

>> Okay, everyone. We're going to go ahead and get started here, so feel free to take your seats. And welcome back. Please congratulate yourselves. This is the final panel of the day, and you-all have been a wonderful audience, so thank you. Has everyone settled in? All right. Terrific. My name is Sana Criss, and I am the Spam Coordinator here at the FTC. Admittedly, when I first mentioned that to someone, they said, well, that doesn't sound very good. So I had to clarify, I'm against it. I don't actually coordinate it, I'm against it, and I work with many of my brilliant colleagues to develop strategies for fighting this ongoing spam problem. So this panel is called "Emerging Threats." And what does that mean, and why is it important? We're going to examine all of the things that you've heard about today in terms of how they are affecting other platforms, whether it's mobile devices, social networking web sites, or voice-over-Internet telephony. We're going to examine what are some of the future threats happening and how can we best protect consumers because at the end of day, that's what it's about. Whether it's consumers or customers, we are all trying to achieve the same goal. This panel is important because it gives us an opportunity to really be proactive, and I think -- I'm going to speak for the agency in saying that's something that we really do best. Our first spam-related case was in 1997. Okay? And CAN-SPAM -- the CAN-SPAM Act became effective in 2004. So that's pretty proactive, if you ask me, using our authority under Section 5 to combat fraudulent and deceptive acts, regardless of the platform. And so the industry members before you, they are similarly situated in that they are on guard in terms of being vigilant in protecting their customers from these emerging threats, and they too are very proactive. So let me introduce some of these wonderful panelists today. Next to me is Mike Altschul. He is the Senior Vice President and General Counsel of CTIA - The Wireless Association. Dave Champine, he is the Senior Director of Product Marketing at Cloudmark, which is a provider of carrier-grade message security. Next to Dave is Scott Chasin.

Scott is the Chief Technology Officer for MX Logic, and MX Logic is a provider of managed e-mail and web security services. Scott is also the chairperson on the MOG subcommittee fighting spambots. So he'll have something interesting to add there as well. Next to Scott we have Rick Lane. Hi, Rick. Rick is here, he's with News Corp. He is the Vice President of Government Affairs, and as you all know, News Corp owns MySpace, the social networking web site. Next to Rick we have Christopher Rouland. Chris, he is a Chief Technology Officer and IBM Distinguished Engineer, working with IBM Internet Security Systems, which advises thousands of the world's business organizations and governments. So I think that you will all agree that we have some experts here on this panel, so without further adieu, Mike, would you like to get us started?

>> MICHAEL ALTSCHUL: Okay. Are the slides controlled? Oh, you can control the slides. Thank you, and thanks again for the Federal Trade Commission for inviting us to participate on this panel and convening these two days. I was fortunate enough to participate in the first of the spam forums a little more than - - what is it now? -- four years ago, May 2003. At that time we recognized that wireless spam and malware was going to be an important issue to our industry. CTI represents wireless carriers and their suppliers and indirectly the 240 Americans who are wireless customers. We were a bit behind the rest of the world in rolling out text messaging and some of the data applications and had observed overseas the explosion of spam which really colored and spoiled the user experience. So sometimes being second isn't such a bad idea. We had the opportunity to learn from overseas and were able to deploy our first generation of these data services in a way that has been, I think, while not perfect, remarkably successful in protecting and filtering spam and malware from -- from wireless users and devices. I'm going to be talking about where the industry is going, though, and as we move forward into basically converged Internet devices where phones are increasingly web browsers, we will leave the protection of the walled garden and some of the filters and protections we've provided. So that's a little bit of background as to how we got started and what I'm going to be talking about. We now have, by our measurements, as I said, 240

million subscribers, and more than half of them have devices which can be used as Internet browsers of one kind or another. 56% of wireless devices in the U.S. can access the public Internet. The first slide that you see before you just makes the point that anywhere you can go from your desktop using a cable modem, DSL line, satellite broadband over power line, WiMax, WiFi, whatever, increasingly you can use commercial wireless device to get to. Little bit surprising if you haven't used it yourself, but in the last year, 18 months, our industry has aggressively rolled out what are called 3G, third generation, services that now offer true broadband speeds. Now, there's a debate in broadband policy circles as to what is broadband speeds, so we haven't used that term so much as identifying equivalents to DSL, which is the typical telephone company offering, or -- or cable modem services. But each of the national carriers, regardless of their technology, is now offering DSL-like speeds to their customers, particularly in the major markets, and increasingly in the smaller markets across America. And Sprint has announced for later this year the deployment of the first fourth generation broadband wireless service. WiMax is the name of the technology, technology that's offering a theoretical maximum download speed of 20 megabits per second, which puts it in sort of cable modem territory. We're going to have the opportunity in the Washington market and in Chicago to be the early adapters and to actually see how -- early adopters, not adapters -- to see how close they come to these speeds because Washington and Chicago are going to be the first test markets, trial markets to be turned on. As the third slide shows, consumers increasingly are using wireless phones and devices to access information, and the form factor is changing accordingly so that we are all familiar with the iPhone. I almost brought our office one today, but somebody else had checked it out. The screens and functions are less and less like a traditional telephone and more and more like a screen on a laptop or PDA. So there's a wonderful -- a couple of wonderful web sites that you can go to and see all the different products that are available in the market in the U.S. We've counted more than 200 of these 3G broadband devices. And they include something called air cards. It's basically a card

that slides into the port on any laptop and is basically wireless broadband connection that will allow a laptop to do anything a -- a wired connection to the Internet will provide. This is just a partial list of the number of -- of handsets with web browsers. You may recognize some of the names. And similarly, another way of accessing the Internet using wireless devices is with WiFi. There's WiFi in this room. If you have a WiFi enabled smartphome, you can get to the Internet either using the carrier's commercial spectrum or using WiFi from any WiFi hot spot. The industry has the benefit of the CAN-SPAM Act that I think you're all familiar with, and in particular, the FCC implemented CAN-SPAM with particular rules for commercial mobile services so as to prohibit the sending of any unsolicited commercial messages to wireless devices, and the FCC has created a web site and a registry much like the do not call registry, where wireless carriers are obligated to list or provide lists of the domain names that they have in use for wireless devices, and spammers, at least law-abiding spammers, are obligated to go to that web site, download the list, and not send messages. Carriers have been aggressive in going after and suing those spammers they can find in the U.S. and who have not been diligent about this, as heard on the earlier panel, and you all know most of the spam seems to come from outside the U.S. But we do have legal protections which are unique to -- to wireless devices. You probably all know that there are at least two types of wireless messages. One -- I'm going to hold up my own personal BlackBerry as an example here. One is something called SMS or short message service, and MMS messages. These are primarily peer-to-peer text messages sent from one mobile device to another, and then the other are e-mail addresses, which are sent just as an e-mail message is sent from any computer to any other e-mail address. The distinguishing feature for an SMS message is it uses a telephone number, a North America ten-digit telephone number, as the address, and is limited to 160 characters as a message set. And e-mail uses the traditional Internet domain address with the at sign and a high-level domain name. This one BlackBerry has five different addresses. I can get the identical message sent to this device and I can send the identical message from this device five different ways. First,

