

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
)
Rules and Regulations Implementing the) CG Docket No. 04-53
CAN-SPAM Act of 2003)
)
)
_____)

SPRINT COMMENTS

Luisa Lancetti
Vice President, Wireless Regulatory Affairs
Sprint Corporation
401 9th Street, N.W., Suite 400
Washington, D.C. 20004
202-585-1923

Joseph Assenzo
General Attorney
Sprint Corporation
6450 Sprint Parkway
Overland Park, KS 66251
913-315-9141

April 30, 2004

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Rules and Regulations Implementing the)	CG Docket No. 04-53
CAN-SPAM Act of 2003)	
)	
_____)	

SPRINT COMMENTS

Sprint Corporation, on behalf of its local, long distance and wireless divisions (“Sprint”), submits these comments in response to the Commission’s March 19, 2004 Notice of Proposed Rulemaking.

As a mobile service provider offering messaging services, Sprint has a keen interest in this docket because of the impact of spam on its network and its customers. Millions of Sprint wireless customers have text messaging service. Sprint has implemented a variety of measures to prevent unwanted spam from reaching its customers, and will implement more in the future. But the battle is relentless – it is difficult and expensive to stay one step ahead of irresponsible senders.

While Sprint is very concerned about network integrity, as well as the satisfaction of its customers, Sprint cautions the Commission against ordering specific technical requirements for implementing the CAN-SPAM Act. Mobile commerce is a new, rapidly evolving space, and its growth should not be prematurely stunted. Technology, too, is rapidly evolving. The

Commission should not hamstring innovation and growth with technological requirements that are likely to soon become outdated and ineffective.

Even if the Commission were to order a specific technical requirement, it is Sprint's experience that technical requirements alone cannot do the job. No technical requirement can eliminate all spam, and carriers should not be put in the position of guaranteeing that subscribers will never receive unwanted commercial messages. Spammers, too, are innovative, and carriers and their vendors will have to continually anticipate and respond with new techniques for combating spam. The good actors will play by the rules; the bad actors will attempt to evade regulation and technology constraints. Instead of mandating a specific technical solution, the Commission should set baseline standards and definitions, allowing carriers and third-party developers to bring forward solutions that are consistent with carrier technology plans and in a way that may offer competitive advantages. The Commission must also take into account that many consumers wish to have a choice about the types of commercial messages they receive. The Commission must not overlook the need to step up enforcement, which may require coordination with the FTC to gain jurisdiction over senders of spam.

A. DEFINITION OF "MOBILE SERVICE COMMERCIAL MESSAGE"

The Commission seeks comment on its interpretation that it should only address messages sent directly to a wireless device. The plan language of the CAN-SPAM Act defines MSCMs as commercial messages that are sent "directly to a wireless device."¹ Text messaging (i.e., short message service) may occur within a provider's IP network, and across providers' IP networks, wireless device-to-wireless device. But it is not this device-to-device messaging that

¹ 15 U.S.C. § 7712(d).

is of concern. Moreover, device-to-device messaging does not involve the use of a domain name, and therefore does not meet the statutory definition of an electronic message.²

Text messages, however, may also be sent from the Internet at large – for instance, from a desktop user’s email platform – to wireless handsets. A person wishing to send a text message to a Sprint PCS customer may either send a message by logging on to sprintpcs.com, or may send a text message from his own email platform. Sprint’s messaging domain, and the format of its user names (*i.e.*, MDN) are widely known. As with email, there are irresponsible senders who abuse text messaging. Sprint systems fend off countless numbers of Internet-originated text message spam. Because this type of Internet-originated text messaging requires a user name and domain – meeting the definition of “electronic message” – senders should be required to comply with the CAN-SPAM Act.

The Commission should not make a distinction between “push” and “pull” methods for receiving mobile text messages, where the message is sent using a user name and Internet domain. Regardless of method, there is a cost to consumers – whether airtime minutes of use, or per message fees. There are also costs to mobile service providers. Whether push or pull methods are used, service providers are required to add capacity to messaging gateways to accommodate volumes of unwanted MSCMs, and must continually implement new and costly measures for screening and filtering unwanted MSCMs.

² See 15 U.S.C. § 7702(5) & (6):

(5) Electronic mail address. The term "electronic mail address" means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the "local part") and a reference to an Internet domain (commonly referred to as the "domain part"), whether or not displayed, to which an electronic mail message can be sent or delivered.

