



TeleCommunication Systems, Inc. • www.telecomsys.com

White Paper

Wireless Spam Issues and Solutions

White Paper

Notices

© 2003 TeleCommunication Systems, Incorporated. All rights reserved. No part of this White Paper, including text, diagrams, or icons, may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording, or otherwise) without the prior written permission of TeleCommunication Systems, Incorporated.

Note to U.S. Government Users

Documentation related to restricted right - use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer - Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement.

Information in this document is subject to change without notice. TeleCommunication Systems, Incorporated may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you license to these patents, trademarks, copyrights, or other intellectual property. Please send licensing inquiries to: TeleCommunication Systems, Incorporated, 275 West Street, Annapolis, Maryland, 21401.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THIS PAPER IS LICENSED AND/OR PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, REGARDING THE CONTENTS OF THIS PAPER, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES FOR THE PAPER'S QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT SHALL TELECOMMUNICATION SYSTEMS, INC., OR ITS DEALERS OR DISTRIBUTORS BE LIABLE TO THE PURCHASER, OR ANY THIRD PARTY ASSOCIATED WITH THE PURCHASER, FOR LOST PROFITS, OR ANY OTHER CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Trademark Attributions

Enabling Convergent Technologies is a registered trademark of TeleCommunication Systems, Incorporated. All rights reserved. All other trademarks, logos and service marks are property of their respective owners.

Table of Contents

INTRODUCTION TO WIRELESS SPAM..... 1
 TEXT MESSAGING..... 1
 WIRELESS SPAM DEFINED 2

THE IMPACT OF WIRELESS SPAM 2
 FINANCIAL 2
 TECHNICAL..... 3
 CUSTOMER RELATIONS..... 3

ANTI-SPAM SOLUTIONS 4
 BUSINESS SOLUTIONS 4
 LEGISLATIVE SOLUTIONS 4
 CARRIER-LEVEL SOLUTIONS 4
 SUBSCRIBER-LEVEL SOLUTIONS..... 5

RECOMMENDATIONS 6

CONCLUSION 7

REFERENCES 8

Acronyms

EMS	Enhanced Messaging Service
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
MIN	Mobile Identification Number
MIS	Management Information Systems
MMS	Multimedia Messaging Service
SMPP	Short Message Peer-to-Peer
SMS	Short Messaging Service
SMTP	Simple Mail Transfer Protocol
TAP	Telocator Alphanumeric Protocol
TCS	TeleCommunication Systems, Inc.
URL	Uniform Resource Locator
WIG	Wireless Internet Gateway

Introduction to Wireless Spam

Have you recently received a message on your wireless phone that asks, "RUA YRLS USR?" Or perhaps, "4U A GR8 OFR?" If you recognized that the first message asks, "Are you a wireless user," and the second translates into, "For you a great offer," you may be among the 29 million Americans who are "texting," or sending and receiving text messages using your wireless phone. If you didn't recognize who sent you the message, you are also among another growing group – those who are receiving wireless spam. Wireless spam refers to unsolicited text messages that are sent to a wireless phone from an unknown person or company via another wireless phone, a wireless phone provider's web site or email.

Since text messaging is inexpensive, easy to send, and reaches large numbers of people, businesses are eager to employ it to drive product branding and sales. However, businesses are increasingly targeting wireless subscribers with whom they have not had a previous relationship. Subscribers' frustration with these unsolicited text messages is growing, and wireless carriers must find a solution.

This white paper examines the key issues pertaining to wireless text messaging and wireless spam. It describes the growth of wireless text messaging, the impact of wireless spam, available anti-spam solutions, and specific recommendations for wireless carriers.

Text Messaging

Text messages are written messages, usually 160 characters or less, sent to or from wireless phones using the SMS (Short Messaging Service) standard. Text messaging is convenient because it does not require computer or Internet access and can take less time than making a phone call, since it eliminates the protocols associated with a phone conversation. Text messaging is commonly used for communicating quickly when you can't place a call (during emergencies, when the cellular network is busy), or when discrete communication is required (such as during a meeting or event). It is also commonly used for receiving daily alerts like weather updates, sports scores or horoscopes.

