

Text and Multimedia Messaging: Emerging Issues for Congress

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Gina Stevens
Legislative Attorney

May 18, 2011

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

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

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: distracted driving, SMS spam, the inability of consumers to disable text messaging, text messaging price fixing, 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, privacy of text messages, and using SMS to support law enforcement and emergency response.

Contents

Introduction 1
Definitions 1
Short Message Service 1
Enhanced and Multimedia Message Service 1
E-mail-to-SMS Messaging 2
Common Short Codes (CSCs) 2
Issues for Congress 3
Distracted Driving Caused By Texting 4
Legislative Activity 4
Executive Activity 5
SMS Spam 5
Legislative Activity 5
Inability of Consumers to Disable Text Messaging 6
Text Messaging Price Fixing 6
Carrier Blocking of Common Short Code Messages 7
Deceptive and Misleading Common Short Code Programs 7
Protecting Children from Inappropriate Content on Wireless Devices 8
"Sexting" 9
Mobile Cyberbullying 9
Legislative Activity 10
Privacy of Text Messages 10
Using SMS to Support Law Enforcement and Emergency Response 12
Congressional and Industry Response to SMS-Related Issues 14

Figures

Figure 1. Path of Intercarrier SMS Messages 2
Figure 2. Path of Common Short Code Messages 3

Appendixes

Appendix. Text Blocking with Selected Major Carriers—Information for Consumers 16

Contacts

Author Contact Information 17

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

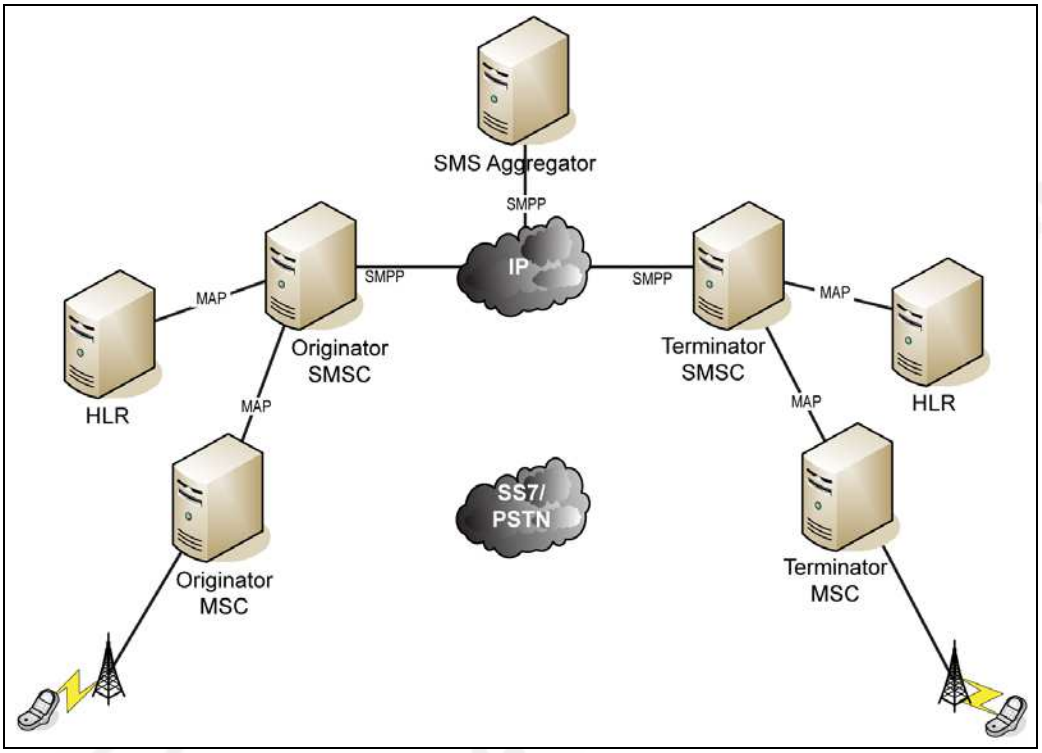
While SMS only allows plain text to be sent, two alternative messaging services allow for more elaborate types of messages. With Enhanced Messaging Service (EMS), formatted text, sound effects, small pictures, and icons can be sent. MMS (Multimedia Messaging Service) allows animations, audio, and video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

