

**SESSION 9: MOBILE SECURITY - WHOSE PHONE IS IT ANYWAY?**

MR. TUMMINIO: Good afternoon. My name is Philip Tumminio, and on behalf of the Federal Trade Commission, I would like to welcome you all to our last panel at the end of this town hall.

The late futurist and science fiction author, Arthur C. Clark, said, "Any sufficiently advanced technology is indistinguishable from magic." I bring this quote up not to suggest that the smartphones of tomorrow will be powered with some magic runes or pixie dust, but as a conclusion after two days of hearings and learning that these phones are magical devices, they are the magic wands of our age and they offer an unprecedented level of features, content and creativity, freedom and connectiveness, a means for us to connect to the market and a means for the market to connect to us.

These devices are, indeed, magic and we need to get a hold of them and make them personal. But as this is happening, they are filling up with data and other information about ourselves and perhaps other people. As we feel the need to personalize these devices and to make them our own, other less scrupulous people also feel the need to make our devices their devices and turn something magical into perhaps a bit of a curse.

*For The Record, Inc.*

(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555

This panel is going to focus on mobile security.

We are going to explore the malware threat to your mobile device. Who can access your phone, what kind of information is at risk, what can you do to protect your phone? These are the questions we hope to answer during this panel.

We are very fortunate to have a great depth of experience among these panelists and a wide breadth of experience. All of these panelists have served as panelists before on panels of similar topics and they enjoy a variety of academic, commercial and government learning and practice, which I think will serve us in answering the questions we have raised, as well as the marquee question of this panel, whose phone is it anyway.

So, with great pleasure, let me briefly introduce our security experts. Sitting from my left and following across, we have David Cole. He is a Senior Director for Product Management and the former Director of Security Response at Symantec, a company that provides software and services.

Mark W. Henderson is Senior Analyst at General Dynamics Advanced Information Systems who is supporting the analyst cell within the United States Computer Emergency Readiness Team, also abbreviated USCERT, within the Department of Homeland Security's National Cyber Security

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

Division.

Finally, we have Dr. Larry Rudolph, who currently works as a senior software engineer at VMware, a leading provider of virtualization and software solutions. He is currently on leave from his position as a principal research scientist at the Massachusetts Institute of Technology.

So, Dave, if you could start us off today. I would like to set the stage, if you could identify for us the stakeholders in the mobile security space.

MR. COLE: I will paint it kind of in broad strokes, and I know Larry has some detail he wants to drill into here. So, I will keep mine fairly brief.

First, of course, is the carriers. There are the hardware providers themselves, the handset providers, the operating system providers and working in conjunction with the handset providers as well. Certainly, much more diverse than the PC world that we are accustomed to, with the largest provider having around 60 percent of share, being Symbian.

Then, beyond that, you have the individuals themselves which is where I will spend a moment to talk about.

Overall, we have seen the threat landscape change pretty dramatically over the last really two to three years.

We have gone from an arena where threats were exploiting technology to one where they are predominantly exploiting

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

people now. One of the big threats we have seen in the past 18 months has been called the storm trojan. It spreads so quickly that people initially thought it was a worm. They thought this thing must be self-replicating and bouncing around the internet of its own accord. But the reality was the deception techniques were so effective, and continue to be so effective, that storm is still evolving and is still a significant threat today.

So, the end user, as we look at the PC world and evolving to a mobile device dominated world in the future, is going to continue to be perhaps the most important stakeholder in many ways in the chain. Of course, there are other folks involved as well as where the phone is a payment device as it is in Japan. You have the merchants, you have the payment processors and the providers and so forth there as well. I think that is kind of my overview.

MR. TUMMINIO: Larry, I am going to ask you the same question, but with a slightly different spin. Who has access to the consumer's phone?

MR. RUDOLPH: Everybody except the consumer.

**(Laughter.)**

MR. RUDOLPH: Let me sort of tick them off in these broad categories. I see four stakeholders in your phone. There are the handset manufacturers, Nokia, Motorola,

Samsung and the like. They have their OS, their content on your phone all the time. There are the operators or the carriers, Verizon, T-Mobile and the like, and they have their own stuff. They may put their own browser or their own software on the phone.

