Text and Multimedia Messaging: Emerging Issues for Congress

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

July 20, 2010

Congressional Research Service
7-5700
www.crs.gov
RL34632

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The first text messages were sent during 1992 and 1993, although commercially, text messaging was not widely offered or used until 2000. Even then, messages could only be sent between users subscribed to the same wireless carrier, e.g., Sprint customers could only exchange messages with other Sprint customers. In November 2001, however, wireless service providers began to connect their networks for text messaging, allowing subscribers on different networks to exchange text messages. Since then, the number of text messages in the United States has grown to over 48 billion messages every month. Additionally, text messages are no longer only sent as "point-to-point" communications between two mobile device users. More specifically, messages are also commonly sent from Web-based applications within a Web browser (e.g., from an Internet e-mail address) and from instant messaging clients like AIM or MSN.

For Congressional policymakers, two major categories of issues have arisen: (1) "same problem, different platform" and (2) issues stemming from the difficulty in applying existing technical definitions to a new service, such as whether a text message is sent "phone-to-phone" or using the phone's associated email address. There are numerous examples of each. An example of the first category would be consumer fraud and children's accessing inappropriate content, which have existed previously in the "wired world," but have now found their way to the "wireless world." An example of the second category would be that spam sent between two phones or from one phone to many phones does not fall under the definition of spam in the CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act, P.L. 108-187); however, if that same message were to be sent from a phone or computer using the phone's associated e-mail address, it would.

The increasing use of text and multimedia messaging has raised several policy issues: applicability of CAN-SPAM Act to unwanted wireless messages; refusal of some carriers to allow users to disable text messaging; carrier blocking of Common Short Code messages; deceptive and misleading Common Short Code programs; protecting children from inappropriate content on wireless devices; "sexting"; mobile cyberbullying; and balancing user privacy with "Sunshine," Open Government, and Freedom of Information Laws.

Contents

Figures

Appendixes

Contacts

Introduction

The first text messages were sent during 1992 and 1993, although commercially, text messaging was not widely offered or used until 2000. Even then, messages could only be sent between users subscribed to the same wireless carrier, e.g., Sprint customers could only exchange messages with other Sprint customers. In November 2001, however, wireless service providers began to connect their networks for text messaging, allowing subscribers on different networks to exchange text messages. Since then, the number of text messages in the United States has grown to over 48 billion messages every month. Additionally, text messages are no longer only sent as "point-to-point" communications between two mobile device users. For example, messages are also commonly sent from Web-based applications within a Web browser and from instant messaging clients like AIM, MSN, or Google Chat.

Definitions

Short Message Service

Short Message Service (SMS) is a method of communication that sends text between cell phones, or from a computer or handheld device to a cell phone. The "short" part refers to the maximum size of the text messages: 160 characters.[1] The term "SMS" is generally used interchangeably with the term "text message."

Even when not being used for a voice call, a mobile phone is constantly sending and receiving information. It is communicating to its cell phone tower over a control channel. The reason for this communication is so that the cell phone system knows which cell a phone is in, and so that the phone can change cells as the user moves around. Every so often, a phone and a tower will exchange a packet of data that lets both "know" that everything is working properly.

The control channel also provides the pathway for SMS messages. When someone sends an SMS message, the message flows through the SMS Center (SMSC), then to the cell tower, and the tower then sends the message to the recipient's phone as a packet of data on the control channel. **Figure 1** illustrates how a SMS message is processed.