I can receive and send SMS messages just to my phone number. For those lawyers in the room, SMS messages probably are not covered by CAN-SPAM, but they're covered by the Communications Act because they use the phone number as an address. I also can use a pin. BlackBerry has its own server, and all BlackBerry devices have a serial number, basically, a pin, and if you know -- and we know in our office the pins of all the users -- you can use that pin as an address. The message will never go to the public switched network or the public Internet, it will just go to the BlackBerry server and then back down to another BlackBerry device. And as it turns out, during September 11th, pin-to-pin BlackBerry messages were probably the most reliable, least delayed ways of communicating because they really didn't touch the public Internet. Also, at that time, there were a lot fewer BlackBerry users than there are today. I also can get -- receive a message sent over the Internet using the AT&T gateway to this device if use my wireless number at ATT.net. That is something subject to CAN-SPAM. It's a traditional e-mail message sent over the public Internet. It goes through a gateway that AT&T provides for its users. There is spam filtering and malware filtering at that gateway, and it is then delivered to this device. Because it's a BlackBerry, it also mirrors my desktop at work, so my office e-mail address, all those messages show up on my BlackBerry device, and I can respond and send messages using my office e-mail address. And I have downloaded a Google application which also synchronizes my personal Gmail account to this device, so just as I can get all the e-mail sent to me at my work address, all of the personal e-mail sent to my Gmail account also comes. So if you counted those, there are five different addresses with at least, you know, two sets of legal rules and five different ways of introducing spam and malware into this device. So those are some of the challenges that we're all facing. While it's possible to send spam messages through the carriers' gateways, one or two messages at a time, the carrier gateways have been very effective in filtering -- in identifying and filtering out real spam attacks. So while one or two may slip by, first it's cumbersome to send multiple messages to a large list or to certainly all the users using phone numbers, and they're very

effective in identifying spam-like messages. When you start moving to e-mail and e-mail that comes to devices like this from outside of carrier gateways, my protection from spam on my office e-mail is only as good as our office IT department's protection. My protection from spam on my Gmail account is only as good as what Google and Gmail provide, what I may provide for myself. One of the -- I'm not going to get into the debate about Net neutrality and, you know, the proliferation of devices. I know someone from Consumer Union is here. Consumer Reports every February reports on wireless devices, and they hate the fact that there are so many different operating systems, so many different technologies. We have GSM, Microsoft OS, and so on. In an ironic way, that has been very good protection for users from malware because there are so many different standards and technologies being used and no one truly dominant operating system or technology. The diversity and robustness we have had as an industry I think has been a benefit. Just as sorts of the Apple/Microsoft operating systems have been more of a benefit to the Apple model. Summarily, as we move from closed systems and wall garden kind of applications to more open access to the Internet, more open access to side loading and downloading content and applications on these devices, carriers' ability to protect and vouch for the security of the network and the applications is going to -- to diminish. This is just natural. The same thing happened when the original Prodigy -- when users demanded more openness than the original Prodigy model or even the original AOL-walled garden model provided. So we started in an environment where carriers operated under pretty much of a closed, walled garden environment. As users have gotten more and more experience with the Internet and with wireless device, they are demanding more openness, more applications, and with that users are going to have to start taking more responsibility, just as we do with our own desktop situations for protecting themselves against malware and spam and will not be able to rely as heavily on carriers and networks to do it for them because carriers and networks are going to have much less control over the user experience. It's not good or bad or a trade-off. It's just what's going to happen as the industry responds to the public's desire for more

open access. So I think that's pretty much it. I just always want to close with a final slide which, at least to me, I find amazing. This is a graph taken from the FCC's most recent report on high-speed Internet access services, their so-called broadband report, and they measured the last six months of -- or the time frame from basically January 1 to June a year ago, 2006. And in that time, which is just coinciding with the rollout of 3G networks by the national wireless carriers, 60%, 59% of all new broadband services or customers were wireless, and not our own growth from a low base, but we added more subscribers, subscriber lines, whatever you want to call it, than DSL and cable combined, and we're quite confident when this year's report comes out we're going to see continued extraordinary growth and acceptance of these wireless services. So with that, thank you very much. >> SANA COLEMAN CRISS: Thank you, Mike. That was a terrific, terrific overview. (Applause) 240 million American wireless customers and 56% of them are accessing the Internet on those wireless devices, so this is certainly an important problem that touches a lot of people. Next we have Dave. Dave, please come on up and tell us about how we can secure all of these customers. >> DAVE CHAMPINE: Sure. Thanks. See. There we are. That's me. Good afternoon. Thanks, everybody, for sticking it out through the last session here. Seems like we've had some great discussions and a lot of consistency, so that's good to hear as well because that means we can start to standardize on practices as well as policies around these issues. Michael did a great job of painting the backdrop of the wireless industry particularly and some of the advances there. That's one of the areas that I will touch on in terms of my take on emerging threats. Just two seconds, if you're not familiar with Cloudmark, we do work largely with many of the service providers in both the fixed and wireless space. We are a global business, so we do see a lot of spam. So just some of the insights will be from a consumer perspective, but some of the insights will also be from a carrier perspective, since those are our -- our largest customers in our base. So a lot of the economics has been covered, and that's actually great because we need to start thinking about this more as a business problem and less as a

technology problem if we're really going to make progress. A lot of people have already brought up the points that I make on this slide, so that will kind of help me get through this quickly as well. We've already identified that these are, in fact, businesses, and we talked about the different products, so I'll be able to skip over my next slide pretty much specifically. But the one area is kind of market expansion, so I'll drill into that a little bit. So there's new technologies that they're able to exploit, new tactics that they're able to exploit, and we have heard about those and will continue to hear more. But one of the things we need to predict behavior is where do they go next. If we are successful in regulating their behavior in their current tactics, where will they go next? That's the nice thing about -- whoops, that's the nice thing about wireless is that it interferes with microphones. (Laughter). Yours will be even worse, I think. He's got an iPhone, so he is going to have a lot more interference. (Laughter). >> (Off microphone). >> He is just showing off now. (Laughter) In any case, if we see these like a free market and the beauty of the Internet is it creates a global free market, they will move on. They will find other places to ply their wares. So let's try to predict those movements and let's not be caught by surprise like we have been for the last ten years. So we've talked -- you've heard about some of the new products or tactics that these businesses are using. Image spam was a big deal last year, starting to actually see somewhat of a tail-off in that in some respects. It's hard to tell whether that's truly a trend or whether that's just people shifting around their tactics. Botnets are big, and Scott will, I think, drill into that quite a bit more, and we've heard about that. But the targeted spams, social engineering, we started to see a huge increase in those. Social engineering I've heard in a number of contexts in the sessions so far. What I'm referring to here is a combination of things, and it's really just playing on human nature as opposed to using specific technical capabilities. One of the things that we've seen most recently, particularly with new viruses and new outbreaks of spam with the things like the Storm Worm and different variants of that, is the timing of their release. So in one aspect you can use