There are independent software providers, third party software, mapping software or the like that have some applications that are on your phone. And, finally, there is the user.

But there is something called over the air, OTA.

Some people might have actually gotten the text message saying OTA with some numbers, which means that somebody up over the air, OTA, has upgraded some software on your phone.

That is their sort of message that told you that in this cryptic way.

Who may that be? That may be the handset manufacturers, the carrier or the third party independent software vendor. But, certainly, does the consumer actually know that or can the consumer do anything to their phone?

And the answer is not very much. I want to sort of talk a little bit more about that.

MR. TUMMINIO: I think we will have the opportunity to get to that in just a bit. Mark, we have heard of the storm trojan, OTA delivery. It might be an appropriate time

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

to do the mobile security threat down. If you could give us all the threats, techniques and different procedures that have been used to sort of deliver malware or viruses to a mobile phone. We are looking for the buzz words, the catch words, things you can use to sound either sophisticated or menacing, depending upon the company.

MR. HENDERSON: Sure, sophisticated or menacing.

So, primarily, USCERT, we certainly deal with all four. I think there are four stakeholders right now, right? So, we deal primarily with the U.S. Government and consumers, and the threats that we are seeing to the U.S. Government and to consumers primarily fall into -- I am big fan of Richard Bejtlich. He defines threats as structured and unstructured. Structured threats we see, we call the advanced persistent threat, APT. Those are individuals that are funded.

And the malware they will typically do will come in the form of a social engineering email, we typically call it a spearfish. Now, the new technique now is called whaling, which is you will target, rather than just several VPs, you will target the head CEO or an individual that works specifically on a particular program that you are interested in getting schematics of information from. We also see within that space, we will see the delivery of like root kits.

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

We have not seen a lot as far as M-commerce or mobile threats in that realm.

As far as unstructured threats, we see all the standard viruses that are delivered. In the M-commerce world, I would say probably the network threat would be the biggest thing we would be concerned about, not necessarily individual delivery of specific viruses. I think the number was 400 viruses. We are concerned about the criminal-to-criminal element that is actually using multiple PC phones to create a largescale network. I do not know whether you call that like a bot-net, but the equivalent of a bot-net in the M-commerce world that would allow them to steal information, perform actions.

One of the other things that we are concerned about is phishing. I think they call VoIP phishing, vishing. For mobile commerce, it would be the equivalent of smishing. We create our own words while we are here.

But people that are receiving unsolicited commercial text messages, that is a concern. People that are receiving text messages that are trojan'ed; people that are receiving text messages -- one that was kind of strange that we have not necessarily dealt with as far as mobile threats, but there was a forum of people that had epileptic

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

seizures and someone sent a Java script to that forum that blinked and then people that were epileptic watched their monitor and then had epileptic seizures. So, it was a very strange threat, but that might be something -- an attack on the user. We have not necessarily seen that yet. But it is certainly out there. I am sure there is a laundry list of others that I have potentially missed, but those are the big ones.

MR. TUMMINIO: David, Larry, are there any significant frauds or scams that you would like to highlight that have not been mentioned?

MR. RUDOLPH: So, Bluetooth was -- it is actually really big in Europe as well. There is something called tothing. The idea about Bluetooth is that -- you know, earlier today we talked about if you have Bluetooth on your phone, it was an advertiser's dream. Your phone is open.

When you get a phone and you turn on Bluetooth, there are three modes of Bluetooth. It can be on or off and it can be discoverable or not discoverable and it could be -- if you know the Bluetooth ID, you can get to it even if it is not discoverable.

Phones come on by default to be discoverable. It means that anyone around, like Starbucks or any industry, can blast an ad and send a message to your phone because it

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

can discover your phone's Bluetooth ID and send a message.

What pops up on the screen is saying the name of your phone wants to send you a Bluetooth message, do you want to accept it. So, if I sent you one it would say, Larry wants to send you a message, do you want to accept it. But the scam is, instead of saying Larry, I would say can you meet me in the bathroom, that is the name of the owner of the phone, would you like to accept it. But that whole name takes up the entire screen and you do not see it is sending you a message, do you want to accept it. That comes off the screen.