Enhanced and Multimedia Message Service

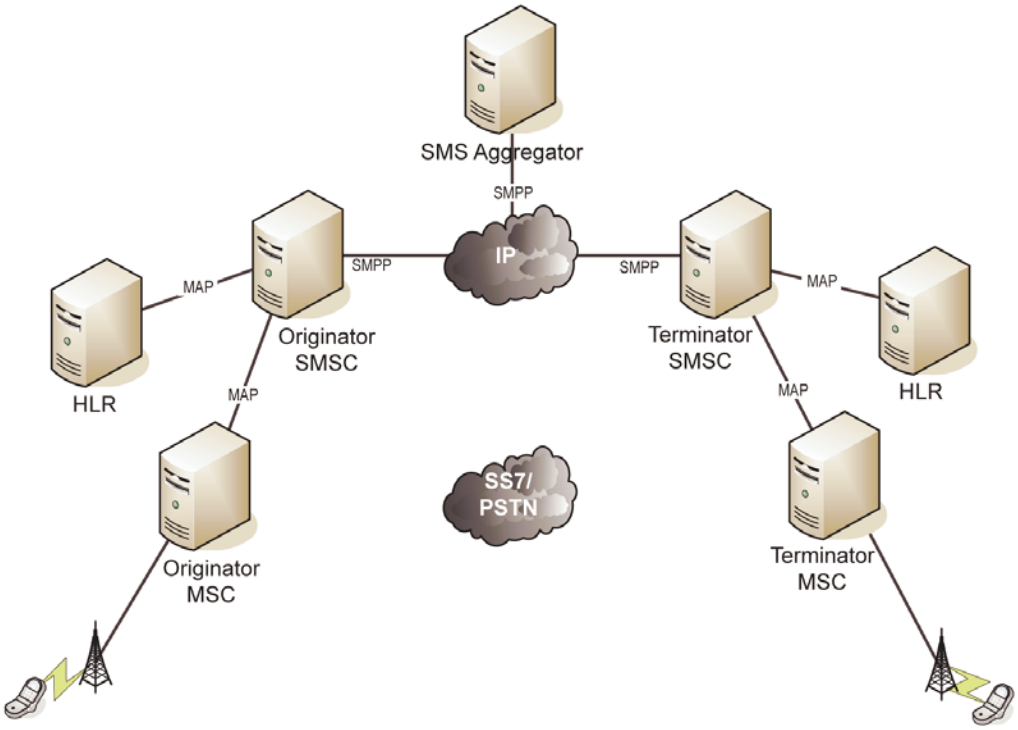
While SMS only allows plain text to be sent, two alternative messaging services allow for more elaborate types of messages. With Enhanced Messaging Service (EMS), formatted text, sound effects, small pictures, and icons can be sent. MMS (Multimedia Messaging Service) allows animations, audio, and video files in addition to text to be sent.

[1] For some alphabets, such as Chinese, the maximum SMS size is 70 characters.

E-mail-to-SMS Messaging

As noted above, SMS messages may be sent between a computer and a mobile phone. However, these messages are sent using the e-mail address associated with the mobile device, such as 2025551212@carrier.com. For that reason, these messages are classified as e-mail and therefore are subject to different and more stringent regulation (see "SMS Spam").

Figure 1. Path of Intercarrier SMS Messages

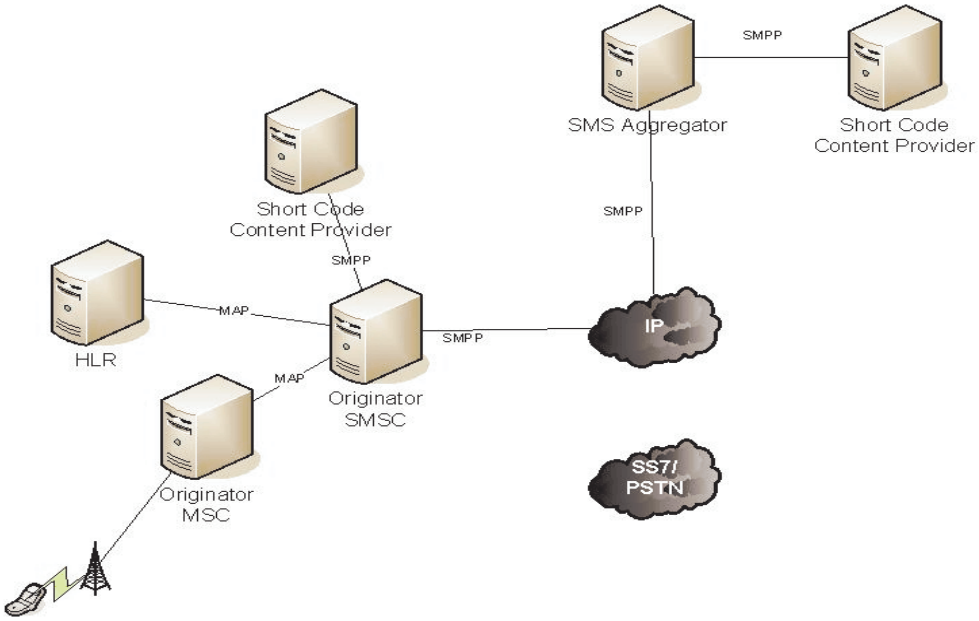


Source: Used with permission from Motorola. Definitions: The "Internet Protocol (IP) cloud" represents an Internet Protocol network used to carry data traffic; HLR = Home Location Register (the central database that contains details of each mobile phone subscriber); MAP = Mobile Application Part signaling protocol; MSC = Mobile Switching Center; the "Public Switched Telephone Network (PSTN) cloud" is included to demonstrate that SMS messages are not carried over it; SMS Aggregator = an intermediary between mobile service providers providing SMS service; SMSC = SMS Center; SMPP = Short Message Peer-to-Peer Protocol.

