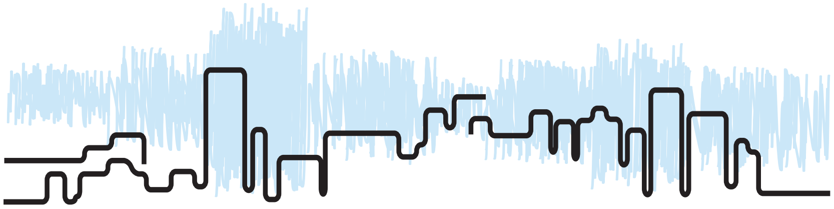
Beyond Voice



Mapping the Mobile Marketplace

Federal Trade Commission
Staff Report

April 2009

Contents

Introduction

Mobile devices, once associated only with voice telephone service, have become the launching pads for new data-driven technologies and services. Today, consumers use their mobile devices for myriad purposes including "chatting" through text messaging, taking pictures, browsing the Web, making purchases, listening to music, viewing videos, playing games across cyberspace, and keeping track of friends and relatives.

To explore these new developments and their impact on mobile commerce ("M-commerce"), the Federal Trade Commission held a public town hall meeting on May 6 and 7, 2008. This town hall meeting, titled "Beyond Voice: Mapping the Mobile Marketplace," follows the FTC's November 2006 forum – "Protecting Consumers in the Next Tech-ade" ("Tech-ade"). Tech-ade participants examined key technological and business developments that will shape consumers' experiences and, thus, consumer protection policy, over the following decade. The FTC's Mobile Town Hall provided the Commission an opportunity for a more in-depth exploration of topics relating to M-commerce.

The Mobile Town Hall reflects the Commission's long-standing interest in educating itself and the public about mobile devices and technology,[1] as well as its interest in ensuring that consumer protection policy is current and relevant. Such interests are a core part of the agency's consumer protection mission.

The Mobile Town Hall consisted of nine sessions, each focused on particular consumer protection issues involving M-commerce.

- Session One panelists addressed the mobile marketplace in the United States. The speakers discussed: (1) the contours of the current mobile marketplace; and (2) factors affecting the adoption of new mobile applications.

- Session Two panelists provided an in-depth look at mobile messaging. Specifically, panelists described: (1) commercial uses of mobile messaging; and (2) consumer protection issues raised by premium rate and unsolicited mobile messaging.

- Session Three panelists distinguished mobile devices from personal computers ("PC") and provided an overview of how mobile devices are becoming powerful tools for consumers.

[1] Indeed, in December 2000, the Commission held a workshop, titled "The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues." At that workshop, panelists provided information about nascent wireless technologies and their effect on privacy, security, advertising and disclosures, and industry self-regulatory programs.

- Session Four panelists addressed location-based services. The panelists discussed: (1) currently available location-based technologies and services; (2) privacy and security issues implicated by the widespread deployment of location-enabled mobile devices; and (3) the responsibility of industry to provide clear notice to and obtain consent from consumers regarding the use of consumer location data.

- Session Five panelists addressed the transition and adaptation of advertising and marketing to mobile devices with particular focus on: (1) the current status of mobile advertising in the U.S.; (2) associated consumer protection and privacy concerns; and (3) predictions regarding the future of mobile advertising.

- Session Six panelists discussed: 1) mechanisms available to consumers to control their mobile devices and the applications that run on those devices; 2) the methods by which consumers are made aware of mobile controls; and 3) recommendations for improving consumer awareness of, and the effectiveness of, mobile controls.

- Session Seven panelists addressed the challenges associated with mobile marketing to children and teens, and methods to help parents manage their children's mobile devices.

- Session Eight panelists addressed the state of industry-developed best practices in the areas of billing, disclosures to consumers, complaint handling, and dispute resolution.

- Session Nine panelists addressed the risks to, and vulnerabilities of, mobile phones to various threats – current and future – as well as precautions consumers can take to protect themselves. The panelists discussed: 1) the stakeholders in the mobile security sphere; 2) mobile security threats and the data at risk from such threats; and 3) the security implications of open platform development, mobile phone recycling, and contactless payments via mobile phones.

Key Findings and Staff Recommendations

It is clear that consumers continue to benefit from the ease and convenience of products and services offered in the highly dynamic mobile marketplace. While the M-commerce industry has made considerable strides in adopting industry-driven best practices in advertising and billing for mobile services, M-commerce presents unique issues for certain segments of the U.S. population, including minors. Collaboration among industry associations, consumer groups, and law enforcement – both domestic and abroad – will be necessary to help prevent unfair and deceptive business practices in the mobile marketplace. Consumer and business education also can play a significant role in empowering consumers as they navigate the ever-evolving mobile marketplace.

Based on these observations, FTC staff has reached several conclusions. First, as to cost disclosures for mobile services, most complaints to state regulatory utilities commissioners involve inadequate disclosures, and recent law enforcement action by the Florida Attorney General highlights this continuing problem. Accordingly, the FTC staff will continue to monitor cost disclosures and bring law enforcement actions as appropriate. The FTC staff will also work with industry on improving its self-regulatory enforcement.

Second, the FTC and its law enforcement partners should continue to monitor the impact on consumers of unwanted mobile text messages, malware, and spyware, and take law enforcement action as needed. Currently, wireless carriers block hundreds of millions of unsolicited text messages every month. The cost to the carriers is substantial, but the cost to consumers of receiving voluminous amounts of unwanted text messages would be far greater. Although spyware and malware have not yet emerged as a significant problem on mobile devices, that situation can change as consumers increasingly use mobile devices for a wide variety of applications, including Internet access. Therefore, FTC staff encourages stakeholders to continue developing strategies that prevent or minimize the spread of spam, spyware, and malware on consumers' mobile devices.

Finally, the increasing use of smartphones to access the mobile web presents unique privacy challenges, especially regarding children. Accordingly, the FTC will expedite the regulatory review of the Children's Online Privacy Protection Rule to determine whether the rule should in any way be modified to address changes in the mobile marketplace. This review, originally set for 2015, instead will commence in 2010, and will provide an opportunity for extensive public comment.

The balance of this report provides a session-by-session summary of each panel that incorporates the panelists' comments, as well as written public comments received in connection with the Mobile Town Hall.[2]

Session One: The Mobile Marketplace – What, How and Who

Session One addressed the mobile marketplace in the United States. The speakers discussed: (1) the contours of the current mobile market place; and (2) factors affecting the adoption of new mobile applications. The speakers were Evan Neufeld, Vice President and Senior Analyst of M:Metrics, and

[2] Panelists' PowerPoint presentations are available at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#May6_08. Comments are available at http://www.ftc.gov/os/comments/mobilevoice/index.shtm. Throughout this report, comments are cited with the name of the submitting party (*e.g.*, Party Name Comments at __). A list of parties who filed written comments is provided in Appendix A. References to the transcript are cited with the name of the commenting party and include a reference to either Day 1 or Day 2 of the transcript (*e.g.*, Panelist, Tr. Day 1 at __). Video webcasts and transcripts for each session are available at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#May6_08 A list of panelists is provided in Appendix B.

Steve Smith, a media critic who works for Mediapost and Access Intelligence. The moderator was Ruth Yodaiken, a senior staff attorney in the FTC's Division of Marketing Practices.

1. The current U.S. mobile marketplace

Steve Smith of Mediapost and Access Intelligence and Evan Neufeld of M:Metrics began Session One by providing an overview of the U.S. mobile marketplace and relevant statistics. Both panelists noted that, according to CTIA - the Wireless Association, there are currently 257 million U.S. mobile subscribers, which translates into a penetration rate of more than 80 percent of the U.S. population.[3] Recent trends suggest that, in the near future, U.S. consumers will more often access the Internet from mobile devices than from PCs.[4] According to Smith, the most notable characteristic of the U.S. market is the interest of mobile users in personalizing their mobile devices and using them for self-expression.[5] The presenters focused their discussion of the current mobile market in the U.S. on three general areas: (1) text messaging; (2) ringtones and ringbacks; and (3) Internet access, mobile television, and new and emerging services.

a. Text messaging

The use of text messaging has exploded in the U.S. and across the globe. According to Neufeld, between 2006 and 2007, messaging usage in the U.S. increased by about 40 percent among wireless subscribers.[6] Additionally, according to Smith, almost 50 percent of U.S. wireless subscribers use text messaging on a regular basis.[7] Smith estimated that 2.3 trillion text messages would be exchanged worldwide in 2008.[8]

Smith opined that text messaging's appeal is that it is private, surreptitious, and personal.[9] Smith further opined that text messaging is the entry point for most commercial mobile services.[10] For example, many TV shows offer viewers the opportunity to vote for a contestant, respond to a trivia quiz, or otherwise communicate with the producers of the show via text message. To illustrate this

[3] Smith, Tr. Day 1 at 16; Neufeld, Tr. Day 1 at 22-23. The CTIA numbers do not take into account the fact that some individuals subscribe to multiple wireless services, and no data were presented to take into account multiple connections or subscriptions associated with the workplace.

[4] Smith, Tr. Day 1 at 18. The terms "mobile device," "mobile phone," and "mobile handset" are used interchangeably througout this report.

[5] *Id*. at 37-38.

[6] Neufeld, Tr. Day 1 at 26.

[7] *Id*. at 23. *See also* American Academy of Pediatrics Comments at 2 (stating that many teens are more likely to use text messaging than phone applications, and that teens and young adults also are much more likely than older adults to use their mobile phones for text promotions, mobile coupons, and mobile search services).

[8] Smith, Tr. Day 1 at 35.

[9] *Id.*

[10] *Id.*

point, Smith pointed out that U.S. viewers of the "American Idol" television show sent 609 million text message votes for their favorite contestants.[11] Smith stated that some TV programmers consider the money they receive from text messaging campaigns to be a significant part of their financial bottom line.[12]

b. Ringtones and ringbacks

The sale of music in the form of ringtones and ringbacks has emerged as a substantial area of M-commerce. A ringtone is the sound made by a phone when it receives an incoming call. A ringback is the sound heard by a person placing a call, before the call is picked up or sent to voicemail.[13] Smith predicted that U.S. consumers will spend about $700 million on ringtones and ringbacks in 2008.[14] As Smith noted, Billboard magazine, which tracks music sales, now has a top-of-the-charts listing for ringtones.[15]

c. The Internet, mobile TV and other services

Only about 10 to 15 percent of wireless subscribers use their mobile devices for Internet browsing.[16] U.S. consumers who use their wireless device to access the Internet appear particularly interested in obtaining information about traffic, restaurants, movies, stock quotes, maps, sports, and weather.[17] Sports information is so commonly accessed through mobile devices that, according to Smith, on Sundays during the 2007-2008 football season, those people who visited ESPN's National Football League webpage were more likely to do so using a mobile web browser than using a personal computer.[18]

There are clear demographic differences among consumers who use mobile devices to access the Internet. Adults in their mid-thirties or younger (especially those under age 25), are much more likely than the rest of the population to access the Internet from their mobile phones.[19] Members of the Hispanic community are more likely than members of other ethnic groups to use mobile browsing and text messaging.[20]

[11] *Id.*

[12] *Id.* (describing how some television programmers generate revenue by including premium text messaging campaigns as an interactive part of their television programs).

[13] Neufeld, Tr. Day 1 at 27-28.

[14] Smith, Tr. Day 1 at 37.

[15] *Id*.

[16] Neufeld, Tr. Day 1 at 26.

[17] *Id*. at 29.

[18] Smith, Tr. Day 1 at 39.

[19] *Id*. at 25, 44.

[20] *Id.* at 44.

Neufeld stated that as the number of mobile devices capable of playing music files (e.g., MP3 files) has increased, so has the number of U.S. subscribers who listen to music on their mobile devices (there has been a 36 percent increase in those listening to music daily using their mobile devices).[21] Mobile subscribers prefer to transfer music onto their mobile devices from their PCs ("sideloading"), rather than downloading it directly onto the mobile device through the Internet.[22]

The use of smartphones – which are mobile phones that offer advanced capabilities beyond a typical mobile phone, often with PC-like functionality – also gives rise to numerous other uses for mobile phones. Consumers use camera and video capabilities to create content that they can then share with others.[23] Although few U.S. consumers watch TV on their mobile devices, the number of wireless subscribers who watch short video clips has grown significantly in recent years.[24] Similarly, mobile instant messaging ("IM") is used by about 9 percent of wireless subscribers, and much of that is the result of very recent growth.[25]

According to Neufeld, one of the most interesting trends occurring in the mobile marketplace is that the mobile phone is evolving into a "viral" medium, meaning that people are passing on mobile technology and information directly to their friends, *e.g.* showing them how to download a new application or sharing a ringtone.[26] (This type of sharing is referred to as "viral" because it is passed from one person to another.)

