

RE:  
Summary of FTC Mobile Marketing Town Hall Meeting

DATE:  
May 8, 2008

The Federal Trade Commission on May 6 and 7 held a Town Hall meeting, entitled Beyond Voice: Mapping the Mobile Marketplace,” to explore issues surrounding the evolving area of mobile commerce (m-commerce) and the implications for consumer protection policy. Below are highlights from the panel discussions.

### **Opening Remarks**

The town hall began with remarks by Commissioner Jon Leibowitz, Federal Trade Commission, who identified the following concerns related to mobile marketing -

1. Providing meaningful disclosure despite being limited by a device’s small screen size;
2. Mobile advertising may interfere with a consumer’s use of a mobile device and the services available through it;
3. Location-based services or advertising could create consumer benefit, but may raise privacy and governmental access concerns, and generate intrusive advertising that clutters a consumer’s mobile device; and
4. The personal nature of mobile marketing heightens issue related to minors.

Leibowitz stated that as mobile technology evolves so to must consumer protection. He recognized industry efforts to self-regulate. He warned that companies should not bury notice and choice in privacy policies and stated that companies should obtain opt-in consent for mobile marketing, particularly for location-based offerings.

Following are selected highlights of the panel discussions:

### **Day One, Session 1: The Mobile Marketplace — What, How, and Who**

This session provided an overview of the mobile marketplace. The presentations focused on the evolving uses of mobile devices, demographics, and consumer habits.

Steve Smith, **Media Critic, Mediapost and Access Intelligence**, stated that mobile devices are moving beyond person-to-person communication to a tool of commerce. He stated that there are 257 million wireless subscribers, up from 55 million in 1997, and that there is 82.4% penetration rate for adults. He stated that in 2008 more US consumers would access the web via mobile devices than a computer. He indicated that mobile devices are the perfect platform whereby convergence, scale, and portability intersect. Smith explained to Jeff Chester, the Center for Digital Democracy, that there is

little research related to the use of SMS messaging for political speech, but that he has anecdotal evidence that the presidential campaigns have been using such technology to coordinate their logistics.

Evan Neufeld, Vice President and Senior Analyst, **M:Metrics**, stated mobile adoption is influenced by pricing of devices and services, the functionality of the device, and bandwidth. He also indicated that the breadth of services used by consumers via mobile devices is rising. He explained that his research demonstrates that consumption of mobile products or services is driven by a consumer's desire to personalize their mobile device through ring tones, "phone bling," or wallpaper as a mode of self-expression rather than consuming media.

### **Day One, Session 2: Mobile Messaging — Unsolicited, Premium, and Interactive Messaging**

Alykhan Govani, Head of Business Development, **MX Telecom**, provided an overview of text messaging and how it is used by marketers to communicate with consumers.

Dorrian Porter, Chief Executive Officer and Founder, **Mozes, Inc.** explained that costs, spam, and frustration with technology undermine consumer adoption of mobile commerce. He said that marketers are hesitant to adopt mobile technology as a channel because of budgetary concerns, technology, and inexperience in designing compelling campaigns. He also stated that regulators should be careful not to restrain innovation.

William Haselden, Assistant Attorney general, **Office of the Attorney General of Florida**, described how the State Attorney General enforces existing advertising law in the SMS services context. He said the Attorney General targets carriers, billing aggregators, and advertising networks that partner with companies that represent that merchandise in their advertisements is "free" when actually a consumer will incur some expense in the process of obtaining the merchandise.

Haselden said the Attorney General's office is developing prescriptive compliance guidelines for online marketers. He stated that the guidelines would require that the price and terms for the merchandise, such as the cost for subscribing to a ringtone service, be disclosed within 125 pixels in any direction from the field in which a consumer enters his wireless number. He also stated that the price must be provided at minimum of 12 point font, written numerically, and be displayed in an obvious color contrast. He stated that if the offered service includes other services, such text services accompanying a ringtone offer, that secondary offer must be displayed in a font size of at least fifty-percent of that of the featured offering. Finally, he said they intend to offer guidance related to marketing to children.