Common Short Codes (CSCs)

Introduced in the U.S. market in October 2003, Common Short Codes (CSCs) are short numeric codes of five or six digits, compatible across carriers, to which text messages can be sent from a mobile phone. Wireless subscribers send text messages to short codes to access a wide variety of mobile content, for example, to vote for contestants on American Idol. Many entities use CSCs to communicate with interested parties: television stations; individual television shows; radio stations; instant messaging services; political, advocacy, and other organizations; magazines, and sports teams—among others. Users send a message to the CSC to subscribe to alerts or other messages. Sometimes these messages are delivered for free by the originator, sometimes there is a fee. **Figure 2** illustrates how a CSC message is processed.

Figure 2. Path of Common Short Code Messages



Source: Used with permission from Motorola. See **Figure 1** for acronym definitions.

"Vanity" CSCs are also available (for a higher price)—these CSCs use letters on a mobile device keypad to spell out words that are easy to remember and are chosen to reflect the service the short code is being used to access.[2] Furthermore, although CSCs can be "compatible" across all carriers, some CSCs are established as business partnerships between a specific carrier and another entity. For example, American Idol has an exclusive partnership with AT&T Wireless.[3]

Issues for Congress

For Congressional policymakers, the major issues that have arisen stem from what could be called "same problem, different platform." For example, issues such as consumer fraud and children's accessing inappropriate content, which have existed previously in the "wired world," have now found their way to the "wireless world."

Other issues stem from the difficulty in applying technical definitions to a given service, such as whether a text message is sent "phone-to-phone" or using the phone's associated e-mail address. For example, spam sent between two phones or from one phone to many phones does not fall

[2] See https://www.usshortcodes.com/csc/search/publicsearchCSC.do?method=showVanity & group=all for examples of such codes.

[3] See http://www.americanidol.com/mobile/ for specific instructions.

under the legal definition of spam; but if that same message is sent from a phone or computer using the phone's associated e-mail address, it does.

Distracted Driving Caused By Texting

According to the U.S. Department of Transportation, approximately 16% of fatal automobile crashes and 80% of all crashes in 2008 were caused by distracted driving. While reading and composing text messages while driving is only one of numerous factors that can lead to distracted driving, such activity is a growing concern among safety and regulatory groups. In response to this concern, there have been various actions taken at the federal and state levels.

Federal Activity

Both the Congress and the Executive have taken actions to mitigate distracted driving caused by texting while driving.

Legislative Activity

S. 1536 and H.R. 3535, have been introduced in Congress that would amend Title 23 of the U.S. Code to reduce the amount of federal highway funding available to states that do not enact laws prohibiting texting while driving. Both are called the Avoiding Life-Endagering and Reckless Texting by Drivers Act, or ALERT Drivers Act, of 2009. S. 1536 was introduced by Senator Charles Schumer on July 29, 2009, and referred to the Committee on Environment and Public Works; no further action has been taken. H.R. 3535 was introduced by Representative Carolyn McCarthy on September 9, 2009, and referred to the Committee on Transportation and Infrastructure Subcommittee on Highways and Transit; no further action has been taken.

A bill similar to those discussed above, H.R. 4153, would amend Title 23, United States Code, to establish national standards to prevent distracted driving. This bill would require the Secretary of Transportation to withhold specified graduated percentages of a state's apportionment of certain federal-aid highway program funds for FY2012-FY2015. This bill was introduced by Representative Todd Platts on November 9, 2009; on November 20, 2009, it was referred to the Subcommittee on Highways and Transit. No further action has been taken.

Two companion bills, H.R. 3994 and S. 1938, both called the Distracted Driving Prevention Act of 2009, were introduced by Representative Eliot Engel on November 3, 2009, and Senator John Rockefeller on October 27, 2009, respectively. H.R. 3994 was referred to the Subcommittee on Highways and Transit on November 4, 2009, and S. 1938 was ordered to be reported with an amendment in the nature of a substitute on June 9, 2010. These bills take a multi-pronged approach, involving the Secretary of Transportation, National Highway Traffic Safety Administration, and the FCC, to reduce distracted driving.

Executive Activity

U.S. Department of Transportation held a Distracted Driving Summit on September 30 – October 1, 2009. Topics addressed included the definitions and data related to driver distractions and inattention; quantifying the risks of distracted driving; technologies available to mitigate distracted driving; legislation, regulation, and enforcement of distracted driving; and how to raise

public awareness of the problem. In conjunction with the summit, on October 1, 2009, President Obama signed an executive order banning federal employees from text messaging when they are behind the wheel of government vehicles and from texting in their own cars if they use government-issued phones or are on official business.