2. Factors affecting adoption of technology and services, and anticipated changes

According to Neufeld, several factors impact the rate of adoption of different services and technology. First, Neufeld opined that pricing affects adoption, and that consumers are wary of using mobile services, such as text messaging, too often because of high costs for voice and data usage.[27] Neufeld suggested further that the costs of such services will drop in the future, which will likely lead to increased use of data services by U.S. subscribers.[28]

[21] Neufeld, Tr. Day 1 at 30.

[22] *Id.* at 31. Even though many phones are capable of being used to download music from the Internet, Americans are much less likely than people in other countries to download music directly, according to Smith. Smith, Tr. Day 1 at 37.

[23] *Id.* at 25, 28.

[24] *Id*. at 30.

[25] *Id*. at 26.

[26] *Id*. at 26.

[27] *Id*. at 21.

[28] *Id.*

Second, Neufeld observed that as mobile devices themselves evolve, consumers will be more likely to explore and use additional services.[29] According to Neufeld, consumers who have smartphones are four times more likely to use their mobile device for social networking, Internet browsing, and listening to music.[30]

Finally, Neufeld opined that the availability of cheaper and additional bandwidth on mobile devices will lead to an increase in the use of mobile programs and services.[31] These developments already are evident as the third generation phone network ("3G"), which has significant bandwidth, has promoted consumer use of mobile devices for social networking and Internet browsing. Neufeld reported that a consumer with a 3G-capable phone is 1.4 times more likely to use social networking mobile services and even more likely to browse the Internet from a mobile phone.[32] Further, Neufeld predicted that Internet browsing on mobile devices will increase as more people begin to buy and use smartphones with broadband access.[33]

Increased consumer use of mobile devices for Internet browsing leads to increased marketing and advertising opportunities for commercial entities. For example, Smith stated that revenue from non-voice phone use constitutes about 20 percent of the revenue that carriers make from mobile service.[34] This market, because of its high penetration, is very appealing to marketers and advertisers.[35]

Much of the U.S. population is poised for increased participation in the mobile marketplace, according to Neufeld and Smith. However, Smith cautioned that the U.S. mobile marketplace has developed in completely unanticipated ways in the past, and no one can really predict how U.S. subscribers will want to use their mobile devices in the future.[36]

[29] *Id*. at 22.

[30] *Id*. at 31-32 (stating also that while smartphones account for only 6.25 percent of the total U.S. device market, there has been a tremendous increase in usage of smartphones for social networking, browsing and music and video).

[31] *Id*. at 31.

[32] *Id*.

[33] *Id*. at 32-33.

[34] Smith, Tr. Day 1 at 18.

[35] *Id*. at 19.

[36] *Id.* at 38-39. Smith noted that text messaging was conceived of as a quick way for carriers to comunicate with subscribers about problems on the network, and as a way to notify subscribers that they had received voice-mail. *Id.* at 33. Smith also stated that it is surprising that the ringtone and ringback market has taken off in the U.S., while the downloading of music has not.

Session Two: Mobile Messaging – Unsolicited, Premium and Interactive Messaging

Session Two panelists provided an in-depth look at mobile messaging. Specifically, panelists described: (1) commercial uses of mobile messaging; and (2) consumer protection issues raised by premium rate and unsolicited mobile messaging. The panelists for the session were Alykhan Govani, Head of Business Development at MX Telecom; William Haselden, Assistant Attorney General, Office of the Attorney General of Florida; Dorrian Porter, Chief Executive Officer and Founder of Mozes, Inc.; and Leigh Schacter, Senior Litigation Counsel of Verizon Wireless ("Verizon"). Lisa Hone, an Assistant Director in the FTC's Division of Marketing Practices, moderated the panel.

1. Commercial uses of mobile messaging

Alykhan Govani of MX Telecom began the session by providing an introduction to text messaging and its use in M-Commerce. As Govani explained, short messaging service ("SMS" or text messaging) is a tool that enables consumers to create and receive short messages that, in the U.S., consist of no more than 160 characters.[37] According to Govani, text messaging allows marketers to target advertisements to a specific audience, to communicate with their audience in real time and, in some instances, to generate revenue for the advertiser.[38] Text messaging empowers consumers to take action upon seeing an advertisement, whether it be to make a purchase or to sign-up to receive additional information.[39]

Govani offered several examples of text messaging campaigns used by advertisers. For example, a print advertisement can instruct consumers to send a text message to a specific short code, which is a 4- to 6-digit code instead of a 10-digit telephone number. Consumers who use their mobile phone to send a text message to the short code then receive a response with more information. In other instances, consumers can use a short code to order a product or service, such as a food item. According to Govani, there is a movement towards use of Wireless Application Protocol ("WAP") billing or billing through the mobile Internet. In the WAP billing environment, consumers use their mobile devices to make web-based purchases, and can pay through a variety of web-based payment mechanisms. By contrast, consumers using SMS premium billing download or order mobile content by sending a message to a short code. These consumers are then charged on their phone bills. According to Govani, WAP billing is much more common in Europe than in the U.S., provides a better experience for consumers, and reduces consumer complaints. Govani opined that some ringtone providers in the U.S. are moving to WAP billing.[40]

[37] Govani, Tr. Day 1 at 51.

[38] *Id.* at 51-55.

[39] *Id.* at 52.

[40] *Id.* at 58-60.

Govani also described the development of Multi-media Messaging Service ("MMS" messaging). MMS messaging allows users to send and receive images, audio, video, and rich text. Govani provided an example of how consumers are able to use their mobile phones to order personalized photographs that the consumers help to create. In Govani's example, a consumer can insert an image of him or herself into a photo with Kobe Bryant, and download the personalized photograph for a fee.[41] Govani predicts that in the next couple of years, U.S. consumers will be able to take pictures of product bar codes and use that bar code data to shop comparatively for other products.[42]

After Govani finished his overview of SMS and MMS messaging, Dorrian Porter of Mozes described his company's business model and some of the M-Commerce challenges Mozes sees for consumers and industry. As Porter explained, Mozes is a service provider that allows third parties to create interactive mobile campaigns.[43] Currently, Mozes is focused on music, and allows for interactions between musicians and their fans.[44] In 2006, when Mozes launched, it had 70,000 visitors; in the first 6 months of 2008, it had more than 700,000 visitors.[45] Porter demonstrated how Mozes can provide a band with the tools to interact with its fans, by creating a fictitious "FTC band" to which anyone could send a text message that was then displayed on a large projection screen at the workshop.[46]

Porter mentioned consumer "hesitancy" and "distrust" as barriers to the growth of M-Commerce.[47] On the marketing side, he noted that it is still difficult to build compelling marketing campaigns.[48] Porter closed by recommending that industry "embrace long-term value propositions"; that policy makers recognize "how big" M-Commerce is and not limit its growth; and that consumers "look to services that are in [the market] for the long haul."[49]

2. Consumer protection issues

The next two panelists, Will Haselden of the Florida Attorney General's office, and Leigh Schacter of Verizon, focused on spedific consumer protection concerns raised by text messages.

Haselden described the Florida AG's efforts to investigate and bring cases against entities that advertise ringtones and text services, particularly those that use the word "free" or a synonym, to sell

[41] *Id*. at 56.

[42] *Id*.

[43] Porter at 62.

[44] *Id.* at 65.

[45] *Id.*

[46] *Id.* at 66-68.

[47] *Id.* at 63-64.

[48] *Id.* at 64.

[49] *Id.* at 68.

products with a recurring subscription plan.[50] Haselden explained that, under Florida law, advertisers' representations and subsequent disclosures must be easily viewable by consumers. Whether or not the representations and disclosures are easily viewable depends upon a number of factors, including their font size, location, and pixel resolution.[51] Additionally, the representations and disclosures must make it easy for consumers to understand whether a purchase is required for a particular service and the cost of making the purchase. To provide guidance to the industry on disclosures, Haselden described a very specific "zone system" analysis of web pages that offer premium text message services.[52] The first zone has the price and term (*e.g.* $4.99 per month) and needs to be near the PIN code or mobile phone number submit field. The second zone describes what the customer will receive, and the third zone is an age description – because Florida law requires customers under age 18 to have parental permission to make purchases.[53]

Schacter described various methods used by carriers and, in particular, Verizon to attack unsolicited text messaging. As a threshold measure, Verizon filters a massive amount of the unsolicited text messages directed to Verizon's subscribers. According to Schacter, in a typical month, Verizon filters 100-200 million pieces of text message spam, accounting for as much as 70-80 percent of the text messages sent to Verizon subscribers.[54] In addition to blocking spam, Verizon works with law enforcement, including State Attorneys General and the FBI, to track down bad actors.[55] Verizon also brings lawsuits under various statutes, including: the CAN-SPAM Act, which prohibits sending certain unsolicited commercial messages to wireless devices generally; the Computer Fraud and Abuse Act, which prohibits computer hacking and certain other schemes designed to disrupt computer networks; and the Telephone Consumer Protection Act ("TCPA"), which prohibits most telemarketing to mobile phones.[56] Verizon's lawsuits generally seek two types of relief: injunctive relief to stop text spammers from sending additional text message spam; and damages, which under the TCPA, for example, can be as much as $500 per call or per message. Schacter also mentioned that Verizon is interested in engaging in collaborative law enforcement efforts to pursue text message spammers in the U.S. and abroad.[57]

Additionally, Schacter offered a few consumer tips for reducing incoming text message spam. First, Schacter said that consumers can work with their carrier to block all text messages, or block mes-

[50] Haselden, Tr. Day 1 at 69.

[51] *Id*. at 71-75.

[52] "Zones" refer to different portions of mobile advertisements that can be used by an advertiser as opportunities to display, for example, disclosures about service fees, product charges, and terms and conditions.

[53] *Id*. at 74-75.

[54] Schacter, Tr. Day 1 at 80 and 86.

[55] *Id.* at 86.

[56] *Id*. at 84-85.

[57] *Id*. at 90-91.

sages that originate from an email address. Second, Schacter recommended that consumers create a nickname to circumvent spammers who generally send text messages to random phone numbers and not names. For example, instead of using a number, 201-615-XXXX@vtext.com for receiving text messages consumers would use a nickname, such as Leigh@vtext.com. Finally, Schacter warned that a consumer should not distribute his or her cell phone numbers to people not known or trusted by the consumer.[58]

Session Three: Mobile Applications – Games, Widgets and More

Panelists in the third session distinguished the mobile device "ecosystem" – which includes applications, hardware and operating systems – from that of PCs, and provided an overview of how mobile devices are becoming powerful tools for consumers. The speakers were Steve Boom, Senior Vice President of Connected Life, Yahoo! Inc.; Andrew Elliott, Director of Services and Software in North America, Nokia; Thomas C. Ford, Global Market Strategist of Consumer Products, Opera Software; and Rich Miner, General Manager of Mobile Platforms, Google Inc. The moderator was Ruth Yodaiken, a senior staff attorney in the Division of Marketing Practices.

1. Understanding the mobile ecosystem

Steve Boom of Yahoo! launched Session Three by discussing the many ways in which the ecosystem of the mobile device differs from that of the PC. First, the PC ecosystem is far more developed than the growing mobile device ecosystem.[59] The hardware and multiple software applications for PCs have evolved over a longer period of time. As a result, hardware and software designers are more familiar with how PCs work and are able to create new products that will work on many different types of computers.[60] Second, the PC ecosystem is accessible and open to consumers, which allows consumers to build their own websites, for example.[61]

By contrast, the mobile ecosystem is made up of many different devices with widely different processing capabilities (*e.g.*, basic phones, feature phones, and smartphones).[62] Multiple operating systems

[58] *Id.* at 89-90.

[59] Boom, Tr. Day 1 at 99.

[60] *Id.* For example, Boom observed that primarily two PC operating systems exist, and one of those systems, Windows, accounted for approximately 90 percent of the PC market in the past. *Id*. Boom further observed that PC-related hardware is easy to develop because it basically uses a standard keyboard and a mouse, which fundamentally operate in the same way. *Id*. at 100. Additionally, PCs use only a limited number of browsers that function using similar protocols without much variation in computer screen size. As a result, designers are able to easily design hardware and software to accommodate browser functionality. *Id*. at 99-100.