social engineering to use a compelling subject line, such as take a look at the video attached of the latest European storm. Another one is sending out a message on a day when traditional antivirus firms are going to be slow to respond because they have researchers who are human who need to be able to take a look at that, they need to be able to reverse engineer it in order to put out a patch. Well, the attackers are getting more sophisticated, and they're saying, well, why don't I just release that on Saturday night right before Easter, when those people will be home with their families, they won't be able to respond, and I'll have a window of opportunity to infect more computers if I -- if I take advantage of that social aspect of engineering. So there's a number of sophistications along social engineering. We have heard about the -- you know, some of the terrorist aspects and ransom aspects, so I won't go into those, but I think it's interesting to point out that there are other trends along those lines. So let's talk about the new markets. It's not just for e-mail anymore. Wherever you look, instant messaging, people are spamming constantly, people are doing harvesting attacks against all the major instant messaging providers. Comments in blogs are pretty much becoming saturated with spam. And it's pretty annoying, and it's -- you know, there's a whole debate whether CAPTA is effective anymore in actually registering blog users and things like that, but you are finding spam becoming an issue in blogs and news feeds. Social networks, I'm sure we'll hear much more about with respect to MySpace, but Web 2.0 is a big concern there as well, it's another vector for people to exploit because you're out there double-clicking on stuff, and that's a great way to get into your computer. So, the big area, though, that we ought to pay attention to is mobile. And really if you take a look at this from a macroeconomic perspective, this is ready to burst. What we've been creating and what CTIA has done a great job of creating is in North America, U.S. particularly what we're concerned with here in this audience, is ready to explode as it has in other markets. We're not used to being late technology adopters in the U.S. We're used to being a mass exporter of technology. But if you take a look at different markets around the world, particularly in Asia and Europe, where they've had

these 3G networks in place for longer and there is no such thing as a smartphone in Korea, for instance, it's just a phone. It happens to be smart. (Laughter). And in that -- in that -- in that region as well, spam on those devices is incredibly high. In fact, in Korea, spam on phones is more common than spam on desktops. And so it's kind of a topsy-turvy model for us to think about. So we do have an opportunity, and because we've got industry support and people working together, we do have an opportunity to get in front of it. But let me drill into it just a tiny bit more. This is a very large, very growing audience, and typically they're uneducated with respect to what the threats are, and we are kind of in a mode of, to borrow a phrase from another Washington person, we're in a phrase of irrational exuberance with the applications and the data services that are being deployed to mobile handsets. Mobile advertising is expected to exceed \$10 billion in the next couple of years. We don't know who's going to get all that money exactly, but somebody's planning on spending it, and they're expecting the consumers to respond in a positive way. There's also a lot of expectations on mobile commerce and mobile banking and mobile peer-to-peer payments and things like this. Well, there's a lot of high expectations that require a lot of trust and a lot of security that just isn't there and a lot of education that absolutely isn't there, so we need to be very careful and very cautious. Basically, I'll break these down into two categories. I won't go into a lot of technical detail, just kind of spell out where things are coming from. Michael mentioned the wireline-to-wireless convergence, technology that is able to bridge all of these, you are starting to see a lot of triple-play and quad-play conversions between your wire servers offerings wireless as well. It's great, but it's opened up the walls to the walled gardens. There's also convergence in the handsets, convergence in the operating systems, which has been a barrier, which is now going to drive more abuse or more opportunity for abuse. So then we have wireless-specific threats. So spam is an obvious one, but we are not a great user of SMS here, so we haven't experienced it all that much, although people who are heavy users, according to some surveys, 18%, 20% have already experienced it here in the U.S. Smishing,

SMS phishing, you can imagine. The problem here is that as we've talked about with phishing, a lot of it is about education and being able to determine what's a legitimate link and what's not. Well, on a screen this big, you don't really have the same kind of tools or visibility into whether that is the a safe link. All you have a button to click okay. If my choice is to click okay, I'm going to do that pretty often. There are a number of exploits already on Symbian OS, which is the most popular operating systems for mobile. There are new threats all the time iPhone creates a great opportunity as we're starting to see convergence between desktop systems and operations and mobile systems. And there's a number of threat vectors already out there. So what I would leave you with is what are the considerations about this, and why is -- why is this one worth particular consideration as opposed to just kind of doing a doom and gloom scenario on this. Let's think about these issues, let's address them before they become a real problem. Young people are the primary users of mobile messaging. As I look around this audience, with all due respect, I would not expect that you're heavy SMS users. If you have children, though, I would expect that they are. If you haven't already gotten a -- an unlimited SMS plan and you have a teenager, I highly encourage you to because you're spending lots of money. I'm sure CTIA members appreciate that, but it's -- it's interesting. They have a nearly unlimited appetite. But that brings up a negative side. That makes youth more of a target because they are the largest segment using this, and so that's a concern that we should pay attention to. There's a different aspect. Mobile bullying is a big deal in the UK, people sending images of kids who have been beaten up, people sending threatening messages to other people. The problem is that a lot of parents give their kids cell phones as a safety line so that they can always get in touch with them, so they always want them to have them, but the -- that same safety line is being abused by their peers to bully them. Now, I don't know what you can do about this necessarily that you would -- you know, you need to take some of the same stands. But the point is that there are different issues at play than we would find in a fixed-line world, and they're harder to monitor because they're so distributed. The

ISPs, in this case, the mobile carriers often have more at stake as well. This can be an identification device. This can be a payment method. And the wireless carrier has a different relationship to that subscriber than a e-mail provider does. An e-mail provider basically is just a flow-through, and they bear no responsibility. They're just a channel. Whereas, with the wireless carrier, they have a totally different set of regulations, they have a totally different set of expectations, and on a regular basis they are bearing the liability for this fraud. And as I mentioned already, it's difficult to manage this, it's difficult to deploy the right kind of tools because there are so many different platforms. And fundamentally, consumers want features first and security later, so it's being very, you know, widely marketed that you have Safari on your phone and you have OSx on your iPhone. That is a great feature, but it's also potentially a security challenge. So we need to keep these -- keep these in mind. It's coming our way, and we have a chance to get in front of it. So thank you for your attention, and on to the rest of the panel. >> SANA COLEMAN
CRISS: All right. Thank you, Dave. Thank you. (Applause). Next we have Scott Chasin to tell us a bit more about this year, and Scott, as you make your way, Dave used a term "smishing," SMS plus phishing. I want to tell you I read today that ginormous is now a word in the dictionary, gigantic and enormous. So I encourage you all to use smishing as often as you like. Continue. Scott, tell us your point on this. >>
SCOTT CHASIN: I am just here to demo the iPhone, I think. I am the local fan boy. So in the interest of time, I have a presentation that I'll give you that really is regarding botnets and the evolution of botnets. That's where I spend a lot of my time today. The CTO of MX Logic. Some of this presentation is a bit technical, so if you're not an engineer, I'll do my best to bring it up a level. One interesting note on mobile spam in Japan -- I've been spending a lot of time in Japan recently -- spam is a huge issue on the mobile phones there. DoCoMo has an incredible amount of saturation of spam on their networks. And the biggest solution that the end users have found is simply to change their e-mail address, and that's partly because there's not a real good technology solution that won't impact the

operator's revenue, since each of the phone users actually pay per message that's inbound. Right? And that's a challenge, I think, that we have that spans across a lot of different devices, a lot of different markets, and it's a -- and I'm going to talk a lot about push and pull -- of how this problem is going to emanate and evolve and impact a lot of different economic infrastructure. So that said, I'm going to talk about the evolution of botnets, and really I only have three slides. I know we're getting into the stretch here. And I'm going to talk historically about what we've seen on the botnet evolution and then really where we're going and give you some examples that will highlight the future. For those of you that probably remember this, in 1988, Robert Chapman Morris created the Internet worm, which used remote scanning vulnerability checks to saturate the Internet. And it spread very, very quickly. That was almost 20 years ago, and here we are today where remote vulnerability testing is still a very valid opportunity for the propagation of worms, not only worms, but the infection of Trojans to create botnets. This push evolution, though, quickly, I think, scaled into the e-mail medium in that the social engineering aspects of e-mail-laden viruses and associated attachments quickly, I think, became news topics and had a lot of success in the '90s. You know, if you remember Melissa and Kournikova, then obviously not too long ago the Sobig and the Mydooms, we saw just a huge wave of -- of, you know, e-mail worms hit the net, largely being propagated by kind of the egocentric, you know, hackers. And I think everybody is in agreement here that times have changed. We've now moved away from, you know, the ego-driven motivations of those that want to create viruses to make a name for themselves, like the '80s hackers did, and now into this new world of organized crime and financial motivation. But that's also, I think, impacted the evolution of how these technologies are developed and deployed. So we've seen e-mail with social engineering wrapped around attachments which were malicious. We're now seeing e-mail, obviously, that have social-engineered URLs, click on this link, then something malicious happens if you do. We have seen within the last couple of years the push mechanic of simply sending out an e-mail that takes advantage of some kind of exploit in your