In Europe, you don't have to look far to see someone sending or receiving a text message. Text messaging has taken off in Europe primarily because most European mobile carriers do not offer fixed calling plans, so "texting" is cheaper than making a mobile phone call. In the U.S., however, it has taken longer for text messaging (or "SMS") to achieve widespread usage. Easy access to email and the perception that a phone is a difficult device to type on have delayed SMS adoption. In addition, wireless calls are less expensive in the U.S., since carriers typically offer calling plans that include a fixed number of minutes for a standard fee. Depending on a subscriber's plan, either a set number of text messages are included in the plan, or subscribers are charged for each message sent and received.

Until a year ago, text messages could only be sent and received in the U.S. by wireless phones that operated on the same carrier network; different technology standards prevented transmission of messages between multiple carriers. With interoperability standards now in place, SMS messages can be transmitted seamlessly between carriers, and U.S. text messaging is gaining real momentum. According to the Cellular Telecommunications and Internet Association (CTIA), U.S. subscribers exchanged 253 million messages in December 2001, and in December 2002 that number rose to over one billion. The 18-25 year-old market segment and the business community represent the most frequent users of text messaging.¹ These users rely on SMS as a form of quick communication, much like instant messaging and email.

Wireless Spam Defined

Wireless phones in the U.S. began receiving spam in April 2000.² Often compared to telemarketing calls, junk mail, junk email, and Internet pop-up ads, wireless spam produces immense frustration for both wireless subscribers and carriers. There are two types of wireless spam. *Wireless user spam* can be defined as unwanted or unsolicited messages received on a mobile handset, sent through the SMS, MMS or EMS gateway to a mobile handset (mobile termination), or from handset to handset (mobile origination). *Network spam* refers to messages sent to solicit or harass a carrier's subscribers or to negatively impact a carrier's network. A subset of spam, *wireless scam*, refers to messages that encourage the receiver to reply to the message by placing a premium voice or data call. Most wireless spam falls into one of the following categories: adult content, financial, wealth, products, Internet and leisure.

The Impact of Wireless Spam

Wireless carriers seeking to maximize the tremendous revenue potential of short messaging services (SMS) and multimedia messaging services (MMS) should be aware of spam's financial, technical, and customer relations impacts.

Financial

Customers, carriers and the marketing industry are each financially impacted by spam. Most subscribers pay from two to five cents per text message, regardless of whether or not it was solicited, and some pay up to 45 cents per message.³ Since subscribers can be disrupted by spam at any time of day or night, they may be inclined to turn their phones off when they do not wish to be disturbed. Wireless phones that remain off are not maximizing revenue potential.

Carriers also incur direct costs, associated with message storage, message capacity, bandwidth, subscriber and management information systems (MIS), maintenance, and customer care. In addition, increased customer care resources are needed to field complaints resulting from bounced mail and spam. However, per-message revenues received from subscribers can offset much of these additional costs.

For the advertising and marketing industry, text messaging is an inexpensive medium for reaching a large target market. Wireless phones are ideal for advertising since they generally belong to one person, are usually on and go everywhere—and open Internet gateways enable messages to be transmitted from anywhere in the world. Mobile advertising (ads directed at wireless phones) has already been reported to generate response rates as high as 20-30 percent, compared to only two percent for direct mail.⁴ With no real out-of-pocket costs, advertisers only need a few responses for mobile advertising campaigns to be successful.

Wireless advertising can also represent a value-added revenue stream for financially struggling wireless carriers. Advertisers who pay a fee to the carrier can gain access to subscribers who have opted-in to receiving ads. However, if subscribers begin to receive spam *in addition* to their opt-in ads, they may become confused and frustrated with the carrier or the advertiser. They may suspect that the carrier or the vendor has shared their number with additional advertisers and that they are now on one or more spam "lists." Thus, spam could compromise a fledgling (and legitimate) advertising industry that otherwise could be beneficial to carriers, subscribers, and advertisers.