[61] Boom noted that a person can build his or her own website and consumers can access it through the Internet without barriers in the distribution channel. *Id*. at 100.

[62] *Id*. at 101.

exist, some of which are tightly controlled proprietary systems.[63] In addition, more than 20 types of mobile browsers exist, and multiple versions of a browser application are not uncommon.[64] Hardware, including screens, varies (*e.g.*, manufacturers have recently developed a "touch-screen").[65] There even can be different implementations of Java – a well-known programming language – so that an application written in Java for one mobile device may not function the same way, or at all, on another mobile device even though the second device runs Java.[66] Thomas C. Ford of Opera Software asserted that because of this issue with Java, Opera Software has had to have a fairly sophisticated tool on its website to help users determine which version of its software will work on the user's phone.[67]

In addition to these compatibility issues, service operators in the U.S. control what information subscribers can access.[68] Rich Miner of Google noted that it is nearly impossible for software developers to get their applications on a mobile handset today.[69] Miner opined that carriers and handset manufacturers impose complex procedures for placing applications on handsets.[70] Thus, most mobile phones are described as having a "closed" platform. Miner claimed that closed platforms can stifle innovation.[71]

2. Applications shaping modern mobile technology

Despite these challenges, a growing number of applications already have been developed or modified to work in the complex mobile ecosystem, and the variety is expected to increase in the future. As noted by panelists in Session One, the evolution of the mobile browser – itself a type of application – is allowing for web exploration, and is being used as a platform for a variety of applications, such as mobile email access and instant messaging. The consumer experience, however, varies based on whether the consumer is using a smartphone or a phone with lesser capabilities.

a. Internet browsing

In the U.S., Internet browsers on mobile devices with lesser capabilities than those of smartphones typically allow users only to see webpages that use a text-based system. Ford claimed that because of

[63] *Id*.

[64] *Id*. at 101-102.

[65] *Id*.

[66] Miner, Tr. Day 1 at 145.

[67] See Opera Comments at 1 (discussing Opera Mini, the first browser that could work on any phone with Java, regardless of the hardware on the phone).

[68] Boom, Tr. Day 1 at 102.

[69] Miner, Tr. Day 1 at 139.

[70] *Id*.

[71] *Id*. at 140.

this limitation, mobile web adoption in the U.S. in past years has not been as robust as it could have been.[72]

On the other hand, Ford noted that as mobile phones and mobile phone browsers are becoming more powerful, consumers expect browsing the Internet on a mobile device to be like browsing on a PC screen.[73] Ford referred to this concept of being able to access similar material and formats on different devices as the "one web" concept.[74]

Many industry players are attempting to meet consumers' growing expectations for "one web" accessibility. For example, Ford noted that for more powerful mobile devices, such as smartphones, Opera Software has a more powerful browser that enables consumers to access many web functions.[75] But for less powerful phones, Opera Software uses a special server that acts as a go-between as the phone attempts to surf the Internet.[76] The server retrieves the Internet material and reduces it in the display sent to the phone.[77] The end result is that, increasingly, mobile web browsers allow consumers using mobile devices to do many of the things they can do with a PC, such as banking, shopping, and checking email.[78]

b. Software development kits – user generated phone evolution

According to Boom, for Internet browsing to take off on mobile devices, it must be possible for many developers – not just large companies – to produce applications that can be run on a variety of devices.[79] For example, Yahoo! has attempted to support the creation of applications that work on different types of operating systems by creating widgets (software) that enable third parties to develop their own software to work across hundreds of different types of mobile devices.[80] The developer creates applications by downloading a Software Development Kit that uses Yahoo!'s Blueprint language, and creates his or her own program.[81] A consumer is then able to use the applications created by these

[72] Ford, Tr. Day 1 at 107.

[73] *Id*. at 106-07.

[74] *Id*. at 106.

[75] *Id*. at 107-08.

[76] *Id*. at 108.

[77] *Id*.

[78] *Id*. at 109, 111.

[79] Boom, Tr. Day 1 at 113-14.

[80] *Id*. at 114-15.

[81] *Id*. at 115.

developers by using a mobile Internet browser to reach Yahoo! Go's website, downloading a program (a Java application), and selecting which applications he or she wants to use.[82]

c. Games

Andrew Elliott of Nokia discussed how mobile browser-based platforms also are being used to support online games on mobile devices. For example, Nokia, which sells many mobile devices around the world, has developed OVI, a mobile browser-based platform for accessing a variety of applications and services, including games.[83] These types of capabilities greatly expand consumers' access to content on their mobile phones.

3. Looking ahead – harnessing new power of mobile devices

All of the capabilities described above highlight one key point – mobile devices are becoming powerful tools for consumers. Miner noted, however, that several factors limit the full functionality of these devices for consumers.

First, Miner opined that the cost of the software that is incorporated into mobile handsets has been rising, thus keeping the cost of the handsets high. Miner recommended that manufacturers reduce software costs by making software applications open source.[84]

Second, Miner observed that most people do not treat mobile devices like PCs because, in addition to small screens and keyboards, other barriers keep the mobile platform closed.[85] For example, a consumer using a mobile device can search for a restaurant, add the restaurant's address and phone number to the device's address book, and call the restaurant.[86] With closed-system devices, however, the address book resides in an environment separate from the Internet map-searching features.[87] As a result, consumers using a closed system cannot move an address from a map program into their address book.[88] According to Miner, an open system would allow for the development of search and address book applications that can work with each other. Miner encouraged software companies to work

[82] *Id.* at 117. Examples of widgets include those that download a daily cartoon, access sports scores, access email, and access photo websites for uploading photos. *Id.* at 116-19. The applications also allow for access to eBay. *Id.* at 120-21. Boom says that these widgets currently allow for such types of functionality on lower end phones as well as the higher end ones. *Id.* at 121.

[83] Elliott, Tr. Day 1 at 123.

[84] Miner, Tr. Day 1 at 136-37. Open source software has many characteristics, including free licensing and free redistribution. The Open Source Initiative (OSI) provides a definition of open source software at http://www.opensource.org/docs/definition.php.

[85] *Id.* at 137-39.

[86] *Id.* at 141-42.

[87] *Id.* at 142.

[88] *Id.*

toward opening up the mobile ecosystem to increase consumer access to online and other content on their mobile devices.

Session Four: Location-Based Services

Session Four panelists addressed location-based services. The panelists discussed: (1) currently available location-based technologies and services; (2) privacy and security issues implicated by the widespread deployment of location-enabled mobile devices; and (3) the responsibility of industry to provide clear notice to and obtain consent from consumers regarding the use of consumer location data. The panelists for the session were Brian Knapp, Chief Privacy Officer and Vice President of Corporate Affairs for Loopt, Inc.; Michael Altschul, Senior Vice President and General Counsel of CTIA-The Wireless Association ("CTIA"); Alissa Cooper, Chief Computer Scientist at the Center for Democracy and Technology ("CDT"); Tony Bernard, Vice President of Operations for Useful Networks, Inc.; Tim Lordan, Executive Director of the Internet Education Foundation; and Fran Maier, Executive Director and President of TRUSTe. Rick Quaresima, an Assistant Director in the Division of Advertising Practices, and Peder Magee, a senior staff attorney in the Division of Privacy and Identity Protection, co-moderated this panel.

1. Current location-based technologies and services

Brian Knapp of Loopt began Session Four by providing an overview of the various technologies used to determine mobile devices' locations.[89] As Knapp explained, due to a combination of market forces and the implementation of the Federal Communications Commission's ("FCC's") Emergency-911 requirements,[90] virtually all mobile devices transmit signals that enable mobile carriers or others to determine the devices' approximate locations at any time.[91] Knapp noted that the use of assisted global positioning systems ("AGPS") is currently the most common method of determining mobile devices' locations in the U.S.,[92] and that determining location via signals that mobile devices send to base stations or cell towers is a rapidly growing practice.[93]

Panelists also discussed the most common consumer uses of location information. Family and friend finder applications that enable users to determine their family members' and friends' locations are among the most well-known and widely used location-based applications.[94] Knapp explained that previous versions of friend finder applications relied on the consumers to input their location informa-

[89] Knapp, Tr. Day 1 at 163-68.

[90] *Id.* 162, 165.

[91] Cooper, Tr. Day 1 at 177-78.

[92] *Id.* at 165.

[93] *Id.* at 163-64.

[94] *Id.* at 159; Bernard, Tr. Day 1 at 183.

tion manually on their mobile devices, while newer versions (including the service provided by Knapp's employer, Loopt) use the information transmitted by the mobile devices to update location continually and automatically.[95] Other common mobile location applications include mapping, social networking, local searching, and gaming.[96]

The panel discussion also touched upon the use of location information to target advertising to consumers. Currently, location-enhanced targeting of advertising largely relies on consumers inputting their location information into their mobile devices manually. Knapp opined that automatically transmitted location information will be used to target advertising to consumers in the near future.[97] None of the panelists provided a current example of an advertising campaign that uses automatically generated location information.

2. Privacy and security issues

Most of the panel discussion focused on the numerous privacy and security issues associated with collecting and disclosing consumer location data.[98] The panelists unanimously agreed that generation of location data by consumers' use of mobile devices raises serious privacy issues. Alissa Cooper of CDT underscored the ubiquitous nature of location data by contrasting mobile devices' automatic generation and transmission of consumers' location information with the generation of other types of data, such as cookies or telephone call logs, which occur only when a consumer performs an action, such as visiting a website or placing a telephone call.[99] Tim Lordan of the Internet Education Foundation discussed a January 2008 poll in which more consumers cited privacy concerns regarding the sharing of their location information than with any other category of information included within the poll.[100] Fran Maier of TRUSTe expressed concern that, as a general matter, consumers are confused as to who controls their location data and who they need to contact to control the use of the data.[101]

[95] Knapp, Tr. Day 1 at 160.

[96] *Id.* at 158-59, 216; Bernard, Tr. Day 1 at 183.

[97] Knapp, Tr. Day 1 at 162, 166, 215-16.

[98] Written comments submitted to the Commission also addressed this issue. *See e.g.*, Hoofnagle Comments (providing survey data to suggest that a supermajority of Californians support limits on law enforcement access to mobile phone location information); CDT Comments (discussing the IETF's Geographic/Location Privacy working group, which has created a set of standards for sending location information coupled with privacy rules for the Internet); Rudolph Comments at 1 (describing concerns about the use of mobile phones for tracking and location services).

[99] Cooper, Tr. Day 1 at 176-77. Cooper cited recent research that found that many consumers do not realize that their mobile devices transmit information that could enable recipients of the information to track them. *Id*. at 177-78.

[100] Lordan, Tr. Day 1 at 189.

[101] Maier, Tr. Day 1 at 194. For example, when a consumer uses a mapping application on a mobile device, the consumer may not know whether the mobile phone carrier, the publisher of the mapping application, or some other party controls the usage and storage of that location data. Maier, Tr. Day 1 at 194-95.

Cooper noted that, in CDT's comments to the FTC regarding behavioral targeting in online advertising, CDT has advocated that location information be classified as sensitive data that receive special protection.[102] By way of example, she stated that unauthorized access to a consumer's location information may reveal potentially sensitive information, such as the consumer's visit to a medical clinic or a government building.[103] Other panelists similarly underscored the issue of consumers' control over the use and disclosure of their location information by pointing out that consumers' inability to control access to the information could lead to dangers like a stalker accessing and using the information.[104]

a. Statutory privacy protections

Several panelists stated their belief that current laws and regulations regarding the disclosure of consumers' location data may be insufficient. In particular, panelists discussed the Customer Proprietary Network Information ("CPNI") rules set forth in Section 222 of the Telecommunications Act of 1934 to protect the confidentiality of certain categories of data contained within consumers' telecommunications service records. With limited exceptions, the CPNI rules require telecommunications carriers to obtain consumers' authorization before the carriers can disclose the protected data.

Location information is one of the categories of information that the CPNI rules protect.[105] Panelists noted, however, that the CPNI rules apply only to telecommunications carriers and not to the numerous non-carriers, such as providers of mapping applications or GPS applications in automobiles, that may offer location-enhanced services without relying on the carriers or the carriers' networks.[106] Furthermore, some panelists questioned whether the CPNI rules apply when a mobile carrier provides a consumer's location information to a third-party location-based application provider.[107] Michael Altschul of CTIA also noted that the CPNI rules provide protection only to the account holder, who may, in fact, be different from the user of the mobile device whose location information is at issue.[108]

Cooper expressed concern that no statute explicitly states what standard the government must meet to obtain either real-time or historical consumer location data.[109] She noted that, consequently, federal magistrate judges have disagreed as to whether the government needs a probable cause warrant

[102] Cooper, Tr. Day 1 at 176.