mail client that then infects your machine simply by viewing the e-mail message. Then we've also seen the automatic execution of attachments that are embedded in messages. Now we're seeing quite common other exploits that are being taken advantage of in common attachments, right, so whether you're talking about office documents or PDFs, these are things that are being targeted. But I would -- I would say that the push method, which has largely been a random shot-gun opportunity for the attackers, is slowly going to decline in its favor and make way for the pull evolution, and that's a random rove bullet point that's infiltrated my presentation. (Laughter). But the -- the move to pull, I think, really represents a reaction to what the industry has done over the last few years, and that is we've created inbound, you know, filtering barriers, and so whether you're talking about inbound content filtering or home firewalls or other inbound security solutions, we've started to drive, in a sense, the threat vector to a pull mechanic. And what that means is that we're seeing oftentimes the threat come down off of a -- an end user click, off of a download where you have some kind of bundled, malicious application that's coexisting with some kind of Trojan carrot, you know, screen saver, I think, application was mentioned earlier. You have even bigger of a threat, the web injection techniques that are being used, taking advantage of browser exploits, leveraging iframes, JavaScript, and with that I think you have what quite could be the big sleeping giant here, which is the cross-site scripting, cross-site scripting forgery issues, which are just now coming to light, really, over the last couple of years, and I think will have an enormous impact on the Web 2.0 infrastructure and industry, and I'll talk more about that hopefully with the panel as well. So this push versus pull evolution is interesting when you start to really look at, you know, the technology and what's driving botnets, really, which is going to be the command and control. We've come a long way from IRC command and control. It's still, however, a low-hanging fruit for what we call the script bots out there, bots that you simply download and install to create your own little botnet are using IRC channels to communicate. But these things are easy to detect, and a lot of the service providers -- one of my roles is chairman of the

botnet subcommittee at MOG, so we get to explore a lot of different methodologies of detection models, and obviously the little hanging fruit here is to be able to detect outbound IRC packets, essentially command and control packets for these bots which are affecting these very large pools of consumers inside of an ISP's network. That's pretty easy to do. What's difficult is when they start using peer-to-peer technology. Or what's difficult is when they start using encryption. So encryption is a very powerful weapon when it comes to how the facilitators of these botnets are controlling each of the infected peers. It means that we can't do deep-packet inspection. It means that we can't use, you know, (Incomprehensible) within the network layer to look for certain characteristics or behavior which might allow us to tell whether this machine was infected or not. So in a lot of ways, the use of encryption is going to spoil a lot of detection capabilities that we know of today, so when I look out in the future, I see two things with bot command and control, again, which is a very powerful thing from a detection perspective that we have to understand. One is the use of encryption, and the second is the use of peer-to-peer networks where essentially there is no single facilitator. Each of the infected machines in the network itself has the ability to pass along command and control instructions to each of its peers. Thus, in fact, if you cut the head off the snake, it still lives. So this is a very difficult thing on the detection side. The other aspect of that is that we're starting to see more and more advancement in the stealth capabilities of the bot infection. We're starting to see the use of basically embedding any kind of command and control packets in high-volume, common transactions, HTTP, from IRC to HTTP. I mean, it's only a matter of time before things like TCP knocking in other types of arbitrary data that's passed through traditional heavily used protocols will also hamper detection efforts, putting us, again, behind from a technology perspective in understanding who's infected and exactly how that infection is occurring. With that we have now the Web 2.0 cross-site encrypting. So you have these criminal organizations, which are building these botnets and facilitating then going out and doing whatever they can to hijack public web

sites, either because of web site insecurities, because the web site is misconfigured, because the web site allows for contributor content to somehow allow the attacker to manipulate those configurations, or because of some other affiliate that is injecting, you know, a banner ad that has JavaScript banner to that site where it is passed through four different sites and presented to a trusted web site. To these are very serious issues in the pull mechanic as the facilitators are quickly learning that by placing malicious code on a compromised web site, they can now very easily test different forms of malicious JavaScript or browser vulnerabilities very easily without that shot-gun, random approach of the push mechanic. The Web 2.0 cross-site scripting issues are very real in that it comes down to stateless authenticated sessions allowing an attacker basically to use your own credentials. Let's say you being logged in to Amazon, you being on a malicious web site, the attacker directs your screen to do a one-click purchase. That's a cross-site forgery, it's a very real threat and one that could become even more prevalent. I know very recently, as of a couple weeks, there are some very high-level consumer and commercial security devices, firewalls, whatnot, that were found to be very vulnerable to cross-site scripting attacks. Another mechanic of the pull evolution of botnets is the use of obfuscation, and this is a very challenging, again, from a researcher perspective, a very challenging issue in that botnets are leveraging more and more stealth, and especially the ones that hang out on hijacked web servers. They're obfuscating that JavaScript code. Even more than that, they're using invasion tactics where they'll present themselves one time to an infected user, and if a researcher tries to go back to that web site to see exactly what's being presented from a code perspective, it's gone. So they're actually becoming very smart about who they attack, so invasion, stealth, and encryption is going to enable more infection and even more important the -- I think the survival times, the long evident of these infections to occur at higher rates. So that said, some other points that I have that are not in this presentation, you know, it's spam, spam, spam, but it's really about bots, so bots are the majority driver of spam today around the world, and I see the future of bots

continuing to evolve. I see lots and lots of challenges, not only on the detection side but also on the remediation side. So with botnets, historically it's all centered around resource acquisition, right, and we saw very early botnets go out, bot masters, facilitators go out and try to harvest as many bots as they could to gain control of as many machines as they could in order to spam victims or in order to hijack credentials, et cetera. That's changed somewhat as we've seen lower-volume, high-value attacks occur, where bots are targeted toward specific institutions or specific individuals. This is also, I think, relevant to some of the newer waves of government phishing attacks that we've seen, government-represented phishing attacks that we've seen very recently over the last few months. So botnet resource acquisition is interesting. Today obviously they focus on your consumer broadband-connected PC, but you can easily imagine tomorrow it will be your television or perhaps your Apple TV box or perhaps your -- your iPhone. So the acquisition of resources is vital for their survival, but even more so, what they are doing, which is also testing our capabilities in the react detection methodologies we have today is that they're testing us, and so for every defense or barrier that we put into place, they now benchmark us as to our reaction time when we release a new signature, how we distribute that signature. So it's very common for these facilitators to now create very polymorphic binaries for these bots and do so at a scale which can't compete with our existing resources that we have on the reactive antivirus signature side. So that's a key, I think, and crucial point that we have to look at is the scalability that we have today versus the scalability that they will have today as well as tomorrow and how that evolves. A couple more points, then I'll release the podium. Another thing that I think that you have to look at -- and I think this is a nice segue -- is when I look at spam and I look at spam in the context of not just e-mail but all the different communication mediums, you know, spam or spit or whatever, it's spam. Obviously, today it's e-mail focused, it's blog focused, comment spam, it's social networking focused, but that's rapidly changing. The definition is basically wherever the consumer attention span is, that's where you'll find spam. So today it's