State Activity

Nineteen states and the District of Columbia have enacted a ban on texting while driving (some states have partial bans on young drivers using the cellphone in any capacity while driving). Additionally, 33 states debated 113 bills to curb driver distraction last year. A complete state-by-state listing is available on the National Council of State Legislatures website.[4]

SMS Spam

The CAN-SPAM Act was and is intended to curb the amount of spam that consumers receive in their e-mail accounts. At the time the act was being considered in 2003, text messaging was in its infancy as a service. As discussed above, SMS messaging is not the same as messaging that uses a mobile phone's associated e-mail address (i.e., 2025551212@carrier.com). At this time, only the latter type of message is covered by CAN-SPAM; messages that are sent "phone-to-phone" through the SMSC are not.

There is no evident reason for messages that appear the same to a user and have the same effect on a user (generally, annoyance) to be treated differently under CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act, P.L. 108-187). Resolving this discrepancy in the treatment of these two types of messages would require a change to the statute.

Legislation in the 111th Congress

Representative Phil Gingrey introduced H.R. 1391, the Stop M-Spam Abuse as a Sales Industry Habit—or "SMASH"—Act on March 9, 2009; the bill was referred to the House Committee on Energy and Commerce. This bill would require the Federal Trade Commission (FTC) to revise the Telemarketing Sales Rule to explicitly prohibit, as an abusive telemarketing act, the sending of "any electronic commercial message containing an unsolicited advertisement" to a mobile telephone number that is listed on the FTC's do-not-call registry.

Senator Olympia Snowe introduced S. 788, the m-Spam Act, on April 2, 2009; the bill was referred to the Senate Committee on Commerce, Science, and Transportation. This bill would (1) exclude applicability of the law to certain classes of messages (e.g., to facilitate or confirm a commercial transaction); (2) exempt from prohibition sending unwanted messages from one wireless device to another or from a mobile service provider to its subscribers at no charge (unless a subscriber has opted out); (3) requires the FTC to revise the TSR to consider messaging practices that are costly or a nuisance to consumers; and explicitly prohibit, as an abusive

[4] Cellular Phone Use While Driving Laws, National Council of State Legislatures, October 2, 2009, http://www.ncsl.org/default.aspx?TabId=17057. See also, National summit to highlight state solutions to growing traffic safety concern, National Council of State Legislatures, October 2, 2009, http://www.ncsl.org/PressRoom/PressReleaseDistractedDrivingSummit/tabid/18643/Default.aspx.

telemarketing act, the sending of any message to a mobile telephone number that is listed on the do-not-call registry.

Inability of Consumers to Disable Text Messaging

Some mobile service customers have expressed frustration to their Congressional representatives about unwanted text messages and the inability to selectively block or completely disable text messaging on their phones. While carriers generally offer a range of text messaging packages, for example, 500 messages for $10, some customers do not use text messaging and, therefore, pay a small fee every time they receive a message. A number of user discussion sites contain posts from users who are frustrated with the extra charges they incur from unwanted messages.[5] In December 2007, a class-action lawsuit was filed against T-Mobile in this matter.[6]

Most carriers offer some form of text blocking to their customers. A June 12, 2008, article by David Pogue in the New York Times[7] outlined the various options being offered by different carriers. The **Appendix** contains information from that article that may be helpful to consumers.

Given that carriers are beginning to offer various forms of text blocking to their customers, it may be advantageous to consumers to wait to see what options the different carriers develop. In that way, competition is given a chance to succeed in this area and carriers are offered the opportunity to assess what their competitors are doing and perhaps improve their own services. Eventually, however, Congress may wish to investigate whether customers are being offered the best possible options to assure that they are not receiving unwanted text messages.

Carrier Blocking of Common Short Code Messages

In September 2007, Verizon notified NARAL Pro-Choice America that it would not participate in its CSC program. NARAL does not charge for its messages and users may opt-in or opt-out as desired, but Verizon stated that it does not accept programs from any group "that seeks to promote an agenda or distribute content that, in its discretion, may be seen as controversial or unsavory to any of [its] users."[8]

This decision was immediately criticized by free-speech advocates, although communications scholars pointed out that the company most likely, from a legal standpoint, did have the right to refuse to participate in the program.[9] Since text messages are not carried over the traditional telephone network, such messages are not protected under common carrier regulation. The next day, Verizon changed its decision and is now participating in NARAL's CSC program, saying in a statement that the decision had been "an incorrect interpretation of a dusty internal policy" that

[5] See, for example, Mobiledia Forum at http://forums.mobiledia.com/topic35359-0-asc-10.html.

[6] RCR Wireless News, "Class Action Nails T-Mobile USA Over Texting Services," January 30, 2008, available online at http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20080130/FREE/927035123/1005/rss01.

[7] New York Times, "How to Block Cellphone Spam," by David Pogue, June 12, 2008, available online at http://www.nytimes.com/2008/06/12/technology/personaltech/12pogue-email.html.

[8] New York Times, "Verizon Blocks Messages of Abortion Rights Group," by Adam Liptak, September 27, 2007, available online at http://www.nytimes.com/2007/09/27/us/27verizon.html.

