective in stopping spam, given the borderless Internet.[90] Effective solutions will require a combination of regulatory intervention, technological innovation, and international cooperation.

Efforts at international cooperation have intensified. At the 2005 Asia-Europe Meeting Conference on eCommerce held in London,[91] member countries committed to conducting regular discussions and taking actions through policy and enforcement officials, including legislation and enforcement, raising awareness, industry self-regulation, technical solutions and partnerships between governments and the Internet community.[92] In addition, the FTC has joined forces with law enforcement officials in the United Kingdom and Australia and agreed to share information and resources to fight spam.[93] The FTC and the UK Office of Fair Trading also

89. FCC CAN-SPAM Order ¶ 70, at 55,773.

90. *See, e.g.*, Press Release, European Union, EU and Asia Unite Against 'Spam,' (Feb. 24, 2005) ("The ASEM joint statement, initiated by the European Commission, encourages all countries to set up national anti-spam strategies and then to engage in international cooperation.").

91. ASEM is a multilateral forum consisting of the 25 European Union Member States, the European Commission, and 13 Asian partner countries, including Brunei, Burma, Cambodia, China, Indonesia, Japan, Korea, Laos, Malaysia, the Philippines, Singapore, Thailand, and Vietnam.

92. *See* Press Release, European Union, *EU and Asia Unite Against 'Spam'* (Feb. 24, 2005).

93. *See* Memorandum of Understanding on Mutual Enforcement Assistance in Commercial Email Matters Among the Following Agencies of the

created the London Action Plan, a global cooperative effort of public and private sector participants designed to promote international spam enforcement and address spam-related problems.[94]

The CAN-SPAM Act is making its way in the global effort to fight spam. Domestically, the FCC has fortified the Act with strict rules to protect consumers and their wireless devices. It is becoming increasingly apparent that as more parties in the United States and abroad are affected by spam, more progressive measures will be taken to curb the problem.[95] If these efforts succeed, businesses and consumers alike may once again come to recognize SPAM® as only a luncheon meat.

United States, the United Kingdom, and Australia: The United States Federal Trade Commission, the United Kingdom's Office of Fair Trading, the United Kingdom's Information Commissioner, Her Majesty's Secretary of State for Trade and Industry in the United Kingdom, the Australian Competition and Consumer Commission, and the Australian Communications Authority, 69 Fed. Reg. 44,008 (July 23, 2004).

94. *See* Press Release, Federal Trade Commission, *International Agencies Adopt Action Plan on Spam Enforcement* (Oct. 12, 2004) *available at* http://www.ftc.gov/opa/2004/10/spamconference.htm.

95. *See, e.g.*, Press Release, Federal Trade Commission, *International Consumer Protection Group Meets in Scotland to Address Cross-Border Fraud Developments*, (Mar. 10, 2005), *available at* http://www.forbes.com/technology/2004/02/27/cx_ah_0227tentech.html ("[The International Consumer Protection and Enforcement Network] also announced the results of a February 2005 Internet sweep to identify fraudulent spam e-mail."); Arik Hesseldahl, *D-Day in the Spam War*, FORBES (Feb. 27, 2004), *available at* http://www.forbes.com/technology/2004/02/27/cx_ah_0227tentech.html ("The good news is that a lot of smart people have been thinking long and hard about fighting back with a new generation of standards and protocols that will make increasingly difficult over the coming years for spammers to ply their trade. And they have the world's richest man—Microsoft Chairman Bill Gates—on their side. Spammers may not be worried yet, but they soon should be.").