in your in box, tomorrow it's in your voicemail, but also think about virtual worlds, virtual economies, on-line massively multi-player games. All of these are experiencing record amounts of fraudulent transactions and spam that's associated with these different mediums. That's it. Thank you. >> SANA COLEMAN CRISS: Great. Terrific. Thank you. Thanks so much, Scott. I think -- (Applause) -- a little bit later we're going to want to explore those bot theories and actually how it is affecting or could affect mobile, so let's reserve that for the discussion period. Rick Lane, come on down. MySpace. >> RICK LANE: Thank you very much. First of all, I'd like to thank the Federal Trade Commission for asking me here today. This is an important problem that needs to be addressed, not just for MySpace and its 182 million registered users but a problem that needs to be addressed because it's negatively affecting the user experience for users across all social networking sites. MySpace, as you know, is a social networking site that allows members to create unique personal profiles on-line and communicate with their friends. MySpace is extraordinary success and good will is based in large part on the special experience it creates for its users. A critical part of this experience is the users' ability to access the large network of members on MySpace. However, like all large communication networks, from the telephone to the fax machine to e-mail, there are always those who are willing to misuse the technologies to the detriment of others in order to make a profit, as we've been hearing today. MySpace is committed to making our community as safe and enjoyable as possible for all of our members, and this is an ongoing process that we are constantly reviewing and updating under the leadership of our Chief Security Officer and a world-class technology and product team and the 200-plus person support organization. In fact, we're looking for another lawyer and two investigators if anyone's out there looking for a job. >> SANA COLEMAN CRISS: No one from the FTC submit. It's not allowed. >> We believe there's no single solution to the challenges of Internet security. MySpace employs a wide variety of methods to help protect our community. Every policy we create, campaign we launch, and tool we employ will always be part of a larger solution. At MySpace, we have taken a

comprehensive approach, which includes both technology, partnerships, legal tools, and education. Some of our back-end features that we have instituted at MySpace is -- one is phish lock. Phish lock is a technology, a tool we use that will automatically lock someone's profile if we believe it's being used for phishing purposes, and in order to stop the massive amount of bulletins that can go out from one site. A user must change his password once they realize it's locked in order to unlock that phish lock and gain access and hopefully gain control of their profile. We've improved filters and use advance filtering technology to prevent spam. We've also limited the amount of e-mails one user can send out each day. As some of you may know, on MySpace, it's an internal e-mail system, it's not an e-mail system that goes outside of the site. We've also implemented MySpace links, which I think is a very interesting tool, that helps us remove bad URLs across all of MySpace. What basically happens is we tag and create a URL -- our own URL is that way once we find a bad URL, we're able to delete it across the entire MySpace network. On the front end -- what did I just do? There we go. On the front end, we have, obviously, the ability, like most of the Internet service providers and others out there, to report spam at any time through a link at the bottom of the MySpace page. You can also have -- block and flag friend requests, which is a mechanism that allows folks who are trying to gain access to your account and block them from getting on. We also block comments, a new feature in the comments section. We heard some of the spamming that is going on is through blogs and comments and other areas, so this allows our users to block that as well. MySpace meets with technology partners, like we all do, an law enforcement around the country to solicit their viewpoints and how we can not only enhance our user security but also support their efforts at every level. One of the more exciting things is working with Microsoft. Obviously, when we find someone phishing on our site and we find the URL, handing it off to Microsoft, who puts it in the database, and once that URL is identified, hopefully it will be blocked by others if they're trying to gain access to that URL. MySpace has also taken a series of legal actions over the last two years to combat spam,

phishing, and other misuse of the MySpace site. We have filed suits against Sanford Wallace and Scott Richter for violations of laws including the CAN-SPAM Act and California antispam act. We have found 10,000 e-mails advertising restricters on MySpace alone. Assisting law enforcement and taking criminal action against the Samy worm -- it says Samy work here but that's because I was doing it on vacation and sometimes you don't pay attention to what you're putting in a slide show -- and the operators of the MySpace plus. One of the most notable cases we've had and successfully was against theglobe.com in June 2006. One of the best things that we felt that came out of that was that the federal court found theglobe.com liable for violations of MySpace's terms of service, which prohibit unsolicited electronic communications and impose liquidated damages of \$50 per e-mail. The court ruled that MySpace was entitled to recover 5.5 million in liquidated damages, and this was the first court ruling in the United States enforcing a liquidated damages provision, such as the one that was found on MySpace's terms of service. Educating our users is one of the most critical issues that we all agree, I think, in this room is necessary of trying to ensure that they are protecting themselves. As was mentioned by Michael, that as we lose control, it's going to be the empowerment of our users to help us protect against unwanted spam. One of the mechanisms we use is a very popular use, Tom Anderson. Tom is your first friend on MySpace, and when you sign up for MySpace, you see Tom. In fact, my nieces, who are 17 and 18 years old think the only reason I have any coolness at all is I know Tom. But besides that, you know, he's somebody who, when he sends out a message, people respond, people read it. And we have used that to help explain to our users about spam phishing and provide them with safety tips so that way they have the tools and knowledge to help protect themselves. When we send those out, that has led to members of our community telling us about phishing URLs that they're aware of so we may be able to take the appropriate action. When I testified in front of Congress in 2001 -- it seems like it's been, you know, longer than that, but 2001 -- on the spam legislation, I emphasized that the goal of any legislation regulating the use of commercial e-mail must not

hinder legitimate businesses from reaching out to potential clients but must specifically target the clear abuses. I believe the CAN-SPAM Act has provided the federal government and businesses with effective tools to go after those individuals. However, we may have reached a time to examine if additional legislation is needed to create an even greater deterrent for those who continue to clog our e-mail systems, social networking sites, and in the future, mobile devices with unwanted spam. Right now it seems that some spammers are treated fines just as a cost of doing business. One step that can be taken without additional legislation is sending more spammers to jail, not just giving them fines. But on the legislative front, some ideas that we have looked at include adding civil forfeiture to the CAN-SPAM Act and creating even more accountability for spammers who hide behind affiliates who do their dirty work in which they profit.

That was something that was mentioned earlier today during the first panel about the problems of affiliates and control thereof. With that, I'm happy to answer any questions, and thank you very much for inviting me here today. >> SANA COLEMAN CRISS: Thank you, Rick. (Applause). Well, terrific. Thanks to all of the panelists. >> (Off microphone). >> SANA COLEMAN CRISS: Oh, my goodness. Chris, I apologize. Talk to us. I know you have some very unique topics to address, so let's hear it. >> CHRISTOPHER ROULAND: Thank you for not forgetting about me. (Laughter). Thank you for having me here. I made a connection with the FTC at the RSA conference early this year in February. I had dinner with Dale Fuller, the former CEO of McAfee, one of RSA's -- and Chairperson Majoras, and I got to talk to her about the future of the FTC no-call list, and she was very interested when I submitted that no-call list would be completely obsolete in 24 to 36 months, as we move to zip and voice-over-IP infrastructure and that we have limited ability to enforce no-call measures against, say, spammers sending messages from Nigeria, Canada, Brazil, or China. Subsequently, I came up to brief her team on that, and that's something we're going to talk about across the panel. What I -- what I have in my slides, however, is kind of a profile of propagation patterns we're seeing from malcode. I thought it was important to frame

where most spam is coming. Most spam we see today is really just payloads from machines, and understanding how it's moving across the network, how they're changing and being optimized for maximum impact is important to understand as we come up with new strategies to defend consumers' machines. I got a little nervous when a couple of the other panelists started to dive into the top of this, but they fortunately didn't spend too much time on it and left me some depth to go into this. This slide's in here.