[9] New York Times, "Verizon Blocks Messages of Abortion Rights Group," by Adam Liptak, September 27, 2007, available online at http://www.nytimes.com/2007/09/27/us/27verizon.html.

"was designed to ward against communications such as anonymous hate messaging and adult materials sent to children." The policy had been developed "before text messaging protections such as spam filters adequately protected customers from unwanted messages."[10]

This issue highlights the difficulty in applying the current regulatory structure to new services. While mobile providers appear to have the legal right to determine what information is available through their CSC programs, Congress may wish to consider whether and how political and other speech might be better protected in those programs.

Deceptive and Misleading Common Short Code Programs

Many third-party content providers use the CSC program and bill the usage through the mobile service provider. For example, content providers can allow mobile device users to download content (e.g., ringtones) or participate in SMS-based "chat." While most of these content providers are legitimate businesses, others use deceptive tactics to gain customers and run up unexpected charges.[11]

For example, as reported by CBS News in February 2008, some customers have subscribed to monthly services without reading the "fine print" and find that the charge is often difficult to remove because it is an independent third party rather than the customer's mobile service provider.[12]

The Mobile Marketing Association has developed "Consumer Best Practices Guidelines"[13] that it expects its members to follow. This code includes limiting subscription periods to one month, after which consumers must re-subscribe, and providing alerts to customers when their chat-related charges reach $25 increments. Although the best practices have not eliminated all misleading programs, over time the industry may bring its members into compliance. More clarity on industry efforts might allow policymakers an opportunity to assess the efficacy of those efforts.

Protecting Children from Inappropriate Content on Wireless Devices

As more mobile devices become equipped to access the World Wide Web and additional content services are made available via CSCs, the risk of children downloading inappropriate content will likely increase. While carriers may follow a set of voluntary guidelines[14] to promote wireless

[10] New York Times, "Verizon Reverses Itself on Abortion Messages," by Adam Liptak, September 28, 2007, available online at http://www.nytimes.com/2007/09/28/business/28verizon.html.

[11] See Class Action Connect online at http://www.classactionconnect.com/cell_phone_issues/category/complaints-in-the-news/ for examples of these types of complaints.

[12] CBS News, "Ringing Up Big Charges For 'Free' Tones," February 22, 2008, available online at http://www.cbsnews.com/stories/2008/02/22/eveningnews/main3867197.shtml.

[13] This document is available online at http://www.mmaglobal.com/bestpractices.pdf.

[14] CTIA—The Wireless Association® has voluntary guidelines for wireless carriers to use in classifying content that they provide directly over wireless handsets. These voluntary guidelines apply only to content that you purchase from your wireless carrier, either on a one-time use or download basis, or as part of a package with a monthly fee such as ring tones, wallpaper, games, music, video clips, or TV shows. Content that is generated or owned by a wireless user, such as text messages, instant messages, e-mail (through chat rooms, message boards, etc.) and picture mail is not (continued...)

safety for children, there is no way to guarantee that children will not be able to access inappropriate content by circumventing carrier-implemented safeguards.

The following types of material can be downloaded on many wireless devices, and may include content inappropriate for children.

- Images, such as background "wallpaper" for the phone screen.
- Games, including some games that are also available for gaming systems.
- Music and songs, including ring tones, ringback tones, and downloads of full songs.
- Video, including certain television shows, movies, and music videos, as well as video programming specially made for, and only available on, wireless devices.[15]

The wireless industry is working to ensure that children do not access inappropriate information over their wireless devices, but there is no definitive research on the success of these efforts. Whether current efforts to protect children from inappropriate content over wireless devices may be an issue of interest to policymakers.

"Sexting"

Sexting is a term coined by the media that generally refers to youth writing sexually explicit messages, taking sexually explicit photos of themselves or others in their peer group, and transmitting those photos and/or messages to their peers.[16] Sexting is not the same as a child sending a sexually explicit photo to an adult, however, the ramifications can be extremely serious because of how child pornography laws are written. In general, regardless of the age of the person who takes the photograph and/or sends it, that photograph is considered child pornography. This has led to situations in which underage girls have been charged with distributing child pornography and others in which teenagers have been required to register as sex offenders.

Although no federal charges have been brought in these types of cases yet, it is conceivable that they could. Congress may wish to consider whether children should be prosecuted under statutes intended to prosecute child predators and pornographers and whether, in certain cases, such prosecutions might be warranted.

(...continued)

included in the wireless carrier's content classification system. Also, content that is accessed by surfing the Internet on a wireless handset is not currently included in the classification system. The guidelines urge carriers to provide separate Web filtering software for Web browsing services. Wireless carriers choosing to follow these voluntary guidelines agree to use at least two content ratings: (1) Generally Accessible or available to consumers of all ages; and (2) Restricted or accessible only to those age 18 and older or to those younger than 18 years old, when specifically authorized by a parent or guardian. The Restricted ratings system generally is based on or uses criteria under existing ratings systems for movies, television, music, and games. CTIA Guidelines are available online at http://www.ctia.org/advocacy/policy_topics/topic.cfm/TID/36.