Technical

Wireless spam encompasses a number of technical factors. Because wireless phone numbers are assigned in blocks of 10,000 with the same area code and exchange, transmitting wireless spam is relatively easy. A spammer looking to reach a large, general, target market only needs to know one subscriber's wireless phone number. If a spammer can identify the last four digits of a phone number as a cell phone number, the chances are likely that all the numbers in that particular "block" are also wireless phone numbers. Wireless spam can be most easily and copiously sent through the Internet as email; the wireless subscriber's email address is usually their wireless phone number followed by the service provider's name. Spam sent from handsets is less common, since the sender typically pays to transmit mobile-originated messages, and mobile-originated messages are usually sent one at a time.

Another technical impact is that wireless phones have limited storage capacity, with some as low as eight 160-character text messages. Unfortunately, the subscriber does not have the option to choose which messages the phone will receive and store and which messages the phone will not accept due to full capacity. If a subscriber receives eight unsolicited messages and does not delete them, then a ninth message, from a colleague or friend, will not be received until the subscriber deletes some of the spam messages. In addition, many handsets audibly alert the subscriber when a message arrives, encouraging them to read it immediately. Thus, subscribers are practically forced to read wireless spam, whereas email spam can often be deleted without being opened.

Finally, carriers must have sufficient network storage capacity to handle the volume of messages resulting from wireless spam. Unsolicited messages strain network bandwidth and delay transmission of legitimate, opt-in text messages. Since customers typically pay for each inbound message, they are more likely to call customer care inquiring about why they are receiving unwanted messages and requesting credit. This requires technical solutions that give customer care representatives access to subscriber message logs and billing systems, as well as the ability to post credits to subscriber accounts.

Customer Relations

From the subscriber's perspective, certain aspects of spam are ambiguous. For example, many subscribers incorrectly conclude that their carrier initiated, approved and sent the spam messages they receive. Since subscribers are often unclear who is involved in the spam's channel of distribution, they may feel the carrier is exploiting them for additional SMS revenue. Such subscribers are likely to churn their service in favor of a carrier they perceive as not supportive of spam. Recent discussions of wireless number portability further provide incentive for a subscriber to exercise this option. Subscriber churn costs carriers in lost revenue due to defection and new customer acquisition costs.

Privacy is another major customer relations concern. Wireless telephone numbers in the U.S. are not listed in the public phone book or available through carrier directory assistance. Therefore, wireless customers may believe that only those people to whom they have given their number have it. If they begin to regularly receive spam messages on their phones, it becomes obvious that their number is no longer just in the hands of people they know. Subscribers again may look to the carrier, holding the carrier responsible for the security of this private information (phone number). Ultimately, spam impacts a subscriber's attitude towards using SMS, which could also affect their adoption of value-added services like MMS in the future.

Anti-Spam Solutions

Due to the complex nature of wireless devices, there is no single, foolproof solution available to prevent transmission of wireless spam. At the current time, a number of business, legislative, carrier-level and subscriber-level solutions are available.

Business Solutions

Business solutions include self-regulation by carriers, updated roaming agreements between carriers, and contractual agreements with content providers. They may also include withholding payment to service providers that send spam messages and obtaining information provided by associations on companies that purchase premium rate voice and data numbers. In addition, overseas carriers have suggested an agreement whereby they themselves would pay a higher rate for sending messaging through mainland networks. However, business solutions often need technology behind them to give customers confidence their effectiveness.

Business solutions work best when the sending party pays to deliver the messages to the end user. In the U.S., where the receiving party typically pays, most business solutions will not work unless the carrier decides to block all messages coming from unknown sources. However, this would eliminate a large source of current SMS traffic and, therefore, legitimate carrier revenue.