Leigh Schachter, Senior Litigation Counsel, **Verizon Wireless**, described Verizon's efforts in fighting text message spam. He said since August of 2007, Verizon has prevented 100-200 million spam messages from being delivered. He said text spam causes harms for consumers by violating their sense of privacy, imposing charges, and that it could expose consumers to offensive material. He explained that text spam could also harm wireless service providers by slowing the network, preventing the transmission of legitimate messages, and degrading a provider's reputation and goodwill. He explained how Verizon uses the CAN-SPAM Act, the Computer Fraud and Abuse Act, the TCPA, and state laws to combat spammers. He said consumers could also work to limit the amount of spam they receive by blocking text messages, using "nickname" features (process by which a user can change their

address), or limit who they provide their wireless number too. As for industry efforts, Schachter recommended using sophisticated filtering technology, working with law enforcement to identify and prosecute spammers, and cooperating internationally.

### **Day One, Session 3: Mobile Applications — Games, Widgets, and More**

This session focused on how different mobile ecosystems open up the world of applications, from games to social networking. Below are highlights of the panel discussions.

Steve Boom, Senior Vice President of Connected Life, **Yahoo! Inc.**, described the key differences between personal computers and mobile ecosystems. He explained that the PC ecosystem is relatively simple, designed to make building applications easy (on Windows or Macs), for only a few browsers (such as Explorer, Firefox, and Opera), to provide open services to the market. In contrast, he noted that the mobile ecosystem is complex, which impacts innovation. Unlike the PC ecosystem, the mobile ecosystem is comprised of multiple operating systems, 20+ browsers, no real industry standards for hardware or screens, and complex distribution channels.

Boom explained enabling applications to function across all mobile devices is a primary challenge to providing access to the mobile ecosystem. However, he explained how Yahoo! Widget Platform removes the complexity often associated with working with a range of devices and provides developers and publishers with a simple way to present information to consumers in a manner that is similar regardless of the device used.

Thomas C. Ford, Global Market Strategist, Consumer Products, **Opera Software**, discussed his company's goal to bring the Internet to a host of devices in such a way that enables mobile users to experience the Web as they currently do on their PCs. He noted that the next billion people who connect to the Internet likely will do so by phone. To match the expectations of consumers, browsers have improved and can lay out information in the manner one would expect to see on a PC. For its contribution, Opera Software has developed two browsers: (1) Opera Mobile, and (2) Opera Mini. Whereas Opera Mobile only functions on some devices, Opera Mini is compatible with billions of phones and provides mobile users with interactive, entertaining, and easier access to the Internet. He also noted that his company has built in encryption mechanisms to provide security to consumers as they browse the Web from their mobile phones.

Andrew Elliott, Director of Services and Software, North America Go-to-Market, **Nokia**, stated that to address the evolving expectations of consumers, Nokia has developed the Ovi Platform. For this platform, Elliott highlighted two applications developed by Nokia to provide consumers with a great gaming experience: (1) SNAP Mobile, and (2) N-Gage. He stated that SNAP Mobile functions on any mobile device with Java and facilitates the formation of social networks among gamers. He also stated that N-Gage takes gaming to a new level, providing consumers with featured games, a library of games, and a showroom.

Rob Miner, General Manager of Mobile Platforms, **Google Inc.**, suggested two take-away points: (1) all mobile phones are about as powerful and interactive as PCs, and (2) openness is a good thing. He said that in November 2007 Google launched its own open platform, Android. Miner said to help develop the software, Google established an Open Handset Alliance and held a competition to build

applications for use on Android. He noted that his company's goal is to provide the nearly 3 billion users of mobile phones with organized access to information, and to reduce the cost of phones. Miner concluded by advocating for a broader, truly open, platform.

Moderator Ruth Yodaiken, Staff Attorney, FTC Division of Marketing Practices, **FTC**, asked what consumers can do to know whether applications that they download will be compatible with their mobile devices. Boom noted that the Yahoo! browser has a page that informs consumers what applications will work on their phones. Elliott commented that the question will become moot over time because the industry's goal is to make applications work across all devices. That being said, he stated that Nokia has features on its mobile devices that inform consumers about applications that they may use on their phones. Miner noted that the situation for consumers was less than ideal due to "fragmentation," leading consumers to experience applications differently across devices. He said that in the future better platforms would enable applications to function across all devices. Ford noted that Opera Software manually runs tests to ensure that applications run properly on devices.