[103] *Id*. at 177.

[104] *Id.*; Knapp, Tr. Day 1 at 161; Maier, Tr. Day 1 at 194.

[105] 47 U.S.C. § 222(f), (h)(1).

[106] Altschul, Tr. Day 1 at 170; Cooper, Tr. Day 1 at 178.

[107] *Id.*

[108] Altschul, Tr. Day 1 at 170-71, 197-99, 211, 214.

[109] Cooper, Tr. Day 1 at 179-80.

to access location data.[110] She stated CDT's belief that the government should be required to obtain a probable cause warrant before it can acquire either real-time or historical location data.[111]

Other panelists disagreed that additional laws are needed to control access to location data. Knapp stated his view that a "patchwork of regulation," including the FTC Act and the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.*, already applies to location data.[112] Other panelists similarly counseled against the creation of new laws.[113] Lordan expressed concern that some existing international legal requirements may threaten consumer privacy rather than protect it. In particular, he noted that the European Union's Data Retention Directive requires the retention of mobile calling records, including location data, for up to two years.[114]

b. Self-regulation and best practices to protect privacy

Panelists discussed the importance of self-regulation and best practices to protect consumer privacy regarding location data.[115] For example, Altschul discussed the CTIA's recently issued *Best Practices and Guidelines for Location-Based Services*.[116] He opined that the guidelines provide needed flexibility for a nascent industry while also providing ample protection for consumers.[117] In particular, he noted that the guidelines draw heavily on the FTC's "two pillars" of consumer privacy: user notice and consent.[118] He also discussed the need for location-based service providers to develop business practices for retaining consumers' location information only as long as the service providers need it to provide the particular services that consumers have authorized.[119]

Maier mentioned TRUSTe's release of mobile industry guidelines in 2004. In addition, she stated that TRUSTe is exploring the possibility of creating a new program under which it would enable mo-

[110] Cooper, Tr. Day 1 at 180.

[111] *Id*. Cooper also suggested that the U.S. should adopt a baseline comprehensive privacy statute that would apply across industry sectors. *Id.* at 209-10. She observed that the U.S. currently has different privacy laws for different sectors so that, for example, consumers' video rental records receive different privacy protections than do their cable television records. *Id*. at 210.

[112] Knapp, Tr. Day 1 at 208-09.

[113] Bernard, Tr. Day 1 at 211; Maier, Tr. Day 1 at 211-12.

[114] Lordan, Tr. Day 1 at 188.

[115] Knapp, Tr. Day 1 at 197; Bernard, Tr. Day 1 at 211; Maier, Tr. Day 1 at 211-12.

[116] Altschul, Tr. Day 1 at 169. (A copy of these guidelines is provided in CTIA's Comments. CTIA Comments at Att. A.)

[117] *Id*. at 173-74.

[118] *Id*. at 174.

[119] *Id*.

bile service providers to use the TRUSTe seal if TRUSTe determines that they follow certain practices to protect consumers' privacy interests.[120]

3. Challenge of providing notice and consent

In accord with the CTIA's recently issued guidance, all the panelists agreed that service providers should provide appropriate notice to and obtain consent from consumers of location-enhanced services. Likewise, the panelists noted the challenges in providing that notice and obtaining that consent.

Several panelists agreed that the methods for providing notice and obtaining consent likely should vary depending on the nature of the particular location-based service at issue. For example, according to the panelists, notice and the ability to opt out may provide adequate consumer protections when it comes to using a consumer's location information to determine which banner advertisement the consumer receives when the consumer uses a mobile device to access a webpage. On the other hand, consumers may expect a more robust notice provision and an opt-in process to consent to their location information being disclosed to other individuals as part of a family or friend finder application.[121] Rather than a one-time privacy notice, consumers may also expect recurring notices when it comes to sharing their location information for certain types of services.[122]

Tony Bernard of Useful Networks noted that some countries have enacted laws that require providers of family or friend finder applications to offer consumers the choice of receiving periodic notices reminding them who can receive their location information through the applications.[123] He explained that, as an aggregator in the location-based services market, Useful Networks runs a server-based application that enables location-based service providers to customize settings to determine how often they provide notice to and seek consent from consumers regarding location information usage and storage practices.[124] He discussed Useful Networks' own practice of sending text messages each month to remind users of its friend finder application and that they have consented to share their location information with their peers.[125] Knapp stated that some consumers have expressed annoyance when they have received such reminder messages.[126]

Panelists highlighted the special concerns of notice and consent when children are the ones using location-based services. Altschul noted that when a parent provides a mobile device to a child (or an

[120] Maier, Tr. Day 1 at 195, 201.

[121] *Id*. at 200.

[122] *Id*. at 202.

[123] Bernard, Tr. Day 1 at 202-03.

[124] *Id*. at 184-85.

[125] *Id*. at 202.

[126] Knapp, Tr. Day 1 at 204.

employer provides a mobile device to an employee), the mobile account holder rather than the potential location-based service user may be the appropriate person to consent to the use of a location-based service or to the disclosure of location information.[127]

Session Five: Mobile Advertising and Marketing – The Transition and Adaptation to Mobile Devices and the Small Screen

Session Five panelists addressed the transition and adaptation of advertising and marketing to mobile devices with particular focus on: (1) the current status of mobile advertising in the U.S.; (2) associated consumer protection and privacy concerns; and (3) predictions regarding the future of mobile advertising. The panelists for the session were Hairong Li, Associate Professor of Advertising at Michigan State University; Michael Hanley, Assistant Professor of Advertising at Ball State University and Co-Chair of the Mobile Marketing Association's Academic Outreach Committee; Ben Ezrick, Senior Strategist of Digital Innovation at Ogilvy Interactive; Jean Berberich, Digital Marketing Innovation Manager for Mobile at Procter & Gamble; Jim Durrell, Director of Product Management for Greystripe; Jeff Chester, Executive Director of the Center for Digital Democracy ("CDD"); Gene Keenan, Vice President of Mobile Services at Isobar Global; Susan Duarte, Counsel for Marketing Practices at Sprint Nextel Corp.; and Marci Troutman, Founder of Siteminis, Inc. Mary K. Engle, Associate Director of the Division of Advertising Practices, and James Trilling, a senior staff attorney in the Division of Advertising Practices, moderated this panel.

1. Current status of mobile advertising

The panelists began by providing an overview of the current status of mobile advertising. Several panelists opined that, contrary to widespread projections, mobile advertising in the U.S. remains in a nascent stage.[128] Panelists noted that mobile advertising is more prevalent in Asian countries than in the U.S.[129] Panelists predicted a number of changes in the U.S. that may contribute to a narrowing of this gap in the future: (1) wider deployment of smartphones that make it easier for consumers to access and use the Internet and ad-supported content; (2) wider consumer enrollment in billing plans that provide consumers free or flat-rate access to unlimited amounts of data via their mobile phones; and (3) deployment of quick response ("QR") code readers on mobile phones.[130]

[127] Altschul, Tr. Day 1 at 171.

[128] Li, Tr. Day 1 at 224; Hanley, Tr. Day 1 at 231, 233; Berberich, Tr. Day 1 at 248.

[129] Li, Tr. Day 1 at 225, Berberich, Tr. Day 1 at 248.

[130] Ezrick, Tr. Day 1 at 240, 242; Li, Tr. Day 1 at 283; Kennan, Tr. Day 1 at 283-84.

Panelists stated that mobile advertising campaigns are usually just one component of an integrated campaign that involves multiple modes of advertising.[131] In addition, panelists noted that SMS text messaging has been the predominant form of mobile advertising in the U.S. to date.[132] By way of example, Jean Berberich of Procter & Gamble discussed the company's "text club" for its Cover Girl product line.[133] The company advertises the text messaging club in media such as websites and magazines.[134] After seeing one of the advertisements for the text message club, a consumer can send a text message to a short code to begin a double opt-in process required to join the club.[135] Procter & Gamble then sends a text message response to the consumer to indicate approximately how many text messages the company will send the consumer each month and asking whether the consumer agrees to receive the messages.[136] The consumer can opt in a second time – thereby becoming part of the text messaging program – by responding "yes" that the consumer agrees to receive the text messages.[137]

Despite the limited range of mobile advertising thus far, the panelists reported that mobile advertising already produces strong results in terms of building brand awareness, increasing consumers' stated intent to buy the advertised products, and prompting consumers to take certain responsive actions such as providing their email addresses or clicking a link to a webpage.[138] By way of example, Ben Ezrick of Ogilvy Interactive discussed advertisements that the company created and placed on mobile Internet websites for a producer of laptop computers.[139] Ezrick stated that brand awareness increased 188 percent among consumers who saw the advertisements and almost 500 percent among consumers who clicked on them.[140] He also noted that consumers who clicked on the advertisements had the opportunity to provide their email addresses in order to be contacted with additional information regarding the sale described in the advertisements.[141]

Because many consumers carry their mobile devices with them at all times, the panelists reported that advertisers see great potential in being able to use mobile devices to provide consumers with real-time, relevant information about products and services.[142] At the same time, the panelists stated that

[131] Ezrick, Tr. Day 1 at 245-46; Berberich, Tr. Day 1 at 247; Keenan, Tr. Day 1 at 280.

[132] Ezrick, Tr. Day 1 at 241.

[133] Berberich, Tr. Day 1 at 250-51.

[134] *Id*. at 251.

[135] *Id.* at 249.

[136] *Id.* at 250.

[137] *Id.*

[138] Ezrick, Tr. Day 1 at 243; Durrell, Tr. Day 1 at 261.

[139] Ezrick, Tr. Day 1 at 242-43.

[140] *Id.* at 243.

[141] *Id.*

[142] Berberich, Tr. Day 1 at 247-248.

advertisers recognize that consumers consider their mobile devices to be personal, private devices.[143] For that reason, the panelists widely agreed that it is important for consumers to have the ability to opt in and opt out of mobile advertising.[144] Gene Keenan of Isobar Global touted the Mobile Marketing Association's ("MMA") mobile advertising guidelines regarding opt-in and opt-out processes for consumers' participation in text message campaigns.[145] Among other things, those guidelines call for advertisers to require consumers to complete a double opt-in process in order to enroll in a text messaging campaign.[146]

Several panelists identified the use of incentives, such as coupons or ad-supported content, as a key factor that drives or will drive consumer acceptance of advertisements on their mobile devices.[147] Michael Hanley of Ball State University discussed his research regarding college students' acceptance of mobile advertising.[148] Hanley recently concluded that approximately two-thirds of college students are willing to accept advertisements on their mobile devices if the advertisements include incentives such as coupons that are relevant to the college students' lives.[149] Similarly, Ezrick reported that one of Ogilvy's clients recently experienced a high response rate when it ran an advertising campaign that provided consumers the opportunity to send a text message to a short code in order to receive a discount coupon for the client's products.[150] Ezrick stated that the rate of consumers who sent a text message to obtain the coupon was six times higher than the rate of consumers who called a toll-free telephone number or visited an Internet website to obtain it.[151] Jim Durrell of Greystripe rounded out the discussion regarding incentives by explaining his company's business model of providing consumers the ability to download free, ad-supported games to their mobile devices.[152]

2. Privacy and other concerns

Jeff Chester of the CDD stated that mobile advertising raises privacy and other concerns similar to those that individuals and groups such as the CDD have enumerated with respect to Internet advertising on PCs.[153] He pointed out that certain demographic groups, such as young consumers, Hispanic

[143] Li, Tr. Day 1 at 229; Hanley, Tr. Day 1 at 231; Keenan, Tr. Day 1 at 270.

[144] Berberich, Tr. Day 1 at 249; Keenan, Tr. Day 1 at 271.

[145] Keenan, Tr. Day 1 at 270-71.

[146] The MMA's mobile advertising guidelines are discussed *infra* at 29.

[147] Li, Tr. Day 1 at 224, 229-30; Hanley, Tr. Day 1 at 235-36.

[148] Hanley, Tr. Day 1 at 234.

[149] *Id*. at 236.

[150] Ezrick, Tr. Day 1 at 244.

[151] *Id*.