[15] FCC Consumer Fact Sheet, "Protecting Children from Adult Content on Wireless Devices," available online at http://www.fcc.gov/cgb/consumerfacts/protectingchildren.html.

[16] National Conference of State Legislatures, 2009 Legislation Related to "Sexting" http://www.ncsl.org/?tabid=17756.

Mobile Cyberbullying

"Cyberbullying," harassing communications sent, for example, via e-mail or text messages or through social networking sites such as Facebook or MySpace, is a growing problem. The issue made national headlines in November 2007 after the suicide of Megan Meier, a 13-year-old Missouri girl. In that case, the mother of a former friend of Megan's set up a fake MySpace page, pretending to be a boy who had just moved to the area and was home-schooled. Within a few weeks of becoming "friends" with "Josh," on October 15, 2006, the tone of his messages changed drastically, with "Josh" saying he no longer wanted to be friends with Megan, because "he" had heard that she had been mean to some of her friends. On October 16, 2006, Megan hanged herself in her closet.

Although, as in the case described above, much cyberbullying takes place in the "wired" world, more recently, these sorts of messages are being sent from and to mobile devices. Since many mobile devices are capable of performing the same tasks as computers, these messages are now being sent via mobile instant messaging, the mobile websites of social networking sites, and text messaging.

The subsequent public outcry over the Megan Meier case led to four bills being introduced in the 110th Congress, three by Representative Linda Sanchez and one by Senator John Kerry; each contained language that would have included the use of wireless devices in the definition of cyberbullying.[17] All would have defined cyberbullying to include "verbal, visual, or written psychological bullying or harassment by an individual or group, using an electronic device or devices including e-mail, instant messaging, text messages, blogs, telephones, pagers, and websites, to support deliberate, repeated, and hostile behavior that is intended to harm others." None of these bills were signed into law.

Legislation in the 111th Congress

Representative Adam Putnam introduced H.R. 780, the Student Internet Safety Act, on January 28, 2009; the bill was passed on June 17, 2009, and referred to the Senate Committee on Health, Education, Labor, and Pensions. This bill would allow local educational agencies that receives funds under Elementary and Secondary Education Act of 1965[18] to those funds to develop and implement programs that promote the safe use of the Internet by students, including cyberbullying awareness programs.

Representative Linda Sanchez introduced H.R. 1966, the Megan Meier Cyberbullying Prevention Act, on April 2, 2009; the bill was referred to the House Committee on the Judiciary. A hearing on this bill took place on September 30, 2009. This bill would amend the federal criminal code to

[17] H.R. 3577 was introduced on September 17, 2007, and referred to the House Committee on Energy and Commerce Subcommittee on Telecommunications and the Internet; no further action was taken. H.R. 4134 was introduced on November 9, 2007; it was passed by the House on November 13, 2007, and referred to the Senate Committee on the Judiciary on November 14, 2007. H.R. 6120 was introduced on May 21, 2007, and referred to the House Committee on the Judiciary; no further action was taken. S. 3016 was introduced on May 14, 2007, and referred to the Senate Committee on the Judiciary; no further action was taken. The bills were substantially similar. H.R. 3577, H.R. 4134, and S. 3016 would have authorized $5,000,000 for educational grants to carry out Internet crime prevention education programs from 2008 through 2012; H.R. 6120 would have authorized $10,000,000 for the time period 2009 through 2013.

[18] U.S.C. 6751 et seq. and 20 U.S.C. 7101 et seq.

impose criminal penalties on anyone who "transmits in interstate or foreign commerce a communication intended to coerce, intimidate, harass, or cause substantial emotional distress to another person, using electronic means to support severe, repeated, and hostile behavior."

Privacy: Disclosure of Text Messages Under Freedom of Information Laws and the Stored Communications Act[19]

Text messages are routinely used to conduct government business. As a result employers, litigants, newspapers, and public interest groups are increasingly seeking access to the contents of such communications in order to shed light on the workings of government. One of the arguments against disclosure of text messages emerging from public officials is that certain delivery platforms or technological devices should, by their very nature, be private because the official owns them, or keeps them in her pocket. Because text messaging represents a relatively new form of electronic communications, state and federal courts are considering requests for access to and disclosure of text messages pursuant to freedom of information and privacy laws.