Next, audience member Alan Chappel stated that he was a fan of the open platform proposed by Google, but questioned whether losing control over the mobile ecosystem would harm consumers by exposing them to mobile spam and spyware. Miner responded that platform builders should take responsibility to provide more security. He cautioned, however, that building higher walls would only provide a false sense of security.

Yodaiken asked what information is used by the platforms and whether the companies have incorporated privacy checks into their systems. Ford suggested that the onus partly should be placed on the application developers to provide security. He noted that his company uses encryption, switches RSA keys, and notifies consumers to safeguard privacy.

To conclude the session, Yodaiken asked what identifying information the companies collect when consumers access their sites. Boom noted that Yahoo! provides an identifier (not specific to the person) when consumers access the site. Elliott noted that while companies do want to capture information about consumers, to protect privacy interests, he stated that companies in their positions require consumers to opt in to gain access to certain services.

#### **Day One, Session 4: Location-Based Services**

This session focused on emerging location-based services, the technology involved in delivering such services, and a discussion of disclosures about tracking and consumer control of location information.

Brian R. Knapp, Chief Privacy Office and Vice President of Corporate Affairs, **Loopt, Inc.** described how marketers are using the ability to determine a mobile device's location to enhance the user's experience. He explained how his company, Loopt, provides a service by which users can track their "friends" location. He said Loopt provides consumers with a choice to share their real-time location with their friends, turn-off of the tracking feature, or spoof their location. He also said that the brand owner is the appropriate entity for providing notice and obtaining a user's consent because the brand owner is the most easily recognizable entity from a consumer's perspective. He urged the

attendees not to accept opt-in consent as a “silver bullet” to all concerns because consumers opt-in without always reading a notice. He said best practices more appropriately address concerns.

Michael F. Altschul, Senior Vice President and General Counsel, **CTIA—The Wireless Association**, described CTIA’s recently published best practices related to location-based services. He said the guidelines were designed to provide flexibility so not to stifle a nascent industry while addressing the need for principals to guide the offering of such services. He said the guidelines were developed to be applied uniformly to any company that offers location-based services because carriers are not the only providers of location-based services.

Altschul provided an overview of the guidelines. He said service providers are required to disclose how location information is used, disclosed, and protected so that a user can make an informed decision regarding the use of location-based services. He also said that after a consumer provides consent to use location-based services, the user must have the ability to revoke that consent. He also provided a list of safeguards that providers must employ to protect a user’s location information. He said the providers must adopt procedures to: (1) protect the security for location information; (2) retain and store location information as long as business needs require; (3) report abuse; (4) comply with laws, in particular, laws regarding the protection of minors; (5) assist in education campaigns; and (6) comply with the guidelines (self-certify).

Alissa Cooper, Chief Computer Scientist, **Center for Democracy and Technology** (“CDT”), said that the CDT believes location information is sensitive information because it is collected all of the time and everywhere, it can reveal potentially sensitive destinations (*e.g.* hospital), provide reveal real-time location (stalking concerns), and can defy a user’s privacy expectation. She said current law does not address concerns, in particular the Telecommunications Act because it applies only to carriers. She said she is concerned that there is not a standard to determine how the government may gain access to location information. Finally, she recommended a baseline consumer privacy law.

Tony Bernard, Vice President of Operations, **Useful Networks**, explained how aggregators serve as intermediary between wireless network operators and third party content providers. He said that location-based service providers should disclose to users how location information will be used, stored, and shared and how the provider will protect the user’s stored data. He also stated that the user should have full control over how the location information will be used.

Tim Lordan, Executive Director, **Internet Education Foundation** described his organization’s educational efforts. He said that the Commission should consider location-based services broadly to determine what consumers consider location information.

Fran Maier, Executive Director, **TRUSTe**, described TRUSTe’s self-regulatory guidelines that were issued in 2004. She identified issues involved in regulating location-based services. Specifically, she said it is difficult to identify which entity (*i.e.* carrier, brand owner, content provider) is in the best position to provide user controls, notice, and obtain a user’s consent. She recommended a standard notice and encouraged companies to use fair information practices. She said the type of notice and required consent will depend on the potential harm associated with the type of service. She said that opt-in consent is not necessary for mobile advertising because the potential harm is minor, but location-

based services should be provided only after providing notice and obtaining opt-in consent. She also indicated that TRUSTe is considering developing a mobile marketing seal.