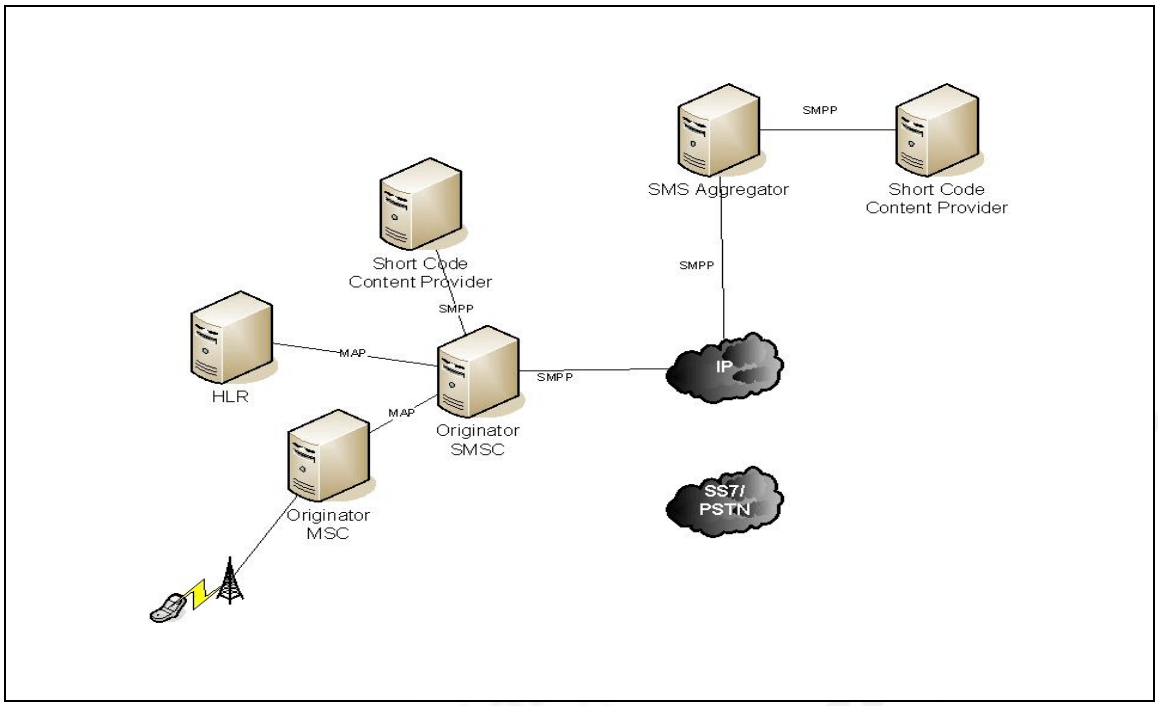


Source: Used with permission from Motorola. Definitions: The "Internet Protocol (IP) cloud" represents an Internet Protocol network used to carry data traffic; HLR = Home Location Register (the central database that contains details of each mobile phone subscriber); MAP = Mobile Application Part signaling 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 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.

[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.

Distracted Driving Caused By Texting

According to the U.S. Department of Transportation, approximately 16% of fatalities in distraction-related crashes were caused in at least some part by mobile devices. Further,

- In 2009, 5,474 people were killed in U.S. roadways and an estimated additional 448,000 were injured in motor vehicle crashes that were reported to have involved distracted driving.
- The age group with the greatest proportion of distracted drivers was the under-20 age group – 16% of all drivers younger than 20 involved in fatal crashes were reported to have been distracted while driving.
- Drivers who use hand-held devices are four times as likely to get into crashes serious enough to injure themselves.
- Using a cell phone while driving, whether it's hand-held or hands-free, delays a driver's reactions as much as having a blood alcohol concentration at the legal limit of 0.08 percent.[4]

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.