Courts have begun exploring ways to apply open government laws to text messages. In Texas, a state judge ordered the City of Dallas to turn over e-mails and text messages sent by city officials from personal accounts and personal hand-held devices to conduct city business, and held that the e-mails and messages were subject to disclosure under the Texas Public Information Act."[20]

In Detroit, Michigan, newspapers filed a Freedom of Information Act (FOIA) lawsuit against that city seeking disclosure of text messages sent by Detroit elected officials on city-issued pagers that related to the city's $8.4 million settlement of two whistle-blower lawsuits brought by former Detroit police officers.[21] The city has argued that disclosure of the text messages would violate the federal Stored Communications Act. A public records directive issued by the city states that all electronic communications sent on city equipment "is not considered to be personal or private."[22] Although the newspapers obtained the text messages through an anonymous source, they continue to press for the release of additional information under public records law.[23] A court ruled part of the information the newspapers wanted was public, the Free Press published text messages related to the cover-up and the Mayor and Chief of Staff were charged with eight felonies.[24] The newspapers are continuing to pursue additional information using the state FOIA.

[19] Gina Marie Stevens, Legislative Attorney in the CRS American Law Division, contributed to this section.

[20] Jennifer LaFleur, *Dallas: City Must Provide Messages From Officials' Personal Accounts*, Dallas Morning News, October 30, 2007, available at http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/DN-emails_30met.ART0.State.Edition1.421befa.html.

[21] *Detroit Free Press, Inc., et al. v. City of Detroit*, No. 08-100214 CZ, Wayne County Circuit Court, MI, at http://info.detnews.com/2008/0307motiontocompel.pdf.

[22] On June 26, 2000, Mayor Kilpatrick signed a "Directive for the Use of the City of Detroit's Electronic Communications System."

[23] A "public record" under the Michigan Freedom of Information Act is a writing that is: (1) prepared; (2) owned; (3) used; (4) in the possession of, or (5) retained by a public body in the performance of an official function….. MCL 15.232(e).

[24] For an excellent chronology of developments, see Reporters Committee for Freedom of the Press, at http://www.rcfp.org/newsitems/index.php?key=121&op=keyword.

New York legislators worked to revise the state's open records law to specifically add text messages to the list of records covered.[25] A new Freedom of Information Law became effective in New York on August 7, 2008, and includes provisions which reflect a recognition of advances in information technology, but does not include a provision on text messaging.[26]

Subject to certain exceptions, the Stored Communications Act (SCA), which is part of the Electronic Communications Privacy Act, bars "a person or entity providing an electronic communications service to the public" from knowingly divulging to any person or entity the contents of a communication while in electronic storage by that service." The SCA distinguishes between two types of providers: "remote computing services" and "electronic communications services."

Courts have been examining whether the disclosure of text messages sent by employees on employer-issued pagers violates the privacy rights of employees, and whether such disclosure is barred by the SCA.[27] The Supreme Court considered a lower court's decision that the city of Ontario, CA, police department had violated the rights of Sgt. Jeff Quon by examining the text messages he had sent and received on his department-issued pager. Quon had claimed that the move was a violation of the Fourth Amendment's protection against unreasonable searches. The Supreme Court, however, reversed the lower court's findings and held that Quon should not have assumed the messages "were in all circumstances immune from scrutiny" [28] and that Quon's Fourth Amendment rights had not been violated. The Court also held that the SCA had not been violated.

Using SMS to Support Law Enforcement and Emergency Response

In April 2008, the FCC adopted rules for the Commercial Mobile Alert System (CMAS), which will deliver emergency text messages to the public during emergencies and natural disasters,[29] and recommended that the Federal Emergency Management Agency (FEMA) be the program's aggregator. The program was mandated by the Warning, Alert and Response Network Act that was signed into law in 2006.[30] Under this law, the FCC was required to develop plans for a commercial mobile-alert system through which wireless carriers would voluntarily transmit text

[25] "Battle Over Public Information Expands," by Ledyard King, Federal Times, March 24, 2008, p. 14.

[26] N.Y. Pub. Off. Law § 84 *et seq.* For a summary of the amendments to the Freedom of Information Law, see http://www.dos.state.ny.us/coog/foilnews2.html.

[27] 18 U.S.C. § 2701 *et seq.*

[28] The Court also found that Quon frequently exceeded the monthly limit on texting, and the department's search was prompted by a desire to determine if the limit was too low. Instead, it found the vast majority of Quon's messages were personal, including sexually explicit comments sent to his wife, his mistress and another officer.

[29] Federal Communications Commission, In the Matter of the Commercial Mobile Alert System, First Report and Order, FCC 08-99, PS Docket No. 07-287, April 9, 2008, available online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-99A1.pdf ("Commercial Mobile Alert System, First Report and Order"). See also, FCC Adopts Rules for Delivery of Commerical Mobile Alerts to the Public During Emergencies (FCC 08-99), April 9, 2008, available online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-99A1.pdf. See also the FCC's Consumer Fact Sheet on CMAS at http://www.fcc.gov/cgb/consumerfacts/cmas.html.