[152] Durrell, Tr. Day 1 at 255-56.

[153] Chester, Tr. Day 1 at 266.

consumers, and African-American consumers are target markets for mobile advertisements.[154] He associated tracking, profiling, behavioral targeting, and impulse buying with mobile advertising.[155] He also stated that mobile advertising is linked to childhood obesity.[156] He further stated that advertisers' access to, and use of, consumers' location information raises special privacy concerns.[157] In light of these numerous consumer protection concerns, he called for the creation of additional mobile advertising standards to address consumer privacy, autonomy, and "special issues."[158] He urged that consumer groups, privacy groups, children's health groups, civil rights groups, and government participate in creating such standards.[159]

Other panelists disagreed, stating their belief that mobile advertising raises fewer privacy and consumer protection concerns than advertising on PCs. Durrell acknowledged that mobile carriers possess personal information about consumers, such as their mobile phone numbers, demographic information, and information regarding the amount that consumers pay for their mobile phone usage.[160] He stated, however, that other companies involved in mobile advertising and M-commerce do not have access to that same information. As an example, he stated that Greystripe generally learns the type of mobile device that its customers are using but does not learn any personal information about the consumers. Ezrick similarly stated that the receipt of mobile advertisements generally enables customers to receive free content or information without giving up any personal information.[161] Some panelists further stated that the website banner advertisements that consumers access with their mobile devices are targeted solely by context, such as the subject matter of the particular website a consumer visits, rather than on the basis of any personal information about the consumer.[162]

Keenan rejected the call for additional regulations and opined that the MMA's guidelines provide significant consumer protections.[163] He also professed that mobile industry participants' interest in customer retention provides strong incentives to respect consumers' interests in privacy and autonomy.[164] Similarly, Susan Duarte of Sprint Nextel stated that mobile carriers' interest in providing

[154] *Id.* at 264-65, 267, 276.

[155] *Id*. at 265, 281.

[156] *Id*. at 265.

[157] *Id.* at 265, 280.

[158] *Id.* at 268.

[159] *Id.* at 267-69, 276, 290.

[160] Durrell, Tr. Day 1 at 258.

[161] Ezrick, Tr. Day 1 at 277.

[162] *Id.*; Keenan, Tr. Day 1 at 281.

[163] Keenan, Tr. Day 1 at 270.

[164] *Id.* at 270-71.

positive consumer experiences so that they retain customers has caused the carriers to act cautiously with respect to permitting mobile advertising.[165]

3. The future of mobile advertising

While SMS text messaging is the predominant form of mobile advertising in the U.S. today, the panelists believed that other forms of mobile advertising, such as MMS messaging, likely will become more prevalent after more U.S. consumers buy more sophisticated mobile devices and subscribe to more robust mobile data plans.[166] Marci Troutman of Siteminis further opined that technological improvements that allow data to load and display more quickly on mobile devices also may facilitate more mobile advertising in the future.[167] Chester projected that ad-supported mobile content will become more predominant in the future.[168]

In looking toward the future of mobile advertising in the U.S., Hairong Li of Michigan State University discussed quick response ("QR") codes – a type of two-dimensional bar code – currently used in mobile marketing campaigns in Japan and other Asian countries.[169] Li noted that QR-enabled mobile phones in Japan allow consumers to scan optically and decode QR codes that are placed on items such as restaurant menus, posters, billboards, and other advertisements, and thereby receive coupons, product information, and other data on their mobile devices quickly and easily.[170]

Session Six: Managing Your Mobile Device

Session Six panelists discussed: 1) mechanisms available to consumers to control their mobile devices and the applications that run on those devices; 2) the methods by which consumers are made aware of mobile controls; and 3) recommendations for improving consumer awareness of, and the effectiveness of, mobile controls. The panelists were Mike Bennett, Executive Director of Consumer, State, and Local Government Affairs for AT&T Services, Inc.; Laurie Itkin, Director of Government Affairs for Cricket Communications and its parent company, Leap Wireless; and Susan Grant, Director of Consumer Protection for the Consumer Federation of America. Robert Schoshinski, a senior staff attorney in the Division of Marketing Practices, moderated the panel.

[165] Duarte, Tr. Day 1 at 274-75, 286.

[166] Ezrick, Tr. Day 1 at 239-40; Li, Tr. Day 1 at 283; Keenan, Tr. Day 1 at 283. See the summary of the Second Panel for a discussion of SMS and MMS messaging.

[167] Troutman, Tr. Day 1 at 273-74.

[168] Chester, Tr. Day 1 at 276, 284-85.

[169] Li, Tr. Day 1 at 226.

[170] *Id*. at 226-28.

1. Mobile Control Mechanisms

a. Controls that block or limit certain functions

Mike Bennett of AT&T opened the panel by discussing controls for mobile phones that block or limit certain functions.[171] Although such controls are often designed and marketed as parental controls for mobile devices used by underage family members, individual mobile consumers also use such controls to manage their devices.[172]

For example, Bennett described how the number of text messages sent or received by a mobile device can be controlled.[173] Mobile carriers offer a variety of text messaging plans, including: unlimited plans; plans that allow a specified number of messages per month without any additional charge; and plans in which subscribers pay a fee for each text message they send or receive.[174] Consumers who have text messaging plans that do not allow unlimited messages often wish to restrict the number of messages they send or receive in a month in order to prevent unexpectedly high text messaging fees.[175] One option available to consumers who wish to avoid such fees is a control that turns off the ability of their mobile device to send or receive any text messages whatsoever.[176] For consumers who wish to use the text messaging functions of their mobile devices, many service providers offer controls that limit the number of text messages that a mobile device sends or receives in a month. When the device reaches the pre-set limit on text messages, its ability to send or receive such messages is turned off.[177] Along with such controls, many carriers offer subscribers the ability to monitor or be notified of their text messaging usage on a real-time basis.

As more mobile devices become capable of web browsing, some service providers also are offering controls on the ability of a mobile device to access the Internet. Web browsing controls currently offered include content filtering, blocking access to certain sites, allowing access only to certain sites, and completely disabling the web browsing capability of a mobile device.[178]

[171] Bennett, Tr. Day 2 at 9, 10.

[172] *Id.* at 12.

[173] *Id.*

[174] *Id*.

[175] *Id*.

[176] *Id.* at 13.

[177] *Id*. at 12.

[178] *Id.* at 10.

b. Controls that limit purchases

Consumers can access a broad range of services and content through their mobile devices. Many of the services and content available through mobile devices also can be billed to a consumer through the consumer's mobile carrier. Many mobile carriers provide controls that enable their subscribers to manage the number of purchases or amount of charges that their subscribers' mobile devices can incur in a billing period. These controls include pre-set limits on the amount of purchases or charges that a device may accrue, as well as pre-paid service plans that do not allow any further purchases or charges once the pre-paid dollar amount has been spent.[179]

As noted above, many mobile service providers offer their subscribers the option to limit the amount of purchases that can be made through a mobile device or to prevent the user of the device from making any purchases at all.[180] Controls that limit mobile purchasing work in much the same way that text messaging controls do.[181] Where the ability to make such device-billed purchases is turned off, the user of the device is prevented from making such purchases. Where a dollar-limit control is used, the ability to make purchases is suspended when the user of the device reaches the pre-set limit. In some instances, a subscriber is able to change the pre-set limits over time or increase the spending limit in the middle of a billing period with affirmative authorization.[182]

Consumers also can limit purchases on their mobile devices by choosing a pre-paid service plan. For example, Laurie Itkin of Cricket Communications and Leap Wireless described how many pre-paid service plans allow subscribers to pre-pay purchases billed to their mobile device.[183] When the user meets the pre-paid purchase amount, the plan does not allow further purchases. Pre-paid service plans also give subscribers the option to change the pre-paid amount from month to month or to increase the pre-paid amount during a billing period.

c. Controls designed to make mobile devices more accessible to consumers with disabilities

Bennett also discussed mobile device controls that service providers offer to make the devices more accessible to persons with disabilities.[184] In particular, Bennett identified mobile controls designed for

[179] *Id.*

[180] *Id*. at 12-13.

[181] *Id.*

[182] For example, under AT&T's "Smart Limits for Wireless" plan discussed by Bennett, users can make modifications to limits they have set at any time and the changes will be effective immediately. *See* http://www.wireless.att.com/learn/articles-resources/parental-controls/faq.jsp.

[183] Itkin, Tr. Day 2 at 16.

184 Bennett, Tr. Day 2 at 43.

sight-impaired consumers that give voice prompts for each button on the mobile device.[185] Based on his familiarity with the rules and regulations of the FCC, Itkin suggested that the majority of carriers probably provide mobile devices that are hearing aid compatible.[186] Some service providers also offer text-messaging-only plans, so that hearing-impaired subscribers are not required to pay for voice service on their devices.[187]

2. Methods of informing consumers of mobile controls

Bennett discussed AT&T's "Smart Limits for Wireless" plan to illustrate how AT&T informs consumers about available controls when consumers purchase mobile devices and service plans.[188] According to Bennett, this plan enables parents to go online to set up controls that regulate how and when their child can use his or her mobile phone. Bennett explained that the primary method used to inform consumers of controls available under this plan is through materials provided to consumers when they purchase mobile devices and services plans. These materials include the instruction manuals for specific mobile devices and targeted flyers highlighting specific mobile controls.[189]

Bennett also mentioned that the "Smart Limits for Wireless" plan is offered for a fee.[190] According to Bennett, AT&T imposes the fee to recoup development costs.[191] Bennett stated that the company currently discloses the fee on its website, but expects to roll out additional advertising that would further highlight for consumers the fee's existence.[192] Along these same lines, Bennett discussed the concern that in spite of the information available to consumers about mobile controls, many consumers are unaware of specific controls.[193] He referred to anecdotal evidence that many consumers, including another panelist, have been shocked by the high text messaging fees and the cost of other purchases by their teenaged children during the first month that they have a mobile device.[194] Such occurrences might indicate that better outreach and information about text-messaging and purchasing controls could be useful.[195]

[185] *Id.*

[186] Itkin, Tr. Day 2 at 44.

[187] *Id.*

[188] Bennett, Tr. Day 2 at 21-22.

[189] *Id*.

[190] *Id*. at 12.

[191] *Id*. at 24.

[192] *Id*. at 23.

[193] *Id*. at 21.

[194] *Id.*

[195] *Id. See also* CFA/CA/CU Joint Comments at 5 (recommending that stakeholders initiate a major effort to educate consumers and businesses about how to navigate the mobile marketplace).

3. Recommendations for improving consumer awareness of and the effectiveness of mobile controls

Following the discussion of mobile controls provided by Bennett and Itkin, Susan Grant of the Consumer Federation of America made several recommendations for improving consumer awareness of and the effectiveness of mobile controls. In particular, Grant recommended better outreach and education to consumers regarding the availability of such controls. She also suggested that carriers could do more advertising of such features, particularly those features for which they do not charge an additional fee. Panelists and audience members further recommended a stronger outreach effort to parental organizations, educator organizations, and other groups, with a focus on parents and minors.[196] The panel also discussed the potential benefits of better disclosures regarding mobile controls that raise privacy concerns, such as location controls.[197]

Session Seven: Children and Teens

Session Seven panelists addressed the challenges associated with mobile marketing to children and teens, and methods to help parents manage their children's mobile devices. The panelists for the session were Michael Becker, Executive Vice President of iLoop Mobile, Inc.; Wayne Keeley, Director of the Children's Advertising Review Unit of the Council of Better Business Bureaus ("CARU"); Riitta Kokko-Herrala, an attorney with the Finnish Consumer Agency and Ombudsman; Todd Haiken, Acting Manager of Public Policy at the National Parent Teacher Association; Jeff McIntyre, Senior Legislative and Federal Affairs Officer at the American Psychological Association; Eileen Espejo, Senior Policy Associate with the Children and the Media Program at Children Now; and David Diggs, Vice President and Executive Director of The Wireless Foundation. Phyllis Marcus and Stacey Ferguson, senior staff attorneys in the Division of Advertising Practices, co-moderated the panel.

1. Self-regulatory and legal constraints on mobile advertising to children

a. Existing self-regulatory guidelines

Michael Becker of iLoop Mobile began the session by highlighting industry best practices that he believes protect children as they interact with mobile marketers. He emphasized that the most important element in a children's mobile marketing campaign is clear notice of key terms such as the subject of the campaign, whether third-party ads will accompany the campaign, whether the child's mobile number will be shared with third parties, and any applicable charges.[198]

[196] *See, e.g.,* Grant, Tr. Day 2 at 33-34.