Legislative Activity

No legislative activity has been taken in the 112th Congress.

In the 111th Congress, S. 1536 and H.R. 3535, would have amended 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 were called the Avoiding Life-Endangering 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 was 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 was taken.

A bill similar to those discussed above, H.R. 4153, would have amended Title 23, United States Code, to establish national standards to prevent distracted driving. This bill would have required 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 was 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

[4] Official U.S. Government website for Distracted driving, http://www.distraction.gov/stats-and-facts/.

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 took a multi-pronged approach, involving the Secretary of Transportation, National Highway Traffic Safety Administration, and the FCC, to reduce distracted driving. No further action was taken.

As of March 2011, thirty 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). A complete state-by-state listing is available on the National Council of State Legislatures website.[5]

Executive Activity

The 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.

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.

Legislative Activity

No legislative activity has been taken in the 112th Congress.

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 have required 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

[5] Cellular Phone Use While Driving Laws, National Council of State Legislatures, October 2, 2009, http://www.ncsl.org/default.aspx?TabId=17057.

advertisement" to a mobile telephone number that is listed on the FTC's do-not-call registry. No additional action was taken on this bill.

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 have (1) excluded applicability of the law to certain classes of messages (e.g., to facilitate or confirm a commercial transaction); (2) exempted 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) required the FTC to revise the TSR to consider messaging practices that are costly or a nuisance to consumers; and (4) explicitly prohibited, as an abusive telemarketing act, the sending of any message to a mobile telephone number that is listed on the do-not-call registry. No additional action was taken on this bill.

Inability of Consumers to Disable Text Messaging

In the past, some mobile service customers had expressed frustration to their Congressional representatives about unwanted text messages and the inability to selectively block or completely disable text messaging on their phones. Carriers generally offer a range of text messaging packages, for example, 500 messages for $10, but some customers simply do not use text messaging and, therefore, pay a small fee every time they receive a message.

In December 2007, a class-action lawsuit was filed against T-Mobile in this matter.[6] At that time, most carriers already offered some form of text blocking to their customers. The **Appendix** contains information from that article that may be helpful to consumers.[7] In August 2008, T-Mobile began allowing text blocking. At this time, all major carriers provide this service.

Text Messaging Price Fixing

A text message class-action lawsuit has been filed that accuses Verizon Wireless, AT&T, Sprint Nextel, and T-Mobile USA of conspiring to set prices at 10 cents a message, then colluding to increase text message prices by 5 cent increments to 20 cents a message. The companies succeeded in having a prior text message price-fixing class action dropped in December 2009, but the attorney representing the plaintiffs was allowed to refile the case after she found information that a trade association, of which all four wireless providers were members, had held committee discussions on text-message prices. A status hearing on the new text message price-fixing class action lawsuit was held May 18, 2011, in federal court. In 2008, the Antitrust Subcommittee in the Senate Judiciary Committee sent a letter to the big four wireless providers to demand they account for the dramatic price increase for text messages.

[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.

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 "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]

[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.

[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.

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 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 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.

---

[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 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.

"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.

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

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

[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.

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.

Legislative Activity

No legislative activity has been taken in the 112th Congress.

In the 111th Congress, three bills were introduced that related to cyberbullying.

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 have allowed local educational agencies that receives funds under Elementary and Secondary Education Act of 1965[18] to use those funds to develop and implement programs that promote the safe use of the Internet by students, including cyberbullying awareness programs. No further action was taken.

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 have amended the federal criminal code to 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." No further action was taken.

Representative Carolyn McCarthy introduced H.R. 6362, the Safe Schools Against Violence in Education Act, on September 29, 2010; the bill was referred to the House Committee on Education and Labor Subcommittee on Healthy Families and Communities on November 18, 2020. No further action was taken.

The bill would, among other things, have amended the Elementary and Secondary Education Act of 1965 to require states to allow a student who is attending a public school that does not have a safe climate for academic achievement, or who becomes a victim of a violent criminal offense while on school grounds, at a school event, or on a school bus to transfer to a safe public school within the school district.