One of our engineers is actually an artist as well, and came up with these -- these icons as well. My favorite is the sequel injection hypodermic needle there, but the point I'm trying to make here is that if consumers, 79% of consumers already have antivirus, why is there a problem today? And obviously there's a technology gap with the protective measures being used by end users today and the propagation methods that are being executed by VXers, which is the term for the virus writers. There's another term in here I heard mentioned earlier today called drive-by malware. This is an interesting trend, and there was a study by a computer security researcher lately. If you do a search on drive-by malware, you'll find this. It's actually a -- he actually took out an ad on Google, and it was -- it wasn't a pop-up ad, it was an ad on the side of the Google search bar, and it said, is your computer virus-free? Click here to get infected. And he had over 1200 hits in a few hours of people clicking to infect their computers. And so I would submit that if consumers are actually asking to get infected, they may actually not have a chance. (Laughter). And there are some things that we need to learn from there and technologies, I think, remains to be invented to help solve some of this problem. This -- this -- I like to use this model because it's a model of typical viral propagation, and for those who can't see it up here, it's basically a bell curve with a long tail. And this infection pattern represents what we had kind of typically seen in viral attacks. This one has an XX, it was about 20 hours on it. What we see is 100% of intensity here represents the maximum infectable population of users, and there's -- the similar model in epidemiology, it's called the SIR model, and it actually maps pretty well onto computer

malcode and malcode infection rates, and SIR stands for susceptibility infection and resistance. And in the computer world, the susceptible population is the population that is using or operating on a platform that is potentially vulnerable to infection from a piece of malicious code. Infection occurs when the malicious code takes a foothold on those machines, and the resistance or inoculation is actually applied when a sample ever that malcode is transmitted to them, just like we get resistance to disease by becoming inoculated or developing resistance, our computers today have to develop resistance by malcode by receiving a small sample of that malcode, and we call those signatures or updates from antivirus companies. The last slide, 79% of our consumers claim to use antivirus software, so what's not working here? One of the changes we're seeing in propagation models is that this model is not very profitable to a spammer or VXer who is operating for profit because in this long tail of infection, we're seeing users get cleaned up. They develop resistance, they receive resistance, and the malcode goes away. And so this model has been gained so that operators can gain the maximum foothold during their propagation attempts and the least amount of population can develop resistance. So ideally, in a bad guy's shoes, you're going to infect the most amount of population with the least resistance being deployed. There's obviously also a technology gap in that we are depending on a sample to be transmitted. So that means we have to find out -- find a piece of the virus itself, transmit a tiny piece of that out to hundreds of millions of PCs. So we began to see a change in the patterns for malcode propagation a few years ago, and we call this first -- this first change of attack short spam attacks. And interesting enough, working in the AV industry for quite a while, you may not know the fastest way to get an antivirus way to put out an update. The fastest way to get an antivirus company put out an update is to have to the media write about it or publish something about it. It can be the smallest, most innocuous virus or Trojan horse. The fastest way to get an update out is to profile it in the media. It's interesting and the VXers have recognized that. They want to get their malcode out under the radar, if you will, not that the media is a very effective malcode detection source, but it's

simply one vector or source of potentially notification to these AV companies. So what they began to do was combine spam distribution methods with malware propagation methods to get a quick shot of malware out and then subside or stop the propagation very quickly. And these two -- these two characteristics generally lead to fewer notifications, fewer emergency updates, and fewer complaints from customers forcing AV companies to submit -- to transmit out the inoculation to the population. But a -- a more modern -- in the last two years, a more modern type of attack has emerged, and I'll expand a little bit on what Dave talked about, and we're calling these attacks serial variant attacks. These serial variant attacks are completely -- and they're doing it to extend this window of infection. What we actually see in the -- in software engineering, we have a term called QA testing or quality assurance testing, and that's where we test our products to make sure that they work the way they're supposed to. We're actually beginning to see QA testing of viruses, so we're seeing computer viruses that are going through rigorous software engineering methodologies to test to make sure they function properly and, most important, that they're not detected by the AV products. So we see entire families, a family of viruses is a group of computer viruses derived from -- or bots derived from a similar code base that are preengineered at once but designed so that the same inoculation or signature pattern won't catch them, then we begin to see the release on these iterative cycles and closely based intervals, again using the spam-based propagation techniques to transmit these out. And you'll see the timing on these serial windows is designed to really tax both our ability to update our systems as well as tax the traditional AV industry's methods. So there are two examples here. One is the Storm worm, which was mentioned earlier, and the other was W32 Stration, which was really one of the more aggressive types of these worms we've seen. Stration was interesting because it almost iterated on a weekly cycle and operated kind of on a normalized schedule, and the first attack we saw, we saw 32 variants in ten hours. Exactly a week later we saw 61 variants in 24 hours. You can read the rest of these. Again, with the Storm worm, starting this year, we saw a maximum

of 55 variants in 19 hours. Of course, if you're updating your antivirus software once a day, you're going to be 54 variants behind on this attack, and so one of the things I think we have to do is challenge industry to invent new ways to detect and block malicious code. This does, however, lead us to some -- some of the -- the more interesting propagation methods we're seeing in the next generation platforms specifically around mobile devices. And I was actually called out last year to a large mobile carrier in Europe, and it was over a hundred million users, it was an emergency, and they wanted us to clean a piece of malware on their network. They were seeing 5,000 sections a week. I said 5,000 sections a week, doing pretty good with a million users. They said Chris, this malcode destroys the cell phone. The users have to replace the cell phones. That's kind of expensive. If you have to replace 5,000 cell phones a week, we will get on this and fix it for you. We found a way to detect it. What we were seeing were variants of a phone virus called the com warrior virus. It's interesting, there have been about 30 variants viruses affecting phones. They were experimenting with diurnal propagation methods. It allows for one type of propagation in the daytime and a different type in the nighttime. In this case, they found the most effective propagation technique for this virus was actually propagate over the Bluetooth vector over the daytime, so actually turn on your Bluetooth on your phone when you're commuting to work on your train, infect everyone around you via Bluetooth. At night it would turn off your Bluetooth, interesting enough to preserve battery life, and transmit to all the people in your phone book via SMS. Next morning it would start the whole thing over again. We actually saw a version of the worm that propagated only over Bluetooth, but your battery life was limited to a few hours. What was happening is consumers were taking their phone into the store and asking for a new battery or new phone -- (Off microphone). So I think the last point there, to tie in voice over IP -- and we'll talk across the panel in this -- we're seeing these methods apply to bot propagation. I think the code knows no boundaries as to platforms, whether it's iPhones, Symbian, Windows, or other mobile platforms. The last convergence we're going to see is in