(6) Electronic mail message. The term "electronic mail message" means a message sent to a unique electronic mail address.

B. ABILITY TO AVOID RECEIVING MSCMs

1. The CAN-SPAM Act Requires Consumer Choice

The Commission asks for comment on its interpretation that the CAN-SPAM Act does not require a flat prohibition against MSCMs. The CAN-SPAM Act clearly envisions that customers have the right to receive MSCMs. But, a sender may transmit MSCMs *only with the prior authorization of the recipient*. And recipients – once they have opted-in – must be given a means to request not to receive future MSCMs.³ In Sprint's experience many consumers find it a benefit to be made aware of new products and services by email. Sprint believes that many consumers also want to receive certain commercial messages on their wireless devices – either because they are interested in certain products and services, or because they have agreed to receive certain MSCMs in exchange for free or reduced-rate service (not unlike agreeing to view daily advertising sponsors in order to view a Web site for free). But, again, that should be the consumer's choice, and the CAN-SPAM Act is clear: senders must obtain prior authorization before sending an MSCM.⁴

2. Sender Ability to Identify MSCM

The Commission seeks comment on four possible mechanisms to enable senders to identify that they are sending an electronic message to a wireless device:

- i) List of Domain Names.
- ii) Registry of individual subscriber addresses.
- iii) MSM-only domain name.

- iv) Common MSM Subdomains.

³ 15 U.S.C. § 7712(b)(1) & (2).

⁴ An opt-out method of obtaining consent is not acceptable. Most experts agree that when the recipient sends back an opt-out, it just validates to the sender that he has a valid email address.

A registry of individual subscriber addresses is more likely to cause problems, rather than solve them, by making a list of valid addresses available for potential abuse. And, while a list of domain names or an MSM-only domain would be useful to help senders identify if they are sending a message to a mobile device, Sprint's experience is that senders are knowingly targeting wireless devices. Sprint is not aware of any incident where it appeared that a sender did not realize it was sending messages to a wireless device. Subdomains offer no advantage either.

3. The Commission Should Not Require Carriers to Support Challenge-Response Mechanisms, or Any Other Specific Technology.

The Commission seeks comment on whether wireless carriers should implement challenge-response mechanisms. As discussed above, it is Sprint's experience that senders are already well aware that they are transmitting messages to wireless devices. Sprint is concerned about the Commission requiring specific technical solutions to try to solve the wireless spam problem. To begin with, many senders are very sophisticated, and intentionally – and continually – work to defeat spam-blocking solutions and evade the law. A dramatic example of this is recent virus attacks on “wired-Web” email systems that directed Personal Computers to send messages to persons on address book lists. Many experts believe that these viruses may be trial runs by spammers to find new ways to unlawfully distribute spam. As in the “wired” world where anti-spam solutions continue to develop to meet consumer demand, Sprint expects that carriers and vendors will compete to develop new solutions for the wireless Internet. Plus, any specific technical solution ordered by the Commission today will not be completely effective, and will quickly become antiquated as device capabilities, and spamming tools evolve.

4. Commercial Message Identification

The Commission seeks comment on methods for identifying messages as commercial. In Sprint's experience, tagging messages – for example, by using “ADV” in the subject line of a message – does little, if anything, to help carriers and consumers avoid unwanted messages. Responsible senders will obtain prior express consent from consumers. It is the bad actors that are the problem, and they are not likely to follow tagging requirements. The Commission can expect that any commercial message identification requirements it imposes will be ignored.

C. EXPRESS PRIOR AUTHORIZATION

The Commission seeks comment on whether express prior authorization should be required to be in writing, and how any such requirement could be met electronically. The Commission also seeks comment on whether the CAN-SPAM Act definition of “affirmative consent” should be used for “prior express authorization.” Written consent is not practical. Today consumers may sign up to receive messages on a sender's Web site, either through wired-Web access or by using their handsets if the sender maintains a site compatible with mobile devices. For example, a consumer may elect to receive notice of new products and services, or elect to receive certain types of alerts (for instance, online auction status alerts). Sprint cautions against requiring specific ways to obtain consent. While today, consumers may provide consent by providing their wireless device address to senders over a Web interface, Commission requirements should not preclude other potential technical implementations that may be developed, such as the use of “secret codes” that the Commission's Notice refers to in order to validate incoming messages. While spam is a serious problem for both carriers and consumers, wireless commerce is just beginning to develop, and the Commission should take care to avoid hamstringing it at this point with specific technical requirements that are likely to soon be

outdated. With respect to the meaning of “prior express authorization,” Sprint believes it is clear on its face, and needs no further definition. For purposes of Section 222, governing the release of location information, the Commission held that “prior authorization” was self-explanatory, and no further definition was required.⁵