Privacy of Text Messages[19]

Text messages are routinely used to conduct government business, both officially and unofficially. As a result employers, [20] litigants, newspapers, law enforcement,[21] and public interest groups are increasingly seeking access to the contents of such communications in order to shed light on the

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

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

[20] Lavis, Amanda J., "Employers Cannot Get the Message: Text Messaging and Employee Privacy," 54 Vill. L. Rev. 516 (2009).

[21] Alyssa H. DaCunha, "Txts R Safe 4 2Day: Quon v. Arch Wireless and the Fourth Amendment Applied to Text Messages," 17 Geo. Mason L. Rev. 296 (Fall 2009).

workings of government. Most states have laws "prohibiting public officials from discussing official business privately and failing to disclose information regarding the operations of government." [22] On the other hand, some contend that text messages should be treated as private because of the nature of the delivery platforms or technological devices employed to send text messages. States are increasingly disregarding the public nature of the employee's position and the property ownership of the device used to send e-mail and text messages, and instead defining public communication based on whether the individual is conducting the public's business. Thus, communication about the public's business, and records documenting the communication are a part of the public record. Because text messaging represents a relatively new form of electronic communication, federal and state courts,[23] legislatures,[24] and commissions[25] are considering access to text messages pursuant to Sunshine Laws, Open Meetings Laws, Public Records Acts, Freedom of Information Acts, and electronic surveillance laws.

In Detroit, Michigan, newspapers filed a Michigan 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.[26] The city argued that disclosure of the text messages would violate the federal Stored Communications Act, which outlaws unlawful access to stored communications.[27] 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."[28] Although the newspapers obtained the text messages through an anonymous source, they continued to press for the release of additional information under public records law.[29] 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 and convicted.[30] In Flagg v. City of Detroit,[31] the district court held that a city's text messages satisfied the

---

[22] Cooper, Cheryl, "Sending the Wrong Message: Technology, Sunshine Law, and the Public Record in Florida," 39 Stetson L. Rev. 411, 413 (2009-2010).

[23] See Disclosure of Electronic Data Under State Public Records and Freedom of Information Acts, 54 A.L.R.6th 653.

[24] 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. N.Y. Pub. Off. Law § 84 *et seq.* (McKinney 2009). For a summary of the amendments to the Freedom of Information Law, see http://www.dos.state.ny.us/coog/foilnews2.html. See also "Battle Over Public Information Expands," by Ledyard King, *Federal Times*, March 24, 2008, p. 14.

[25] The Florida Commission on Open Government Reform reviewed open government laws to recommend areas for legislative review and amendment, and found that while e-mail communications between public officials become part of the public record, text or instant messages "most likely" do not. Ibid. at 413.

[26] *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.

[27] 18 U.S.C. § 2701-2708. 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." 18 U.S.C. § 2702(a)(1).

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

[29] 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...." Mich. Comp. Laws Ann. § 15.232(e).

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

[31] 252 F.R.D. 346 (E.D. Mich. 2008) (applying Michigan law).

definition of "public records" under Michigan's Freedom of Information Act (FOIA)[32] because they captured communications among city officials or employees in the performance of an official function. For purposes of the discovery rule governing production of documents, the district court concluded that the city had "control" over any such "public records" in the possession of a third party service provider under contract with the city by virtue of its statutory obligation to maintain these records and make them available for examination or inspection.[33]

Courts also have examined 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 Stored Communications Act (SCA).[34] The United States Supreme Court in *City of Ontario v. Quon* overturned a federal appellate court decision which had held that officials in the City of Ontario, CA, engaged in an unconstitutional search and seizure when they acquired and read the contents of messages sent to and from a city police officer's city-provided pager.[35] In *Quon v. Arch Wireless Operating Company*,[36] the court of appeals for the Ninth Circuit concluded that, under certain circumstances, an employee sending text messages from an employer's device has a reasonable expectation of privacy under the Fourth Amendment. The United States Supreme Court resolved the case by applying settled principles for determining when a search is reasonable.[37] In *City of Ontario v. Quon*, the Supreme Court held that officials had acted reasonably when they reviewed transcripts of messages sent to and from Sergeant Quon's city-issued pager in order to determine whether service limits on the pager's use should be increased. The Court assumed, without deciding, that Quon had a reasonable expectation of privacy for Fourth Amendment purposes, but found that the search of the transcripts was reasonable.