the next 18 months in the United States, our mobile carriers will converge voice over IP and mobile handsets. When we get a SIP stack or voice over IP stack on our handsets, that becomes a very attractive way for not only spit, but receiving calls. We have dribs and drabs, two and a half million over here, five on Vonage, a few on Comcast. When our carriers get 250 million users overnight, we are going to have a very target-rich population in which we will begin to see attacks against that population over this new protocol. So I think that was it for me, and we'll go to the panel. >> SANA COLEMAN CRISS: Yes. Thank you so much, Chris. (Applause). So much of this information is just draw-dropping, when you hear about some of these potential threats. What I want to do is spend just two minutes honing in on exactly what are these threats. I want Scott, for example, to tell me how can my mobile phone be turned into a spam bot? Just tell me how that works. >> SCOTT CHASIN: If you have an iPhone, it can't. (Laughter). Spoken like a true fan boy. You know, it's largely going to depend on the security of the operating system. The open paths into that device. I think, obviously, it's been shown -- Chris has mentioned -- that Bluetooth can be an enabler. I think there's lots of different threat vectors that exist. The problem that we have is that we want these things to become more and more advanced, which means more capabilities, so they are resembling, you know, truly a mobile desktop, and I think that the iPhone is a really good example of a device that, within its first few hours of being born, was hacked over and over and over again and continues to be. And so it's only a matter of time before we see that, you know, transmission, the bridge that's built. We've seen it in spots around the world, but I think that it's -- it's -- it's around the corner. It's not here today simply because the bot resource acquisition is just so enamored with our consumer broadband PCs, but there's a lot of different paths in there. >> SANA COLEMAN CRISS: Okay. Okay. That's good. Thanks so much, Scott. Now, a few of us here on this panel, we talked about how what's happening overseas is really a good way of determining what we're going to see here in a few years. I want to hear concrete examples. What's happening? Chris, you gave a good one. >> CHRISTOPHER ROULAND: Sure. Actually,

the -- we studied malicious code from overseas quite a bit, and certain parts of the world we're seeing some more advanced on-line technologies. A great example is Latin America, where PayPal technology is standard in all on-line banking. The new malware we see there is particularly scary. We're calling it state full phishing bots. The way they work is your computer gets infected with this bot. Once you log into the bank, it hijacks your credentials and withdraws via their built-in PayPal functionality money from your account. Normally it wouldn't be a big deal; however, it maintains state or keeps track of the money. When you go to re-render or review your HTML page, it adds that balance back in so your balance appears to be whole. Typically for on-line fraud, you've got 90 days for HCH to remit a fraudulent HCH, and after that it's over. We're seeing this very sophisticated threat, and maintaining on-line transactions is made to defraud the consumer. We have a lot of exposure there as we move to those types of on-line services. >> SANA COLEMAN CRISS: Terrific. Dave, you talked about in Asia they have been using 3G for a while. What can we expect based on what you know? >> DAVE CHAMPINE: We've seen a number of things that are jaw dropping. There was an example I ran across a few days ago called flexi spy. There are products available for sale by pseudo legitimate businesses, and you can literally download this onto Symbian, BlackBerry, or Windows Mobile, and it is a complete espionage tool. You can record voice conversations, you can intercept all SMS messages and e-mails, you can remote-control the device over SMS. So things like this already exist, and they're already serious problems, and it's just that we haven't experienced them here because we don't have the same usage profile as Europe and Asia. >> SANA COLEMAN CRISS: Okay. And are you seeing solutions being developed in Europe and Asia or -- >> Yeah, definitely. Some of it is coming through traditional security vendors. A lot of it is -- is coming through a collaboration of the carriers, the handset manufacturers, and the security firms. That's probably something that -- because it is a bit more of a closed loop, there's more constituents, but at least it is a bit more of a closed loop, we're seeing that more in the mobile space than we have historically in the wired space. >> SANA COLEMAN CRISS:

Dave, you used a great word, "collaboration." That's an ongoing theme for this summit, and I think that's what we'll see here in the States, in the U.S. and North America, that it will be about collaboration between public and private entities, for example, global cooperation, so that's good to highlight. >> Yeah, and I think we have a better opportunity because there aren't as many national boundaries and nationalistic tendencies, hopefully. >> SANA COLEMAN CRISS: Yeah, yeah. Well, good. Well, Mike, I know that you work with hundreds of wireless providers, and your organization can be such a good source of information. Are you guys considering whether or not to kind of get consumer feedback on their experience with malware on their cell phones? Is that something you anticipate being able to -- to study? >> We don't have the visibility, as an industry association, that any of our members and our large members have, but there are industry forum -- or I guess we should say fora, where the subject matter experts from the industry gather regularly and share this information, and we've participated in that. So it is being monitored. It's not necessarily being monitored by CTIA. And again, because it is a global industry, global platforms, we have the benefit of knowing what's going on elsewhere. One of the earlier questions you asked is what else have we seen and what are some of the responses. A couple of years ago I think that everyone was aware of the Bluetooth vulnerability and identify theft basis. There was something I guess that was nicknamed blue snarfing, where if your phone was turned on the Bluetooth port, malware could actually access a lot of stored information in a device and be exported, not over the commercial spectrum, but through the Bluetooth space. Just last month I was visiting -- there's a Bluetooth special interest group here in Washington state, and they were talking about how they have reengineered the Bluetooth specification and interfaces, now release 2.1 or whatever, so as to make Bluetooth more secure. So that kind of iterative learning of vulnerabilities and engineering solutions and then releasing them, you know, that will allow us, we hope, to remain a little bit ahead, a half step ahead, of most of these threats. >> SANA COLEMAN CRISS: Uh-huh. Well, terrific. Rick, you know, we watched in amazement as he talked about the different

cases that MySpace has brought against one of our very own panelists from earlier today, in fact. It sounds like the exploits are just -- they're really taking advantage of technological vulnerabilities. MySpace is uniquely situated. You've got a community, you've got a captive audience, and these technological tools are -- they seem to be easy to use. Can you tell me about what technological steps your guys may be using to -- to thwart the efforts of the bad guys. >> We're always trying to develop new and innovative ways of protecting our users. It really is the biggest complaint we get from users, especially when somebody has hijacked their profile and their friends think that they're sending out these bulletins on different ads for different types of products and services that are out there, and it is really hindering the users' experience. Obviously, there are things that we are looking at and doing and testing that we don't talk about because you don't want to give a roadmap to the bad guys of what we're doing. But you know, looking at working more closely with law enforcement and the cases that -- and the FTC and others to go after those individuals who, again, are using -- someone was talking about social engineering, I think, is the term that someone used. I mean, MySpace and social networking sites are created for interaction, and they are using those vulnerabilities across FaceBook, MySpace, Zanga, and the rest as a way to hijack or sell products or do other malicious things. So there's an educational aspect, as you mentioned, and talking about the technological side, I think the phishing or stop phishing programs that we have and in other areas I think are helpful. But sometimes it's just overwhelming, and you just need to try to figure out through the entire community what can be done. I think giving more tools to our users and having them help report when things are going bad, as we were talking about earlier on CTIA, is going to be one of the most effective tools that we have. >> SANA COLEMAN CRISS: Wonderful. That's good. Getting effective tools, technological tools, that is just another theme that we're hearing throughout the day and we'll hear more about that tomorrow. So thanks for sharing that. Another thing you said, Rick, was the arrests being perhaps the greatest deterrent for these bad guys, and I just want to put a plug in for