### **Day One, Session 5: Mobile Advertising and Marketing — The Transition and Adaptation to Mobile Devices and the Small Screen**

This session focused on the general transition of advertising and marketing to mobile devices, discussed mobile-specific advertising campaigns, and addressed issues such as the targeting of advertising in the mobile space and strategies that advertisers use to adjust to small mobile screens. Below is an overview of the six presentations during this session, as well as highlights of the subsequent panel discussion.

#### A. Panelists' Presentations

Hairong Li, Associate Professor of Advertising, **Michigan State University**, stated that personalized mobile phones have become central to increasingly mobile lifestyles. He defined mobile advertising as any communication for promotional purposes by use of mobile devices. He identified two kinds of marketing strategies: (1) the push strategy, and (2) the pull strategy. From the pull strategy, Prof. Li highlighted QR Code, which is commonly used in Japan to provide consumers with coupons and discounts. Based on his mobile advertising research, primarily in Asia, he concluded that:

- The mobile phone is a dream medium for advertisers, but it has not been realized;
- Consumer initiated processes should be the primary form of mobile advertising;
- Mobile phone users are especially sensitive to intrusive advertisements; and
- Added value is the real driver for user acceptance of mobile advertising.

Michael Hanley, Assistant Professor of Advertising, **Ball State University**, discussed his research on incentivized mobile advertising among college students. Prof. Hanley identified three issues with acceptance of mobile advertising: (1) trust, privacy, and control, (2) device experience, and (3) advertising relevance. He also found that increasingly consumers are open to mobile marketing provided that they have an option to choose to receive the advertisements, and the advertisements are relevant. Prof. Hanley said that incentives would provide a positive motivation for college-aged consumers to embrace mobile advertising. Prof. Hanley shared the following findings on mobile trends among college students:

- Incentives are key;
- The annoyance level is not what was expected;
- Consumption of mobile content has slowed;
- Text messaging is the most pervasive mobile content application; and
- The risk associated with mobile advertising has not been a barrier to targeting college students.

Benjamin Ezrick, Senior Strategist of Digital Innovation, **Ogilvy Interactive**, addressed the increased mobile receptiveness among youth. He noted that mobile is going from the “third screen to the first screen.” He stated that over 233 million mobile phones within the US have the ability to access the mobile Internet, yet many do not. He explained that the introduction of the iPhone was significant

for mobile marketers because it introduced a device optimal for mobile browsing. Ezrick provided the following mobile marketing solutions:

- Text message campaigns;
- Wireless Application Protocol (WAP) pages (on and off deck);
- Videos;
- Coupons (by using QR codes, though few U.S. phones currently have this application); and
- Downloadable context.

Jean Berberich, Digital Marketing Innovation Manager – Mobile, **Procter and Gamble**, identified mobile marketing as a way to provide consumers with what they want. She stated that companies should establish and implement privacy guidelines. She also presented a case study that demonstrates that consumers enjoy engaging and interacting with brands via mobile marketing when they have choice, and the advertisements are relevant.

Jim Durrell, Director of Product Management, **Greystripe**, introduced his company as a mobile gaming distributor. He explained that Greystripe provides consumers with easy access to games by combining free gaming with mobile advertising. He stated that there are some concerns whether the games are really free because the normal data charges to use the mobile devices still apply.

Jeff Chester, Executive Director, **Center for Digital Democracy**, stated that consumer interests must be part of the best practices development. He noted that youth have deeply worked mobile devices into their own psycho-social development. He urged children and civil rights groups to take part in the mobile marketing dialogue. He expressed concern that people are being targeted and asked to give up their personal data.

#### B. Highlights of Panel Discussion

The moderators' questions mostly involved challenges associated with launching mobile marketing, and issues facing consumers with mobile marketing interactions. Below are highlights of some of the comments made with respect to this concern.