Courts also 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.[38]

Using SMS to Support Law Enforcement and Emergency Response

In May 2011, the FCC and FEMA announced the implementation of a Personal Localized Alerting Network (PLAN). This program was previously called the Commercial Mobile Alert System (CMAS), which has been under development since April 2008 under rules developed by the FCC.

[32] Mich. Comp. Laws Ann. § 15.232(e).

[33] Ibid. at 356.

[34] 18 U.S.C. § 2701 et seq.

[35] *City of Ontario v. Quon,* 130 S.Ct. 2619 (2010), rev'g, *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), cert. granted sub nom., *City of Ontario v. Quon* (Doc. No. 08-1332), 130 S.Ct. 1011 (2009).

[36] 529 F. 3d 892 (9th Cir, 2008) *re'hg. en banc denied,* 554 F. 3d 769 (9th Cir. 2009).

[37] CRS Report R41344, *Public Employees' Right to Privacy in Their Electronic Communications: City of Ontario v. Quon in the Supreme Court*, by Charles Doyle.

[38] 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.

The PLAN system will be operational in Washington, DC, and New York City by the end of 2011 and in the rest of the country by April 2012. PLAN will deliver emergency text messages to the public during emergencies and natural disasters.[39]

The program was mandated by the Warning, Alert and Response Network Act that was signed into law in 2006.[40] Under this law, the FCC was required to develop plans for a commercial mobile-alert system through which wireless carriers would voluntarily transmit text 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:[41]

- 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."[42]

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;[43] an Order on Reconsideration and Erratum;[44] and a Third Report and Order.[45] Of particular note, in the Third Report and Order, the FCC—

---

[39] 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.

[40] 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).

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

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

[43] 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.

[44] 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.

[45] 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 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
- adopted a compliance timeline under which participating wireless providers must begin CMAS deployment.

The FCC continues to refine the rules for providing PLAN/CMAS. The most recent set of requirements is contained in the *Third Report and Order*, released August 7, 2008 (Docket No. 07-287). The WARN Act did not provide a mandatory deadline for the implementation of PLAN/CMAS.

The National Continuity Programs (NCP) Directorate, within the Federal Emergency Management Administration (FEMA), will take on the responsibility of acting as a gateway and aggregator of alerts for dissemination through PLAN/CMAS.[46] On December 7, 2009, FEMA and the FCC jointly announced that FEMA had adopted the CMAS Government Interface Design specifications. This triggered requirements in the *Third Report and Order* for wireless carriers that have agreed to participate in the PLAN/CMAS program to begin development and testing. The deadlines established by the FCC give these carriers until April 7, 2012, to provide PLAN/CMAS alerts sent through the IPAWS gateway.[47] The four major wireless carriers will participate in the program.[48]

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;

[46] "Nationwide Emergency Mobile Telephone Alert System Soon to Be Realized," Press Release, U.S. House of Representatives, Committee on Homeland Security, May 30, 2008.

[47] FCC Public Notice, "FCC's Public Safety and Homeland Security Bureau Sets Timetable in Motion for Commercial Mobile Alert Service Providers to Develop a System that Will Deliver Alerts to Mobile Devices," December 7, 2009, at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-2556A1.pdf.

[48] Daily Report for Executives, "FCC, FEMA Initiate Testing Phase of Wireless Emergency Alert System," by Alexel Alexis, December 8, 2009.

- 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.

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

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.[49]

[49] "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

Gina Stevens
Legislative Attorney
gstevens@crs.loc.gov, 7-2581

GalleryWatch.com
http://www.crsdocuments.com