Legislative Solutions

Wireless anti-spam legislation is becoming a hotly contested subject in both the U.S. Senate and House of Representatives. Eager to eliminate the problem of wireless spam before it gets out of control, legislators have recently introduced a number of proposals. These bills include language that would prohibit text, graphic, or image messaging sent to wireless devices; prohibit unsolicited advertising being sent to wireless phones; create opt-in/out systems; and require advertisers to provide detailed contact information with the message. Opponents to these proposals argue that the industry has already taken the necessary steps to limit unsolicited messages, and a new law would affect the future use of technology. For the carrier, pursuing legal solutions to combat spam is often costly; the culprit may be difficult to identify and, even if discovered, may be outside local legal jurisdictions.

Carrier-Level Solutions

Since networks are open and tied-in with the Internet, carriers need a dedicated gateway and portal to serve as the gatekeeper between advertisers and subscribers. A strong gateway solution should include the following technical capabilities:

Carrier Configuration - Enables a carrier to maintain a global database of known spammers and to refresh detection data periodically; configuration changes can be made on the fly without any SMS traffic flow interruption; since the rules apply to all subscribers it saves them the hassle of doing it themselves.

Known Spammer Defense Mechanisms / Black Lists - Provide customized detection methodologies for known spammer email addresses and email domains; can validate destination domain names to detect spam sources.

Blocking - Blocks or denies messages if they are transmitted from a known messaging relay server.

Multiple Sources - Blocks messages from multiple sources. Carriers who support multiple methods of receiving messages, such as email, web sites, inbound modem pools, and even person-to-person messaging, should have a solution that allows anti-spam rules to be applied to all input sources.

Count Thresholds - Sets a limit on the number of messages received from input sources specified by source IP address, domain name, and protocol; used in denial of service protection and in enforcing commercial contracts that specify the message volume that can be transmitted.

Denial of Service Protection - Blocks or denies spam or malicious messages that arrive in large volumes; can be applied at a specific URL or IP address level or globally; blocks messages of a maximum size, or by total time of an active SMTP session, and limits the time allowed for a SMTP client session to complete a SMTP primitive transaction. Throttling is also used in Denial of Service Protection.

Throttling Defense Mechanisms - Recognize spam based on the rate of message traffic by identifying: number of messages received from a specific source addressed over a period of time, number of messages received by a specific receiver, number of messages sent from a particular protocol source, number of messages sent from a particular email domain, or number of messages sent from a particular information provider.

White Lists - Provide simple-to-use rules that specify that any messages containing certain criteria will bypass existing defense mechanisms. Rules can contain messages with valid IP, domain or URL sender source addresses; messages by MINs; messages from registered users; messages from personal calendar events; SMS to alias messages; and SMS to MIN messages.

Pattern Matching - Provides the ability to block messages containing phone numbers and to detect key words, exact expressions, and partial expressions. Pattern matching can be applied to the subject header or to the body of the message and is one of the most frequently requested spam defenses.

Subscriber-Level Solutions

Since subscribers know best which messages they should receive, they should be involved in the process of preventing spam. Some of the options currently available to subscribers include:

Opt-out - Provides the most basic and foolproof mechanism. Some messages that were originally benign may become annoying to the subscriber over time. A messaging portal should provide the subscriber with automated mechanisms to opt-out of these types of messages. The most preferred mechanism is a web site, but a mobile-originated message reply could also provide a means for the subscriber to opt-out of further messages from that particular address.

Black List - Enables an end-user to block messages based on the sender's address, sender email domain, specific registered user aliases, and particular sources (e.g., SMTP, HTTP, TAP or SMPP).

Quarantine - Filters out and stores messages in a separate bucket or folder for future review. This bucket is similar to a separate email folder where all questionable messages can be reviewed separately. Since most subscribers are not likely to want to maintain an email

account for their wireless device (in addition to home and office email accounts), quarantine should be used sparingly, if at all.

Filtering - Detects messages based on criteria such as subject line or body of text provided by the end user. A messaging portal solution should provide a place where the user can enter this information from a web page.