[30] Warning, Alert, and Response Network Act, Title VI of the Security and Accountability for Every Port Act of 2006, P.L. 109-347, 120 Stat. 1884 (2006).

messages sent out by the government. The FCC has divided the types of messages the government will send out to mobile-phone users into three broad categories:[31]

- Presidential Alerts deal with national emergencies and will take precedence over any other impending alerts
- Imminent Threat Alerts deal with emergencies that may pose an imminent risk to people's lives or well-being.
- Child Abduction Emergency/AMBER alerts will be related to missing or abducted children.

In addition, the FCC says that all subscribers with roaming agreements will receive timely alerts "provided the subscriber's mobile device is configured for and technically capable of receiving alert messages from the roamed upon network."[32]

The architecture adopted by the FCC calls for a centralized alert-aggregator where federal and state emergency-response agencies would send their warning messages to be authenticated and dispersed to the appropriate participating commercial mobile services. Noting FEMA's role in developing the proposal for the adopted architecture, the FCC recommended the agency as its first choice to serve as the alert aggregator and FEMA has accepted that role

The FCC has issued a Second Report and Further Notice of Proposed Rulemaking;[33] an Order on Reconsideration and Erratum;[34] and a Third Report and Order.[35] Of particular note, in the Third Report and Order, the FCC—

- adopted notification requirements for wireless providers that elect not to participate, or to participate only in part, with respect to new and existing subscribers;
- adopted procedures by which wireless providers may elect to transmit emergency alerts and to withdraw such elections;
- adopted a rule governing the provision of alert opt-out capabilities for subscribers;
- allowed participating wireless providers to recover costs associated with the development and maintenance of equipment supporting the transmission of emergency alerts; and

[31] Commercial Mobile Alert System, First Report and Order, paras. 26-32.

[32] Commercial Mobile Alert System, First Report and Order, para. 79.

[33] Federal Communications Commission, In the Matter of the Commercial Mobile Alert System, Second Report and Further Notice of Proposed Rulemaking , FCC 08-164, PS Docket No. 07-287, July 8, 2008, available online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-164A1.pdf.

[34] Federal Communications Commission, In the Matter of the Commercial Mobile Alert System, Order on Reconsideration and Erratum, FCC 08-166, PS Docket No. 07-287, July 15, 2008, available online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-166A1.pdf.

[35] Federal Communications Commission, In the Matter of the Commercial Mobile Alert System, Third Report and Order, FCC 08-184, PS Docket No. 07-287, July 15, 2008, available online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-184A1.pdf.

- adopted a compliance timeline under which participating wireless providers must begin CMAS deployment.

At this time, the technical standardization process at FEMA is not yet complete and CMAS is, therefore, not operational.

Congressional and Industry Response to SMS-Related Issues

The issues discussed in this report have prompted different levels of response from Congress and the wireless industry:

- Issues that are being addressed by industry, so policymakers may wish to wait and see how those efforts play out;
- Issues that have not risen to a level of priority in Congress, but would require statutory action to effect change; and
- Issues that have triggered a legislative response.

As wireless communications technologies, and the issues that accompany them, evolve over time, so likely will the approaches that industry and Congress will take to ensure consumer safety and satisfaction.

Appendix. Text Blocking with Selected Major Carriers—Information for Consumers

AT&T

Customers must log in at mymessages.wireless.att.com. Text-blocking and alias options are available under "Preferences." Messages from specific e-mail addresses or websites can also be blocked from this page.

Verizon Wireless

Customers must log in at vtext.com. Text blocking options are available under "Text Messaging"/"Preferences." Select "Text Blocking." Consumers may block text messages from e-mail or from the Web, including blocking specific addresses or websites.

Sprint

Customers must log in at http://www.sprint.com. Sprint does not offer auto-blocking, but consumers can block specific phone numbers and addresses. On the top navigation bar, select, "My Online Tools"/"Communication Tools"/"Text Messaging." On the Compose a Text Message page, under Text Messaging Options, select "Settings & Preferences." In the text box, customers can enter a phone number, e-mail address, or domain name to block.

T-Mobile

Customers must log in at http://www.t-mobile.com and select "Communication Tools." T-Mobile doesn't yet offer a "block text messages from the Internet" option. Customers can block all messages sent by e-mail, though, or permit only messages sent to the phone's e-mail address or alias, or create filters that block text messages containing certain phrases.[36]

[36] "How to Block Cellphone Spam," NYTimes.com, Pogue's Posts, June 12, 2008, available online at http://pogue.blogs.nytimes.com/2008/06/12/how-to-block-cellphone-spam/?scp=1&sq=Text%20Blocking&st=cse.

Author Contact Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508