- Gene Keenan, Vice President of Mobile Services, **Isobar Global**, stated that the Mobile Marketing Association has been proactive by creating guidelines, which is important because the mobile phone is a personal device and equally susceptible to the concerns facing the Internet.
- Marci Troutman, Founder, **Siteminis, Inc.**, expressed concern that the carriers may have too much power and suggested returning control to the retailers.
- Susan Duarte, Counsel for Marketing Practices, **Sprint Nextel Corp.**, stated that carriers are concerned about providing consumers with positive experiences.
- Berberich stated that consumers have a choice about whether to provide information. However, she expressed concern over the how such data is collected and managed.

- Prof. Li expressed concern that with mobile marketing, unlike Internet advertising, consumers' mobile data packages often require them to pay for all connection time.
- Hanley expressed concern that data charges are inhibiting the growth of the mobile Internet because consumers are unclear on the charges that they may incur.

From the audience, Bennet Kelley of the **Internet Law Center**, asked whether there is any evidence of harm from mobile advertising, and questioned why mobile advertising should be treated differently from Internet advertising. Chester responded that the Center for Digital Democracy had filed a complaint and that the FTC had subsequently issued principles suggesting that harm existed. He noted that mobile marketing presents a different harms because mobile is a unique medium.

### **Day Two, Session 6: Managing Your Mobile Device**

This session, which was moderated by Commissioner Leibowitz, focused on the availability of and consumer awareness about mechanisms for managing mobile devices, such as provider-based options for limiting text messages and capping purchases made from cell phones.

Mike Bennett, executive director of Consumer, State and Local Affairs for **AT&T**, stated that his company's goal is for there to be no unexpected charges on customers' wireless bills, full disclosure, and customer peace of mind. He said that all carriers now are offering free content filtering, free blocking of cell phone Internet access, and free purchase blocking. He noted that at AT&T, the purchase blocking function is twice as popular as the content filtering function. AT&T now has a new service, SmartLimits, that, for \$4.99 per month, offers the ability to set limits on the number of text messages, monetary limits on downloads, time-of-day restrictions, and blocking of specific numbers.

Laurie Itkin, director of government affairs for **Cricket Communications**, explained the benefits of flat-rate, unlimited service wireless plans, which Cricket pioneered. Customers are billed in advance, and have no surprises on their bills. In addition, limits can be placed on the amount of premium content that can be purchased, and opt-in is required for downloads. Itkin stated that it is not possible for customers to incur unexpected expenses. Customers can cancel their service at any time, and port their numbers to another carrier.

Susan Grant, director of consumer protection for the **Consumer Federation of America**, expressed concern about inadequate or misleading disclosures concerning unauthorized charges, privacy, unwanted marketing, and marketing to children. She added that all tools to manage accounts should be offered free of charge, and that spam and spyware protections should be automatic. She expressed concern that privacy policies usually do not clearly explain what will happen with customers' personal information, and customers are not in a position to assess this because what is happening is invisible to them. Grant noted that customers may need to change settings to prevent collection of location information and behavioral tracking, and stated her support for a do-not-track registry. She added that sensitive personal information should not be collected, and that customers should not be able to consent to its collection.

In response to questioning, Bennett stated that there is a charge for SmartLimits because it took AT&T three years to develop it; the company has not started advertising this service yet because it is new, and they wanted to ensure that it works well first. Other options are offered free of charge.

Grant was asked about her support for contextual notice, and she emphasized that it is important for notice to appear when it is relevant, for example at the point of risky behavior, in order to be more meaningful.

Concerning service limits, Bennett noted that in customers may specify up to 15 numbers from which text messages would continue to be delivered even if limits placed on the account were reached. Itkin added that her company has a new option that allows unlimited broadband data service at a flat rate.

In terms of consumer education, Grant stated that it is unrealistic to expect consumers to go to companies' web sites for information, and that most customers do not read bill stuffers. Rather, information on account controls should be included in advertising.

### **Day Two, Session 7: Children and Teens**

This session was divided into two parts: marketing to children, and parental controls. The format was a combination of presentations and roundtable discussions.

In part one, marketing to children, Michael Becker, executive vice president of business development for **iLoop Mobile**, reviewed some of the many methods for users to opt in to mobile marketing, such as SMS text messages, click to call, banner ads, Bluetooth, picture recognition via camera phones, QR codes, and viral marketing. He provided several real-world examples of mobile content programs, and discussed best practices, such as requiring opt-in, not using the word "free" when standard rates apply, age verification, clear disclosures, and not charging for downloads until after the content has been delivered.