White List Only - Some subscribers prefer to receive SMS messages only from a few, select, known sources; all other messages are blocked.

Recommendations

Since there is no single solution for the ongoing battle against wireless spam, a combination of business solutions, carrier-level solutions and subscriber-level solutions is recommended. This comprehensive approach provides the most reliable, accurate and effective defense against unwanted text messages.

TeleCommunication Systems (TCS) has devoted significant resources over the past six years to developing the TCS Wireless Internet Gateway™ (WIG), which provides a robust set of network- and subscriber-level features. These features include white lists, black lists, blocking, filtering, denial of service detection, throttling, pattern matching, known spammer lists, opt-out, count threshold and a carrier configuration interface tool to prevent malicious spam messages from being sent to wireless subscribers. The highly reliable TCS WIG solution focuses on all points of entry into a carrier's network, including SMS, EMS, MMS and web messaging.

At the network level, the TCS WIG prevents excessive messages from being transmitted into the system from a particular source on a global level set by the carrier's system administrator. A limit on the number of messages that one sender can send, as well as a limit on the number of messages a receiver can receive, prevents excessive usage of the gateway, which would slow other messages from being sent as well as prevent a large volume of spam messages. It also rejects SMTP messages from pre-configured sources, such as a sender's email address, IP address and/or domain determined by the system administrator. Black and white lists are used to define exceptions to the message limit. TCS' black list capabilities prevent the system from being overwhelmed by large amounts of unsolicited messages. This eliminates messages that inconvenience subscribers. The WIG can also define a white list of message sources that are not subject to the anti-spam limits. Typically these messages will be from the system administrator and other trusted sources. The TCS WIG provides additional anti-spam functionality and preventive measures to guard against potential denial of service attacks, including subject line and message body filters, expression-based pattern matching, maximum session time-out, and validation of IP addresses and domain names.

At the subscriber level, the TCS WIG allows subscribers to provision the anti-spam feature to determine who, where and what type of message they can receive or block. With its web-based subscriber anti-spam configuration, subscribers can filter and block incoming messages based on classification of incoming messages. Subscribers can determine valid from invalid senders by filtering based on MIN, name, alias, domain, or subject header.

Conclusion

In the U.S., wireless messaging is rapidly gaining popularity. It is a quick, easy and relatively inexpensive way to communicate when it is not feasible to make a phone call. The prevalence of wireless spam is increasing almost as quickly as the popularity of wireless messaging. Wireless spam results in potentially significant financial, technical, and perceptual effects for carriers, subscribers and advertisers. With the proliferation of spam, carriers are faced with the daunting challenge of providing a reliable solution to ensure their subscribers aren't faced with financial, technical, and privacy issues that could result in subscriber churn, reduction in service usage, cancellation of features, or curtailing promising revenues from marketing and advertising sources before they can gain momentum. TCS' Wireless Internet Gateway™ is a complete, carrier-grade portal solution that provides vigorous anti-spam functionality at both the network and subscriber levels, focusing on all points of entry into a carrier's network. Additionally, it empowers subscribers to choose which messages to receive or view, and which messages to block.

If you would like further information on TCS' anti-spam solutions, please call 1.877.223.1529 (from the US) or +1 410.263.7616 (outside the US)—or send an email requesting more information to WIG@telecomsys.com.

TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401 USA

www.telecomsys.com

References

¹ Megna, Michelle. "Sell Phone Madness." New York Daily News Online. 10 July 2003. <http://www.nydailynews.com>.

² Cramer, Evan. "The Future of Wireless Spam." 2002 Duke Law and Technology Review 0021. 28 October 2002. <http://www.law.duke.edu/journals>.

³ Motsay, Emily. "Trash or Treasure? Industry takes on Wireless Spam." RCR Wireless News. 7 July 2003: 11.

⁴ Pesola, Maija. "The Novelty Could Quickly Wear Off Mobile Advertising." Financial Times, London. 18 July 2001: 11.