[197] *Id.* at 18-19.

[198] Becker, Tr. Day 2 at 59-60.

Becker referenced the MMA's Consumer Best Practices Guidelines governing mobile campaigns, including those that address campaigns directed to children.[199] In all campaigns, the MMA's guidelines require an application provider to respond with assistance if a consumer texts the keyword "help" to the provider's short code, and requires the provider to stop sending messages to the consumer's phone if the consumer texts the keywords "quit" or "stop."[200] In addition, under the MMA's guidelines, all short code programs must be approved by wireless carriers; this approval includes carrier review of the mobile marketer's "application flow" (*i.e.*, the marketer's intended consumer experience) to ensure that the proposed program meets the MMA's best practices requirements before a mobile campaign goes live.[201]

To supplement the MMA's guidelines, various content providers have implemented additional protective features when marketing to children. Becker touted the best practice of requiring a double opt-in not only for "premium rate" child-directed mobile campaigns, but also for those campaigns for which "standard rates" apply.[202] Moreover, he recommended avoiding use of the word "free" in children's campaigns when standard rates or other charges may apply.[203]

Wayne Keeley of CARU questioned whether the MMA's guidelines and industry best practices described by Becker sufficiently protect children. For example, he expressed concern that advertisers may not adequately disclose the type of content that will be included in the advertising.[204] He also expressed concern that current disclosures may not indicate how children's mobile phone numbers will be used (*e.g.*, whether they will be provided to third parties).[205] Finally, he recommended placing controls on general audience advertising that is likely to appeal to significant numbers of children.[206]

Panel participants also discussed implementing age screening to ensure that advertising campaigns do not reach children below the intended target age.[207] Becker demonstrated an age screen that required a user to enter a birth date to register for an SMS campaign.[208] Keeley stated that, depending on the wording of the age screen, children may falsify their ages in order to gain access to the mobile

[199] *See* the MMA's "Consumer Best Practices Guidelines for Cross-carrier Mobile Content Programs (United States)," *available at* http://www.mmaglobal.com/bestpractices.pdf.

[200] Becker, Tr. Day 2 at 54.

[201] *Id.* at 58-59.

[202] *Id.* at 54, 56.

[203] *Id.* at 56.

[204] Keeley, Tr. Day 2 at 63.

[205] *Id*.

[206] *Id*. at 67.

[207] Becker, Tr. Day 2 at 58-60.

[208] *Id*. at 58.

content being offered;[209] FTC staff echoed this assessment.[210] Becker noted that several technologies exist to prevent abuse of age screening systems.[211]

b. Legal constraints: the Finnish example

Currently in the United States, no laws specifically govern mobile marketing campaigns aimed at children.[212] By contrast, other countries, including Finland, have adopted laws addressing child-directed mobile marketing campaigns. Riitta Kokko-Herrala of the Finnish Consumer Agency discussed the constraints that Finland places on mobile marketing campaigns aimed at Finnish children. Finnish law prohibits advertisers, including mobile advertisers, from marketing to children under age 15 without a parent's consent.[213] Finnish law also prohibits SMS messages sent by one child to another if such messages include advertisements (*i.e.*, forward-to-a-friend messages).[214]

The Finnish Consumer Agency has brought several cases against carriers and content providers involving minors who used their mobile phones to engage in significant purchases without a parent's consent. In addition, the agency has negotiated a set of industry best practices aimed at restraining marketers' ability to target children and placing limits on children's ability to incur costs associated with mobile purchases.[215]

c. Possible changes to the U.S. approach

Panelists debated whether a complete ban on child-directed mobile advertising might be warranted, and agreed that one was not.[216] In particular, Becker emphasized that, although he saw no conflict between recognizing 18 as the legal contracting age and directing fee-based mobile advertising campaigns to children under that age, content providers must ensure that they: 1) provide children with clear and

[209] Keeley, Tr. Day 2 at 62.

[210] Marcus, Tr. Day 2 at 64.

[211] Becker, Tr. Day 2 at 64-65.

[212] However, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6508, and the Federal Trade Commission's COPPA Rule, 16 C.F.R. Part 312, apply to the online collection, use, or disclosure of personal information from children under 13, regardless of the type of device children use to access websites and other online services.

[213] Kokko-Herrala, Tr. Day 2 at 74.

[214] In addition, in Finland, child-directed advertising must immediately be recognizable as advertising, and Finnish law prohibits the use in child-directed ads of material not suitable for children. *Id.* at 74.

[215] One tenet of the Finnish best practices is that minors should not be able to make purchases via mobile devices that they would not otherwise be able to make. With respect to interactive television games, game hosts in Finland may not urge children to participate via SMS messages, may not use tempting prizes, must disclose the price per message and the total price for one game, and must advise children under age 18 to consult their parents before playing. *Id.* at 77-79.

[216] Becker, Tr. Day 2 at 60; McIntyre, Tr. Day 2 at 86-88.

comprehensive notice; 2) educate parents on the types of transactions children are able to engage in on their mobile devices; and 3) obtain parental consent before children under age 18 participate.[217]

While likewise not supporting a ban, Jeff McIntyre of the American Psychological Association ("APA") expressed grave concern about the ability of very young children to distinguish between commercial and non-commercial content.[218] Building upon an earlier point – that children may not be able to understand certain key terms and conditions of an advertising offer[219] – McIntyre stated that children 10 years of age and younger lack the developmental capacity to fully understand the terms and conditions that marketers may include in their mobile ad campaigns.[220] In the APA's opinion, a mobile campaign directed to very young children may be inherently unfair. McIntyre argued that to avoid this problem, at the very least, the burden of initial contact should be shifted so that U.S. mobile marketers are forced to go through parents to reach their children.[221] Eileen Espejo of Children Now, also expressed concerns about children's capacity to distinguish content from commercials. [222]

Panelists briefly mentioned additional regulatory approaches to child-directed mobile marketing. Espejo called upon lawmakers to consider adapting and updating COPPA so that the law clearly applies to the mobile web and the mobile ecosystem.[223] When asked whether a regulation similar to the FTC's 900 Number Rule is warranted to govern mobile advertising campaigns directed to children, none of the panelists advocated for a rule.[224]

Finally, following up on a comment from the audience regarding the possibility of a Do Not Call Registry governing minors' mobile numbers, Todd Haiken of the National Parent Teacher Association argued for a self-regulatory system in which wireless carriers and content providers know, from the outset, whether the end user of a particular mobile handset is a child or an adult, and parents are able to place their children's mobile phone numbers on whitelists and blacklists accordingly.[225] David Diggs

[217] Becker, Tr. Day 2 at 60-61.

[218] McIntyre, Tr. Day 2 at 88.

[219] *See* Espejo, Tr. Day 2 at 71.

[220] McIntyre Trd. Day 2 at 87-88. McIntyre also questioned whether children under age 18 are able to understand privacy agreements or to properly assess privacy concerns. *Id.* at 87.

[221] *Id* at 91.

[222] Espejo, Tr. Day 2 at 70.

[223] *See also* Children Now Comments at 3 (requesting the FTC to revisit and clarify its COPPA rule to require affirmative express consent from parents when advertisers collect information used to send individualized ads to children as part of behavioral advertising).

[224] *See* Haiken, Tr. Day 2 at 92. *But cf.* Grant, Tr. Day 2 at 35-36 (noting, on an earlier panel, that "the 900 number rule really provides some important protection to consumers and it would be useful to have something analogous for [the mobile] space").

[225] *Id*. at 84-85. Ritta Kokko-Herrala commented that a similar system functions in Norway, but not in Finland. *Id*. at 84.

of the Wireless Foundation acknowledged that wireless carriers currently are unaware of who the end user of a particular mobile handset is.[226]

2. Parental control of children's handsets

a. Existing parental controls

According to Diggs, the top five U.S. wireless carriers currently offer, at no cost, a relatively common set of parental controls, including: 1) the ability to turn off Internet access; 2) the ability to filter web content; and 3) the ability to block unwanted text messages or phone calls. They also offer web-based mobile bill monitoring.[227] Diggs predicted that, in the near future, wireless carriers will compete for subscribers based on their ability to provide family-friendly controls.[228] In an effort to make this information more readily available to parents, each of the leading wireless carriers' websites now gathers this information under the common search term "parental controls."[229]

In addition to enhancing parental control features, the wireless industry has launched an initiative to educate parents about child safety. The Wireless Foundation's "Get Wise About Wireless" program addresses issues such as cyber-bullying and provides tools to engage parents and children in a conversation about the rights and responsibilities of each regarding the use of the child's mobile device.[230] One aspect of the Foundation's program is a family contract for responsible mobile phone use that asks the child to agree not to download or subscribe to any service on the child's mobile phone without parental permission. In return, parents must agree not to overreact in the event the child misuses the phone.

b. Suggestions for additional controls

Haiken suggested that wireless carriers alter the default settings for mobile phones so that a parent must opt out of, rather than into, various controls available on handsets intended for use by a child.[231] Carriers might, for example, limit a phone's ability to receive SMS messages, requiring parents who want their children to receive or send such messages to specifically opt out of this default parental control.[232]

[226] Diggs, Tr. Day 2 at 93.

[227] *Id*. at 98-100.

[228] *Id*. at 100-101. Under Finnish law, wireless subscribers have the right to block call or text services that cost additional money; carriers must offer blocking services to consumers free of charge. Kokko-Herrala, Tr. Day 2 at 76.

[229] Diggs, Tr. Day 2 at 102.

[230] *Id*. at 96-97. *See also* Wireless Foundation Comments at 8.

[231] Haiken, Tr. Day 2 at 72.

[232] *Id*. at 72-73.

Panelists discussed the fact that parents want to be able to contact their children at any time of day, and want the comfort of knowing that their children can contact them whenever necessary. According to Haiken, mobile phones cause significant in-school disruptions.[233] School systems are extremely reluctant to allow students to carry mobile devices on campus, not only because they are a distraction, but also because they may be used to effectuate problematic behavior such as cyber-bullying. On the other hand, in emergency situations, student access to mobile devices is crucial. Diggs recalled that on September 11, 2001, two school systems in the Washington, D.C. metropolitan area allowed students to contact their parents using their mobile devices.[234] Based on that experience, both systems revisited their ban on mobile devices in school and liberalized their policies.

Diggs suggested that parental controls offered by the wireless carriers may provide a solution to the challenges facing both schools and parents. Features such as time-of-day restrictions could be used to limit what a student is able to do with his or her mobile device during certain hours of the day.[235] Parents could choose to make text messaging or web access off-limits on their child's mobile device during the school day, or restrict web access to strictly educational sites. Panelists agreed that this is a promising area for collaboration between industry and educators.

Session Eight: Best Practices

Session Eight addressed the state of industry-developed best practices in the areas of billing, disclosures to consumers, complaint handling, and dispute resolution. The panelists were Peter Avery, Principal Administrator of the Organisation for Economic Co-Operation and Development's ("OECD's") Committee on Consumer Policy; Alykhan Govani, Head of Business Development at MX Telecom; Laura Marriott, President of the Mobile Marketing Association ("MMA"); James Bradford Ramsay, General Counsel and Supervisor/Director of the Policy Department, at the National Association of Regulatory Utility Commissioners ("NARUC"); and Gary Schwartz, Co-Chair of Interactive Advertising Bureau's ("IAB's") Mobile Advertising Committee. Lois Greisman, Associate Director of the Division of Marketing Practices, moderated the panel.

1. Finding and evaluating complaints

Previous panels identified various problems in the areas of M-commerce advertising, billing, and dispute resolution. Following up on these points, James Bradford Ramsay of NARUC opened the panel by providing additional details about billing and dispute resolution practices. In particular, Ramsay noted that it is difficult to quantify the number of billing problems because often such problems

[233] *Id*. at 105-106.

[234] Diggs, Tr. Day 2 at 107-108.