D. ELECTRONICALLY REJECTING MSCMs

The CAN-SPAM Act requires that the Commission develop rules that “allow recipients of MSCMs to indicate electronically a desire not to receive future MSCMs from the sender.” The Commission seeks comment on how that can be accomplished technically, and specifically asks carriers to comment on whether they have systems in place to allow subscribers to block messages from a sender upon request. The Commission also seeks comment again on challenge response mechanisms, and also on whether subscribers could supply a “secret code” to senders – so that carriers block based anything that did not contain the code.

Sprint does not currently have systems in place that allow subscribers to block messages from a sender upon request. However, Sprint has employed a number of measures to block and filter unwanted commercial text messages. And in response to consumer requests, Sprint does have the capability to “manually” block spam senders. Sprint is working with potential vendors to evaluate solutions that would put more control directly in the hands of its subscribers. But as already noted, technical solutions have their limitations. For example, spammers falsify router and header information. And they change IP addresses and domain names. Sprint anticipates that it will implement additional network and consumer protections, and that new solutions must

⁵ “We find Section 222(f)'s requirement of “express prior authorization” leaves no doubt that a customer must explicitly articulate approval before a carrier can use that customer's location information. Thus, no rules are necessary because the statutory language is unambiguous, imposing clear legal obligations and protections for consumers.” In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, WT Docket No. 01-72 (July 8, 2002)(footnote omitted), paragraph 5.

continue to evolve. But, the Commission should not put carriers in the position of being guarantors that consumers will never receive unwanted commercial messages. Even if carriers were to implement a specific technical requirement, spammers simply pose too much of a moving target, and the requirement would soon be outmoded. In this regard, the use of secret codes would most likely require significant carrier investment, with little guarantee that it would be effective for any meaningful period of time before spammers found a way to circumvent it. It would also require the cooperation of senders that the Commission does not have jurisdiction over.

E. EXEMPTION FOR COMMERCIAL MOBILE SERVICES PROVIDERS

The Commission seeks comment on whether there is any need for the CMRS provider exemption given that the Act already has an exclusion for “transactional and relationship” messages, which are defined to include messages sent regarding product safety or security information, notification to facilitate a commercial transaction, and notification about changes in terms, features, or the customer’s status. The Commission seeks comment on whether there are any other kinds of messages that CMRS providers send their customers that do not fall within the transactional/relationship message exclusion.

Carriers should be exempt from the prior authorization requirement. Sprint has found that its customers appreciate receiving information about new wireless products and services, new rate plans, new handsets, and the like. Yet, as a courtesy to its customers, Sprint also maintains a do-not-contact list which allows customers to indicate that they do not wish to receive any information of this type from Sprint by telephone or email, for example. Allowing carriers to communicate new product and service information without prior express authorization would be consistent with the TCPA exception that allows carriers to contact existing customer

with service offers without checking against the federal Do Not Call list, provided that they do check against internal, carrier specific lists.

CONCLUSION

Sprint has a keen interest in curbing unwanted MSCMs – for the sake of its customers and its network. Carriers, however, cannot guarantee that customers will not receive unwanted MSCMs from irresponsible senders. Rather than mandating certain technical solutions or placing unrealistic burdens on carriers to stop all spam, Sprint urges the Commission to clarify standards and definitions, and – in cooperation with the FTC and state authorities – step up on investigations and enforcement actions.

Respectfully submitted,

SPRINT CORPORATION



Luisa Lancetti
Vice President, Wireless Regulatory Affairs
Sprint Corporation
401 9th Street, N.W., Suite 400
Washington, D.C. 20004
202-585-1923

Joseph Assenzo
General Attorney
Sprint Corporation
6450 Sprint Parkway
Overland Park, KS 66251
913-315-9141