In response to a question, Becker stated that the key elements that should accompany marketing to children are clear notice of what the offer is about and what the charges are, and "age challenges"—requiring birth date in order to continue. Also, most importantly, consider whether a program that markets to children should be conducted at all. In reference to whether there is a conflict between 18 being the legal age to enter into a contract and marketing to children that involves incurring a charge, Becker stated that it is important that parents educate their children as to proper use of the phone.

Riitta Kokko-Herrala, an attorney with the **Finnish Consumer Agency**, provided an overview of Finland's approach to children's marketing issues. She stated that most children have a cell phone by age 7, and they send a lot of SMS messages, which are cheap; users are only charged for messages that they send, not those received. No marketing to children under 15 is allowed without parental consent. She noted that SMS messages can be used to pay for products, but that currently there is no way to know whether a contracting party is a minor. Best practices include requiring birth date, no purchases by children under 10, parental consent for those under 15, and protection of children from direct invitations to make purchases.

On parental controls, David Diggs, executive director of CTIA's **Wireless Foundation**, reviewed the Get Wise About Wireless campaign, which includes a family contract for responsible cell phone use. He provided an overview of the tools that are offered free of charge by wireless carriers, and noted that in the future, carriers will begin to ask for consumers' business based on their family-friendliness.

Eileen Espejo of **Children Now**, asked that the Children's Online Privacy Protection Act be updated to apply to the mobile ecosystem.

### **Day Two, Session 8: Best Practices**

This session focused on industry best practices and guidelines, how companies participate in self-regulatory programs, and the available tools for limiting potential for fraud and deceptive acts.

Laura Marriott, President, **Mobile Marketing Association ("MMA")**, described MMA's best practices and guidelines for the mobile marketplace. She said that in June MMA would release a more robust best practices related to minors. She discussed some specifics of MMA's guidelines, such as requiring MMA members to obtain a user's prior consent for single rate program offerings, and requiring a double opt-in for premium rate program subscriptions. She also explained how the MMA guidelines are developed through a committee process that solicits feedback from the community at public forums. She described the monitoring and auditing features of MMA's guidelines. She said that through a CTIA program all applications for short code programs are reviewed for compliance with the MMA guidelines. She also explained that there is in-market monitoring to ensure that programs are advertised and promoted in a manner that is consistent with MMA guidelines. She said that when a program is found to be noncompliant, the content provider is notified, given a cure period, and if not corrected, the program is shut-off.

Peter Avery, Principal Administrator, Committee on Consumer Policy, **Organisation for Economic Co-Operation and Development ("OECD")**, discussed his organization's efforts in providing guidance in the mobile space. He said the OECD would release new guidelines that focus on information disclosures, protection of minors, and unauthorized use of mobile handsets and security issues. Peter said that OECD guidelines are generally non-binding and contain no enforcement procedures. He explained as an intra-governmental body, OECD relies on pressure from member countries to encourage compliance. He encouraged industry and policy makers to cooperate with international efforts to address common issues related to the mobile marketplace.

Gary Schwartz, Co-Chair of the Mobile Advertising Committee, **Interactive Advertising Bureau ("IAB")**, explained that IAB views the mobile marketplace as a new interactive marketing channel and is actively supporting its growth. He explained that consumers do not differentiate between "clicks" on the web accessed from a computer and those from a mobile device. He also stated that IAB is developing new guidelines for this channel as it is with all platforms. He indicated that the guidelines will have proactive enforcement mechanisms, but declined to provide specifics because the best practices are not finalized. Schwartz also said the guidelines would likely have a section related to minors.

James Bradford Ramsey, General Counsel and Supervisor/Director – Policy Department, **National Association of Regulatory Utility Commissioners**, said the states play an important role in protecting consumer rights from deceptive acts in the wireless industry. He explained that billing issues continue to be a problem despite the low number of filed complaints. He said consumers are often unaware that they are improperly billed and do not know where to report complaints. He stated that industry cannot resolve the problems on their own because bad actors do not follow self-regulatory best practices and companies have little incentive to cease profitable practices. He said industry could be encouraged to change its behavior through enforcement actions brought by state attorneys general and education.