[235] *Id*.

are under-reported by consumers.[236] For example, according to Ramsay, researchers in a multi-national survey found that almost 60 percent of people who had complaints about their mobile data transactions never made a complaint to anyone.[237] Ramsay suggested that such under-reporting may be due, in large part, to the complexity of consumers' phone bills, as well as consumers' unawareness of where to submit complaints.[238]

Many states are exploring the extent of billing problems. The State of California, for example, is holding hearings on the unlawful practice of adding unauthorized charges to phone bills, which also is known as "cramming."[239]

2. Existing best practices

Laura Marriott of the MMA provided an overview of the MMA's role in developing best practices. The main industry guides in existence are produced by the MMA and used by the more than 600 member companies.[240] MMA's membership includes: 1) wireless carriers and CTIA–The Wireless Association ("CTIA"); 2) companies advertising products, selling content (such as ringtones or videos), or using mobile services to promote name brands (these are all referred to as "content providers"); and 3) aggregators, which act as intermediaries between companies (*i.e.*, brand owners and content providers) and mobile end users/carriers. Aggregators typically have contractual relationships with both the wireless carriers and the content providers, and arrange for product to reach end users, and payment to flow to the content providers.

The MMA's guidelines include a general Code of Conduct that, according to Marriott, sets out "consumer privacy and protection standards;"[241] best practices guidelines for businesses operating in the United States, which set out rules for certain mobile content services;[242] and best practices for mobile advertising and marketing to children.[243]

Gary Schwartz of the IAB provided an overview of his organization. The IAB is an industry association that has established a policy task force to develop a self-regulatory program for providers of

[236] Ramsay, Tr. Day 2 at 136.

[237] *Id*. at 138.

[238] Ramsay noted, for example, that a survey conducted approximately five years ago by AARP revealed that many of its members did not know to call their state utility commission if they have complaints. Ramsay, Tr. Day 2 at 139.

[239] *Id.* at 139, 142. The state attorney generals have been active in challenging unauthorized billing practices..

[240] For example, in contracting with content providers, T-Mobile requires commitment to content guidelines that are consistent with the MMA's Advertising Guidelines. T-Mobile Comments at 5.

[241] Marriott, Tr. Day 2 at 117. *See* MMA Comments (534331-00013).

[242] *See* MMA Comments (534331-00010).

[243] *See* MMA Comments (534331-00011).

mobile services.[244] To date, the task force has explored topics such as privacy best practices, consumer choice, notice, and data security.[245]

Peter Avery of the OECD described the OECD's role in the mobile sphere. The OECD is an intergovernmental organization that is comprised of the world's 30 most developed countries.[246] In June 2008, the OECD's Committee for Consumer Policy ("CCP") examined how the OECD's 1999 electronic commerce guidelines applied to some areas of M-commerce.[247] The CCP produced a consumer protection policy guidance paper, which focused on: 1) adequate disclosures for consumers; 2) the increased risk of commercial exploitation of minors; and 3) security issues.[248]

3. The adequacy of disclosures

According to Ramsay, most consumer complaints concern inadequate disclosure problems rather than out-and-out fraud, although he also noted that cases of blatant fraud do exist.[249] To address complaints concerning inadequate disclosures, the MMA's guidelines require different levels of consumer consent to be obtained depending upon the nature of the program or service. For standard rate programs,[250] such as sending a text message to a short code, the MMA's guidelines require a consumer to participate by "opting in," which is simply the act of participating.[251] For example, the consumer would send a text message to a short code, and the act of doing that would indicate, according to Marriott, that the consumer had agreed to pay the standard rate.

On the other hand, when a consumer's action would incur a "premium rate charge" – that is a charge higher than the rate for standard messaging – the MMA's guidelines require additional action by the consumer – often referred to as a "double opt-in." For example, if a consumer signs-up for a $9.99 monthly subscription for content (*e.g.*, to receive ringtones or stock information on a regular basis), the provider of the content would take some action to verify that the consumer has authorized the transaction. Such action might include sending a message to the consumer to provide further

[244] Schwartz, Tr. Day 2 at 131.

[245] *Id.*

[246] Avery, Tr. Day 2 at 121.

[247] According to Avery, the 1999 guidelines refer to principles for transparent and effective protection in the following areas: fair business advertising and marketing practices, online disclosures, confirmation processes, payment, dispute resolution and redress, privacy, and education and awareness. Avery, Tr. Day 2 at 122. *See* Avery Comments for a full discussion. *See also Guidelines for Consumer Protection in the Context of Electronic Commerce* (OECD 1999), available at http://browse.oecdbookshop.org/oecd/pdfs/browseit/9300023E.PDF.

[248] *Id.* at 125.

[249] Ramsay, Tr. Day 2 at 140.

[250] The standard rate is the standard charge imposed on a consumer by a carrier for sending or receiving any text message.

[251] Marriott, Tr. Day 2 at 118.

notice of the applicable rates, and then asking the consumer to confirm by reply text, that he or she agrees to purchase the subscription and accept the charge.[252] When subscriptions relate to mobile chat are involved, some content providers will impose a triple opt-in requirement.[253]

4. Dispute resolution

Notwithstanding the various industry guidelines, consumer disputes do occur. Accordingly, Avery opined that it is important to establish effective and transparent mechanisms to address consumer complaints.[254] The challenge, however, can be determining which entity is responsible for addressing consumer complaints. Alykhan Govani of MX Telecom stated that much of the handling of consumer complaints is under the control of carriers.[255] In response to a consumer complaint, most carriers will refund charges without much examination.[256] In some instances, however, a carrier will elect to send the complaint to the aggregator or directly to the content provider.[257]

5. Monitoring and reviewing compliance

In support of the MMA guidelines, CTIA has launched a global initiative for the industry to monitor compliance with the MMA guidelines in the area of short code use.[258] Under this initiative, to be assigned a short code, which can be used by an entity to market goods and services to mobile users, an entity must submit a short code application.[259] According to Marriott, the applications are reviewed by a third party, Nielson Mobile,[260] to ensure that the information in the application comports with the MMA's consumer best practices for advertising and promotion.[261] When an application is found to be

[252] *Id*. at 119.

[253] *Id.* The panelist did not define "triple opt-in" requirements.

[254] Avery, Tr. Day 2 at 159.

[255] Govani, Tr. Day 2 at 145-46. Govani indicated that when aggregators file a short code application, they provide a customer support toll-free number, support email address, a website, and even personal email account information for their senior executives. *Id.*

[256] *Id*.

[257] *Id.*

[258] Marriott, Tr. Day 2 at 148 (stating that the auditing initiative is run by Telephio, recently acquired by Nielson Mobile).

[259] A short code is similar to a phone number, but with fewer numbers, and it can only be used for mobile messaging. Short codes are typically used by companies for marketing campaigns. For example, as alluded to in the summary of Session One in this report, some TV shows allow viewers to vote in polls or contests by texting specific messages to specific short codes.

[260] *Id*. at 149.

[261] *Id.*

non-compliant, the carrier and the content provider are notified and given a period of time in which to cure the problem.[262] The results are not disclosed to the public.[263]

Aggregators also can play a role in monitoring and reviewing compliance. For example, some aggregators work with content providers to ensure that the content provider's material, including scripts, is compliant with the MMA's standards before a campaign is launched.[264]

Many aggregators also spot check the billing patterns of their clients to determine whether cramming or other unauthorized activity is occurring.[265]

6. Improving industry guidelines and practices

The panelists generally agreed that industry guidelines and best practices should be continually reviewed and improved. For example, the MMA revises its guidelines every six months.[266]

Improving industry practices, however, also can be a matter for law enforcement. For example, according to Ramsay, some state entities, such as the Florida Office of the Attorney General, are pursuing law enforcement actions and holding public workshops on these topics. Further, Ramsay stated that state and federal regulators should keep a careful watch on industry practices to ensure that consumers are being protected.[267]

Session Nine: Mobile Security – Whose Phone Is It Anyway?

The final panel addressed the risks to, and vulnerabilities of, mobile phones to various threats – current and future – as well as precautions consumers can take to protect themselves. The panelists discussed: 1) the stakeholders in the mobile security sphere; 2) mobile security threats and the data at risk from such threats; and 3) the security implications of open platform development, mobile phone recycling, and contactless payments via mobile phones. The panelists concluded with assessments and predictions regarding the mobile security environment. The panel featured David Cole, a Senior Director in the Symantec Consumer Products Division; Mark W. Henderson, a Senior Analyst supporting the United States Computer Emergency Readiness Team ("US-CERT"); and Larry Rudolph, a Senior Staff Engineer at VMware on leave from his position as principal research scientist at the

[262] *Id*. at 150-51.

[263] *Id*. at 150.

[264] Schwartz, Tr. Day 2 at 152; Govani, Tr. Day 2 at 154-55.

[265] *Id*.

[266] Marriott, Tr. Day 2 at 148.

[267] Ramsay, Tr. Day 2 at 144.

Massachusetts Institute of Technology. Phillip Tumminio, a senior staff attorney in the Division of Marketing Practices, moderated the panel.

1. Mobile security stakeholders

David Cole of Symantec initiated the discussion by describing how several stakeholders in the M-commerce market share responsibility for mobile security.[268] These stakeholders include the carriers, handset providers, mobile operating system providers, and individual handset users.[269] The security environment has changed over the last three years, as bad actors have begun to exploit the handset user rather than the handsets themselves.[270] Larry Rudolph of VMware also identified independent, third-party software providers as stakeholders, and remarked that all stakeholders seem to be able to provide software updates to consumers' handsets over the air, although many consumers are unaware of, or unable to obtain such updates themselves.[271]

2. Mobile security threats and the data at risk on mobile phones

Mark Henderson of US-CERT identified several techniques threatening the mobile phones of consumers, government, and enterprise clients.[272] These techniques include the "structured" threats of malware propagated through social-engineering email,[273] "whaling,"[274] and, to a lesser degree, the delivery of rootkits.[275] "Unstructured" threats include standard viruses and attack methods now common in the PC realm.[276] Handsets also may be attacked using "botnets,"[277] Voice over Internet Protocol ("VoIP") phishing,[278] and unsolicited text messages hiding Trojan viruses. Rudolph pointed out that

[268] Cole, Tr. Day 2 at 176.

[269] *Id.*

[270] *Id.* at 177.

[271] Rudolph, Tr. Day 2 at 178.

[272] Henderson, Tr. Day 2 at 179.

[273] *Id*. Social engineering attacks rely on human interaction rather than technological tools to manipulate people into performing certain acts such as divulging their personal information. Targeted social engineering attacks that are launched via email are dubbed "spearfishing" attacks.

[274] *Id.* A "whaling attack" is a social-engineering attack that targets a company executive or project head rather than staff-level employees.

[275] *Id.* at 179-80. A rootkit is a type of malware that is designed to take control of a computer system, without authorization by the system's owners and legitimate managers.

[276] *Id.* at 180. Approximately 400 mobile viruses have been cataloged to date. *Id.*

[277] Botnets are networks of computers that have been infected with viruses which allow access to the computers by third parties who use the infected computers for nefarious purposes.

[278] Henderson, Tr. Day 2 at 180. VoIP phishing, also known as "vishing" or "smishing," is a term used for a scheme in which messages that arrive as a text message or voicemail instruct consumers to place a call to a number that the message falsely represents as belonging to the consumers' bank or other financial institution. The consumer reaches a phone tree and is instructed to provide his or her account number and PIN. The phone number called is usually provided through a VoIP service.

mobile handsets that are Bluetooth enabled are particularly vulnerable to intrusions. According to Rudolph handsets ship with their Bluetooth feature set to "discoverable," and third parties in proximity to a phone in "discoverable" mode can discern the phone's Bluetooth ID and broadcast advertisements or fraudulent messages to that phone.[279] He added that mobile viruses typically have an impact only on smartphones. He predicted that as smartphones become more prevalent, the risk posed by mobile viruses also may increase.[280]

In contrast to the impact of viruses, the loss or theft of handsets without password protection currently poses the most significant threat to mobile phone users.[281] Modern handsets contain a myriad of sensitive data, including geo-location data, personally identifiable information about the user, carrier information, information from other applications cached on the handset, email information, and passwords.[282]

To safeguard against the theft of data, Henderson advised that users maintain the phone numbers of their carriers or others who could remotely wipe data from a phone if the handset is lost or stolen.[283] More importantly, users should avoid storing passwords on their phones, disable unused services or features on phones (such as Bluetooth and infrared ports), and physically secure the phones themselves.[284] Cole agreed with these suggestions, observing that the risk is proportional to the kinds of data stored on phones.[285] More sensitive data calls for more intensive security measures such as password protection, data encryption, and use of mobile anti-virus software.[286] At the same time, users may be likely to disregard warnings about storing data on mobile phones, either because they believe the convenience of having such data accessible outweighs the risk or because users do not understand how to implement protective measures.[287]

3. The security implications of various trends

The panelists addressed several questions from the audience regarding mobile phone usage and security, commencing with a question regarding the trend towards open mobile platform development

[279] *Id.* at 181-82.