tomorrow's panel with criminal law enforcement will be here and present and telling us all about it. So I hope everyone comes back for that. Now, let's open it up to the audience just for a few moments here. Do any of you have any questions for these panelists? Looks like I have one here. Let's take a look. Okay. And one in the back. Okay. Great. Let's start with this one. We've heard about financial motives earlier. What are some of the other motives that spammers have -- have going on for them, and what are some of the motives regarding these -- these emerging threats? Is it financial also, are there other motives here for these guys in terms of targeting mobile phones and social networking web sites? >> I would say no, it's all about the money. >> SANA COLEMAN CRISS: All about the money. Okay. Anybody care to add to that or -- >> I mean, there are trends, and I think that we've seen in recent news, very recent, of using in particular botnets as, you know, weapons, so whether that's, you know, denial of service attack to take down the, you know, critical infrastructure of a government, and we've seen throughout the last four years lots of examples of that, and that's a growing trend. We've also seen the terroristic use of botnets for dissemination of hate messaging, such as the Silver worm and its infections. So there are, outside of economic gains, which I would say is primary today, the motivation, there are trends that can point to, you know, botnets and the delivery capabilities of them and the destruction capabilities of them to -- to be used for malicious purposes or to promote, you know, certain ideologies. So there are good examples of that. >> SANA COLEMAN CRISS: So not just about the money. We've got issues like terrorism, we've got some serious issues here that are at play. That's a good thing to raise. Thank you, Scott. And we have an audience member. >> This is in a similar vein. I mean, I don't understand -- >> SANA COLEMAN CRISS: I'm sorry. I hate to interrupt. Could you state your name and affiliation. >> I'm sorry. I'm Julia Sonja with the FCC. I don't understand the economic incentive of a worm destroying cell phones, assuming it's not made by the manufacturer of the equipment of the replacement phones. What's the economic incentive? >> SANA COLEMAN CRISS: Good question. >> Let me answer a different things that we've observed, which is just a variation on an old

fraud, and it's not very high-tech, but in the U.S. we've had 900 code -- area code numbers which end up generating a premium charge to the caller, and there are some countries in the 809 Caribbean area code that have similar numbers that look like ordinary numbers. So it's been a problem for 20 years or so from wired and wireless phones. The etiquette of wireless phones where you actually will have a call record and many people will take a look, see they've missed a call and want to call back, generated -- has generated sort of a phishing kind of scam where people will call and, either through spoofing or whatever, leave one of these numbers on the caller's phone solely to generate revenue to one of these sites and drive additional revenues to the site. >> Also on the -- so a piece of malcode that destroys a mobile phone is a buggy piece of malcode. Other revenue-generating opportunities available for mobile phone malcode have been leveraging premium SMS services or reprogramming your phone book to dial through an alternate long distance carrier. A good example of one of these phishing attacks, it sends you a message to send a text message in response to a premium service to unsubscribe you from a Spanish dating service. So it keeps sending a text message to your phone asking if you want to unsubscribe to the dating service you've joined for \$10. A lot of people said, jeez, I want this thing off my phone, and they just pay. >> And let me just add that, you know, on the bright side, it's not a pathogen's interest to kill its host. (Laughter). >> I would say that some of this is -- some of this is related to the new frontiersness of it, so a lot of this is just kind of testing the waters, how much can we do. There are instances in India, for instance, where they sent out bulk SMS messages saying there was a various that would actually pass from the phone to the user, and they had, you know, many, many thousands of people responding in great fear. They had SMSs that went out in Lebanon saying that you've won a new car, and they had something like 100,000 people show up at the dealerships. Just creating that kind of chaos in itself is a tool. >> And also in terms of sending out malicious code to distract, you send it over here so everyone's focusing on the right while you're doing very small attacks on the left that no one's noticing because everyone's

focusing on the right, and that's a standard technique as well.

>> SANA COLEMAN CRISS: Okay. Very good. Very good. Yes, sir.

>> Carl Settleman, Federal Trade Commission. I just have a question that sort of anticipates, I think, what's going to be discussed tomorrow in terms of your own views of the emerging threats. What steps, non-technological steps, do you think that agencies like the Federal Trade Commission or that Congress should mandate in terms of trying to get out ahead of this and trying to prevent some of these things from happening, and what sort of suggestions would you-all make in terms of, you know, maybe your top one or two things you would see as being beneficial to consumers in terms of heading off these problems and reducing the aggregate cost that the problems can entail and impose on consumers collectively over the next decade? >>

Certainly, consumer education from as many different voices and corners as possible, industry, the government, everyone has an important role with emerging technologies and emerging threats.

>> I would say along those lines, working closely with -- with the carriers, service providers themselves. They are going through a transition time, particularly in the U.S., and so both helping to reinforce the education, helping to standardize the policies and practices, but also acknowledging that they are switching revenue streams and that, you know, you can't be too Draconian about this. It still needs to be a business venture.

>> I would say it's definitely collaboration and research, more research is needed. And this is, you know, a global epidemic, it's not -- it's not just in the U.S. And you know, the threat vector is so distributed worldwide that we can't take that perspective. So I'm also, in the context of just spam, you know, there's a lot of research, I think, that still needs to be done around how we manage identities on-line. There's, I think, a good opportunity there. I, for one, would really appreciate just having a new sort button on my mail client that could tell me whether or not that message was human originating versus machine originating. That one little thing, obviously, impacts the entire ecosystem of identity, but nonetheless, it's those kind of thoughts that we need to look at from a long-term research perspective. But research and collaboration. >> One of the things I mentioned was providing (Off microphone) --

right now at the federal level and government you have criminal forfeiture, but the government and law enforcement can't go after everybody. They just are limited in their resources, and creating some more teeth that we have on our side to go after individuals I think would be a great deterrent so it's not just a cost of business. On the education side, can't agree more that it's very important. The problem that we find, though, on the education front is, first of all, no one listens, as we heard earlier, and it's the same problem we find on the on-line child safety front is that those who listen are the ones who already know, and those who don't listen are the ones who don't know. It's a very frustrating situation. And getting to those 30% or 40% of the folks who aren't being active on this front is the difficult part, but that's where, as someone mentioned earlier, the vulnerabilities are. And I -- I just don't know how to answer that one. >> There's -- there's been some really interesting work done around sovereign network borders and treating the 26 undersea cables that come into this country as ports of entry and having the borders -- the customs and border protection agency enforce those, just as they would secure physical ports of entry, inspect and block all this -- this crud that's coming into our country and allow law enforcement to focus on problems inside this country instead of sending our own law enforcement guys to Nigeria or Egypt to take these guys down. So I think it's something worth exploration and consideration is to treat these ingress as ports of entry. >> SANA COLEMAN CRISS: Well, terrific. Okay. I think that is our time for today, and I just want to share with you a few of my own observations, and that is I'm echoing the brilliance of these panelists. Again they talk about collaboration, when they talk about filling the technological gap, as someone put it. And this outreach, making sure people listen to what we're telling them about how to prevent problems and how to make our education efforts even better than they are and business education; right? CTIA members, they need to know. All of these providers, they need to know how to secure their systems as they enter into the world of convergence more and more. And so I want to thank you all for highlighting those very important points for us, and I invite everyone to join us again tomorrow

bright and early. Let's hope for good weather. And thank you.
Thank you all. (Applause).

(Session ended at 4:13 p.m. CDT.)

* * *

This text is being provided in a rough draft format.
Communication Access Realtime Translation (CART) is provided in
order to facilitate communication accessibility and may not be a
totally verbatim record of the proceedings.

* * *