Alykhan Govani, Head of Business Development, **MX Telecom**, explained that aggregators play a role in monitoring content providers to ensure compliance with industry guidelines. He explained that consumer complaints drive MX Telecom’s review of content, but that his company reviews all short code programs for compliance before the program is submitted to a carrier. He explained that it is not feasible to monitor advertisement changes once a program is approved because of the large volume of advertisements and the ease by which a content provider can modify its program. He said that if alerted to an issue, such as by a consumer complaint or observing a spike in charges, MX Telecom will then review the content and, if necessary, terminate the program.

### **Day Two, Session 9: Mobile Security – Whose Phone Is It Anyway?**

This session provided an overview of security issues facing mobile devices. The presentations focused on inadvertent enabling of unauthorized access (*i.e.*, Bluetooth, Wi-Fi) as well as consumer awareness of risks, including storing data on these devices, and awareness of security measures.

Dave Cole, Senior Director, Consumer Products, **Symantec**, identified the following as stakeholders in mobile security: (1) hardware providers, (2) the cell phone user, (3) merchants, and (4) payment processors. He stated that “Common Warrior,” a virus that infects cell phones, was one threat that spread by Bluetooth and SMS. However, he said that the biggest threat to consumers was the “Taxi Mishap,” or losing one’s cell phone. He stated that consumers could encrypt their information or use mobile anti-virus software to protect against unauthorized access.

Larry Rudolph, Senior Staff Engineer, **VMware**, identified the following with access to consumers’ cell phones: (1) handset manufacturers, (2) operators and carriers, (3) independent software providers, and (4) the cell phone user. He noted that the first three have over the air (“OTA”) capabilities, such that they can upload software onto consumers’ cell phones. Rudolph explained that the default Bluetooth mode set on cell phones is “discoverable,” which permits anyone to deliver text messages to the phones. He stated consumers currently face few viruses and mobile threats because the majority of today’s 3 billion cell phone subscribers have dumb phones, but predicted the number of attacks would increase as consumers switch to smart phones. He said that consumers could only truly protect their data if they removed the secure digital (“SD”) cards from their phones.

Mark W. Henderson, Senior Analyst, **United States Computer Emergency Readiness Team (US-CERT)**, stated that there are two categories of OTA threats: (1) structured threats (*e.g.*, whaling), and (2) unstructured threats (*e.g.*, unsolicited text messages). He noted that consumers risk unauthorized access to data stored in cell phones unless they password protect their phones. He encouraged

consumers to protect themselves by disabling unused services on their phones and using secure modes on applications.

Moderator Philip Tumminio, Staff Attorney, FTC Division of Marketing Practices, **FTC**, asked whether Google's open Android platform exposes consumers to mobile threats. Rudolph stated that Android permits third parties to obtain location and voice data from phones. Henderson suggested following vendors' security measures.

A member of the audience asked whether there is a secure way to dispose of or recycle cell phones. Henderson suggested returning the handsets to the providers or destroying the phones. Rudolph cautioned that it is difficult to completely remove data from phones because SD cards are now built into many cell phones. Sally Mann of the **Council of Better Business Bureau** asked how, with the rise of environmentalism, consumers may safely dispose of their phones. David Diggs, Executive Director, **The Wireless Foundation**, responded that cell phones no longer contain chemicals that once posed a hazard to the environment. He also stated that most consumers can delete their data.

Tumminio asked how easy it is to install security software onto mobile phones. Cole responded that the installation process is difficult, but noted that in the future cell phones may come with security software already loaded. Tumminio also asked whether downloading music from PCs to cell phones will place cell phones at risk of infection. Henderson stated that users could reduce risks of infection by following guidelines and best practices.

A member of the **Federation of America** asked about the interception of information by RFID readers. Rudolph stated that information could be read from a mile away.

### **Closing Remarks**

The town hall meeting concluded with remarks by Deputy Director Mary Beth Richards of the FTC Bureau of Consumer Protection. She noted that the deadline for comments and research relating to the mobile marketplace has been extended to June 6, 2008.

She also announced the next town hall meeting, which will take place on July 24 in Seattle, Washington in conjunction with Washington Law School on the topic of contactless technologies.