[280] *Id*. at 183. The largest mobile threat to date has been the 2005 Comwarrior virus. This virus affected users in 20 countries and spread using Bluetooth and MMS, but ultimately had little impact. *Id.*

[281] *Id.* at 184.

[282] Henderson, Tr. Day 2 at 185-96. The National Institute of Standards and Technology ("NIST") provides a publication discussing mobile phone forensics and the data at risk.

[283] *Id*. at 186.

[284] *Id.* at 187.

[285] Cole, Tr. Day 2 at 188-89.

[286] *Id*. at 189.

[287] Rudolph, Tr. Day 2 at 190-91. Rudolph stated that determined thieves can circumvent many protective measures.

and its implications for mobile security. Rudolph opined that open platform development had mixed blessings. On the one hand, open development projects, such as Google's Android project, can lower the (currently high) cost of mobile software design and spur the creation of beneficial applications by smaller third parties.[288] At the same time, democratized access to mobile architecture could facilitate access by hackers and other malevolent actors.[289] Henderson further cautioned that open-source systems could result in handsets becoming "bricked" (rendered unusable) if users install incompletely tested applications produced by third parties, independent from the handset maker, carrier, or major vendor.[290] Although open-source security solutions exist, they are not as "trusted" as those provided by a major vendor.[291] Cole remarked that open-source development could make the market more competitive and provide more options to consumers.[292] However, users will need to be educated to make good decisions regarding selection of third-party applications on their devices in order to mitigate security risks.[293]

The panelists then considered the risks to data stored on mobile phones when users part with them in mobile phone recycling programs. Henderson noted that two years ago, US-CERT recommended that government users of handsets return them to their information technology staff or physically destroy them at the end of their tenure.[294] Rudolph advised that physical destruction, particularly with water, might be the only solution to prevent data compromises.[295] The moderator, Phillip Tumminio, noted that the FTC publishes a pamphlet on the safe recycling of mobile devices which provides useful information on that topic to consumers.[296]

An audience member, Sally Mund, of the Council of Better Business Bureaus, commented that consumers may be aware of ecological hazards related to disposal of mobile devices into the trash, but unaware of the data at risk on the devices.[297] Mund asked the panel what efforts the industry has made to educate increasingly environmentally conscious consumers about the potential data risks of disposing of phones through recycling programs.[298] David Diggs, a participant on an earlier panel and

[288] *Id*. at 194.

[289] *Id*. at 195.

[290] Henderson, Tr. Day 2 at 195-96. As a consequence, a user could risk voiding the phone's warranty.

[291] *Id*. at 196.

[292] Cole, Tr. Day 2 at 197.

[293] *Id*. Cole predicted that the mobile handset security market will evolve differently from the PC security market.

[294] Henderson, Tr. Day 2 at 198-99.

[295] Rudolph, Tr. Day 2 at 199.

[296] Tumminio, Tr. Day 2 at 199 (referencing "The 411 of Disposing of Your Old Cell Phone," available at http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm).

[297] Mund, Tr. Day 2 at 200.

[298] *Id*. at 201.

a member of the Wireless Foundation, responded from the audience that the Wireless Foundation recommends that users wipe the memory of their phones.[299] The Wireless Foundation has collected four million phones as part of its recycling program, and has experienced only a handful of instances, all "benign," where data stored on the phone "came back in some form."[300] Although mobile phone components have become less toxic, the Wireless Foundation still recommends recycling phones over disposal in the trash.[301]

In response to another question from the audience, the discussion turned to the installation and updating of mobile security software. Cole stated that such software has been geared to enterprise users, and installation is not as easy as it should be.[302] Cole said that users want security software to come pre-loaded on phones and predicted that, unlike the PC security market, the mobile security market will conform to this expectation.[303] Rudolph agreed, but expressed concern that the currently "closed" mobile software development environment prevents third parties from developing novel security solutions that large developers might miss, thereby placing consumers at risk.[304]

The discussion then briefly turned to the practice of "sideloading" – installing applications to mobile devices via connection to a PC or a portable storage device. Henderson advised that users should be cautious about such practices because they could lead to the transmission of viruses or other malicious software from one device to another. Henderson noted that US-CERT publishes guidelines providing users with best practices for limiting risks from such activities.[305]

Susan Grant, a participant on an earlier panel, from the Consumer Federation of America, asked about the security implications of mobile phones used as contactless payment devices.[306] Rudolph answered that some newer mobile phones include near-field communications technology, such as RFID cards, that function like credit cards.[307] Unlike credit cards, phones are shipping with "active" RFID technology that can calculate and transmit updated account information.[308] Phones actively broadcast-

[299] Diggs, Tr. Day 2 at 201. Diggs noted that data may still remain on a phone after a typical memory wipe, but that the data are for the most purposes "pretty benign."

[300] *Id*. at 202.

[301] *Id*.

[302] Cole, Tr. Day 2 at 203.

[303] *Id*. at 203-04.

[304] Rudolph, Tr. Day 2 at 204.

[305] Henderson, Tr. Day 2 at 205.

[306] Grant, Tr. Day 2 at 206.

[307] Near-field communications technology is a short-range, high frequency wireless communication technology that enables the exchange of data between devices over about a 10 centimeter distance. This technology is being used to enable mobile devices to be used for contactless payments.

[308] Rudolph, Tr. Day 2 at 206-07.

ing data are susceptible to "man-in-the-middle" attacks, where third parties can read the data from the user's phone.[309]

4. Assessments and predictions

In closing, Cole stated that it is easy to exaggerate the digital threats currently facing mobile phone users and miss the greater threats posed by fraudulent payments and loss of the phone (and the data it contains).[310] According to Cole, the main threats to consumers who increasingly access the Internet with mobile devices will be deception and fraud targeting the user rather than the device.[311]

Henderson stated that US-CERT, in conjunction with the NIST Computer Security Research Center, offers two publications on wireless device usage and mobile phone forensics that contain valuable resources for mobile device users.[312] Henderson stated that user behavior must be focused on securing mobile devices, and that public and private sectors should partner to design secure protocols and prevent criminal conduct.[313]

Rudolph pointed out that the biggest mobile security threat may occur when malevolent actors learn how to crack codes implemented by carriers and deliver viruses via over the air software updates to handsets.[314] Rudolph further observed that users will increasingly connect to the Internet using mobile devices over WiFi networks rather than carrier networks, thus exposing mobile devices to threats similar to those that PCs have faced.[315] Rudolph called for more transparency in mobile device network management, and specifically for greater user access to mobile handsets, including, for example, the ability to install applications of their choosing onto their mobile handsets.[316]

The panel concluded with the moderator observing that the number of attacks on mobile handsets has thus far not been large, but that it could easily grow if precautions are not taken.[317]

Conclusion

The mobile marketplace continues to expand at a rapid pace. In the months following the Mobile Town Hall, the number of marketers entering the mobile space has increased, new devices have pro-

[309] *Id.* at 207. Rudolph noted that such attacks already have occurred in the Netherlands.

[310] Cole, Tr. Day 2 at 207.

[311] *Id*. at 208.

[312] Henderson, Tr. Day 2 at 208-09.

[313] *Id*. at 209.

[314] Rudolph, Tr. Day 2 at 210.

[315] *Id.*

[316] *Id*. at 211.

[317] Tumminio, Tr. Day 2 at 212.

liferated, and the number of new mobile applications has continued to swell. As noted by then-FTC Commissioner, now-Chairman, Jon Leibowitz in his opening remarks at the Town Hall, the emerging mobile marketplace raises a host of opportunities as well as a host of consumer protection challenges.[318] The Town Hall participants, who encompassed a wide variety of stakeholders – advertisers, device manufacturers, telecommunications carriers, aggregators, consumer advocates, law enforcers, and regulators – all evinced a keen interest in protecting consumers in the rapidly growing mobile marketplace. The FTC staff applauds the commitment of the mobile industry to address consumer protection challenges. At the same time, the FTC staff is committed to policing the wireless space to ensure consumer protections are in place.[319]

[318] Commissioner Leibowitz, Tr. Day 1 at 9.

[319] *Id.*

Appendix A: Panelists

Panel 1

Evan Neufeld, Vice President and Senior Analyst, M:Metrics
Steve Smith, Media Critic, Mediapost and Access Intelligence

Panel 2

Alykhan Govani, Head of Business Development, MX Telecom
William Haselden, Assistant Attorney General, Office of the Attorney General of Florida
Dorrian Porter, Chief Executive Officer and Founder, Mozes, Inc.
Leigh Schachter, Senior Litigation Counsel, Verizon Wireless

Panel 3

Steve Boom, Senior Vice President of Connected Life, Yahoo! Inc.
Andrew Elliott, Director of Services and Software, North America Go-to-Market, Nokia
Thomas C. Ford, Global Market Strategist of Consumer Products, Opera Software
Rich Miner, General Manager of Mobile Platforms, Google Inc.

Panel 4

Michael F. Altschul, Senior Vice President and General Counsel, CTIA–The Wireless Association
Tony Bernard, Vice President of Operations, Useful Networks
Alissa Cooper, Chief Computer Scientist, Center for Democracy and Technology
Brian R. Knapp, Chief Privacy Officer and Vice President of Corporate Affairs,
Loopt, Inc.
Tim Lordan, Executive Director, Internet Education Foundation
Fran Maier, Executive Director and President, TRUSTe

Panel 5

Jean Berberich, Digital Marketing Innovation Manager – Mobile, Procter & Gamble
Jeff Chester, Executive Director, Center for Digital Democracy
Susan Duarte, Counsel for Marketing Practices, Sprint Nextel Corp.
Jim Durrell, Director of Product Management, Greystripe
Benjamin Ezrick, Senior Strategist of Digital Innovation, Ogilvy Interactive
Michael Hanley, Assistant Professor of Advertising, Ball State University
Gene Keenan, Vice President of Mobile Services, Isobar Global
Hairong Li, Associate Professor of Advertising, Michigan State University
Marci Troutman, Founder, Siteminis, Inc.

Panel 6

Mike Bennett, Executive Director – Consumer, State, and Local Government Affairs, AT&T Services, Inc.
Susan Grant, Director of Consumer Protection, Consumer Federation of America
Laurie Itkin, Director of Government Affairs, Cricket Communications

Panel 7

Michael J. Becker, Executive Vice President of Business Development, iLoop
Mobile, Inc.
David S. Diggs, Executive Director, The Wireless Foundation
Eileen Espejo, Senior Associate, Children and the Media Program, Children Now
Todd Haiken, Acting Manager, Public Policy, National Parent Teacher Association
Wayne J. Keeley, Director, Children's Advertising Review Unit of the Council of Better Business Bureaus
Riitta Kokko-Herrala, Attorney, Finnish Consumer Agency and Consumer Ombudsman
Jeff J. McIntyre, Senior Legislative and Federal Affairs Officer, American Psychological Association

Panel 8

Peter Avery, Principal Administrator, Committee on Consumer Policy, Organisation for Economic Co-Operation and Development
Alykhan Govani, Head of Business Development, MX Telecom
Laura Marriott, President, Mobile Marketing Association
James Bradford Ramsay, General Counsel and Supervisor/Director – Policy Department, National Association of Regulatory Utility Commissioners
Gary Schwartz, Co-Chair of the Mobile Advertising Committee, Interactive Advertising Bureau

Panel 9

Dave Cole, Senior Director, Consumer Products, Symantec
Mark W. Henderson, Senior Analyst, United States Computer Emergency Readiness Team (US-CERT)
Larry Rudolph, Senior Staff Engineer, VMware

Appendix B: Parties Filing Written Comments

1. American Academy of Pediatrics (Jenkins, Renee)
2. Avery, Peter
3. Center for Democracy & Technology (Morris, John)
4. Children Now (Espejo, Eileen)
5. CMOR: Promoting & Advocating Survey & Opinion Research (Fienberg, Howard)
6. Consumer Federation of America et al. (Grant, Susan)
7. CTIA - The Wireless Association (Altschul, Michael)
8. Hoofnagle, Chris
9. Mobile Marketing Association (Marriott, Laura) (multiple submissions)
10. Opera Software (Ford, Thomas)
11. Rudolph, Larry
12. Rule, Scott
13. T-Mobile USA (Wolverton, Amy)
14. Wireless Foundation (Diggs, David)

ftc.gov