So, you just see the name, and it just appears on your phone out of nowhere. The problem is that Starbucks, or any industry on the street, or any -- they keep their Bluetooth networks closed. You cannot discover them, but they can discover you. So, the whole thing is sort of reversed. Your phone is open so that people can hand you ads when you walk on the street as opposed to sort of opting in or closing it.

That has been a big threat around for Bluetooth and it has not been reported because it is just like a little annoyance. You get them in the airport all the time if you leave your Bluetooth phone open.

Just an aside, I have been scanning everyone's Bluetooth devices around here. Anyone that had an open

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

Bluetooth device, I actually recorded your name and Bluetooth number with my phone for the heck of it.

MR. TUMMINIO: It will not be part of the record.

MR. RUDOLPH: It will not be part of the record.

**(Laughter.)**

MR. RUDOLPH: I just wanted to say one other thing along that area is that we have not seen that many viruses or threats. There is some phishing and these are disaster, but it actually is very minimal. There is something like three billion subscribers to cell phones. One out of every two persons in the world has a cell phone. Most of those are -- they are called basic phones. I call them dumb phones. They are not really capable of very much. But as time goes on, they will all become smartphones, just the technology is there.

So, the market of smartphones that can get attacked is actually small today, but it is growing exponentially.

In fact, within a few years, there will be three billion smartphones and then we may see things change a lot.

MR. COLE: I would concur with what Larry said. I mean, we really have not seen many mobile threats today.

The biggest one was 2005. It was a threat called Comwarrior, which spread to about 20 different countries. It used

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

Bluetooth, as well as MMS, but in all likelihood, it spread predominantly through MMS, and it really did not have that much of an impact. I mean, bluntly, it did not.

It is kind of funny. We used to do security reviews and I poignantly remember going and doing a security review of a company where they had the servers right next to the Mr. Coffee machine. In the write-up we said, your worst threat is the Folger's, a big Folger's mishap. And I think today, the biggest threat to your phone is the taxi mishap.

It is losing that data that you have not password protected, that you have not encrypted on the phone, which is nonetheless very private and personal and valuable.

So, I think while we can talk about high-tech threats, I mean, the one that stands to affect us all here in the most near future is that. But that is not to say that we should not look at things, like the unsolicited text problem, SMS problem that they have in Asia, Korea, Japan and so forth. There are some interesting lessons we learn from the U.K., as Larry mentioned, and from Asia as we look out at how these technologies can be abused.

MR. TUMMINIO: I would like to follow up and explore the data that can be found on these phones. Cell phone forensics. What, Mark, is found on the average third generation phone today? Who can find it if the phone is lost

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

and then recovered? And what kind of danger are consumers in if it is not properly secured?

MR. HENDERSON: Can I get that one, two, three real quick, and then I will make sure I address all three. The first one, what kind of data, right?

MR. TUMMINIO: Yes.

MR. HENDERSON: How do you explain it?

MR. TUMMINIO: It was your best recollection of item number two, and the third is what can consumers do to protect --

MR. HENDERSON: What can they do, oh, okay. That is a triple threat. Okay, what can you get off of a cell phone? There is a very good document that NIST released on cell phone forensics and you can explore -- I can give you the actual NIST publication, if you would like, later offline.

So, one of the things that you can do is certainly review that NIST publication, but the things you can currently pull off that, you can get geo-location data, you can get personally identifiable information, PI information for that individual. You might be able to get their carrier information. If the individual has stored any information regarding other applications they intentionally connect to through their phone, you might store that locally and that

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

would be cached locally.

Some people currently use their phone as kind of a password keeper on their cell phone. In our environment, we typically cannot carry cell phones where we are. So, people in a commercial world will have like their wife's email account number, their State Farm insurance number, their Social Security Number for their grandmother, all kinds of random information on their phone, and all of that is collectible. If someone gets your phone and it is not password protected, that is not necessarily a problem because there is ways to get around that.

The best suggestion I would have for that would be some phones allow you, after your phone has been lost or stolen, to do a remote wipe of the phone and you can contact certainly tools like -- companies like BlackBerry, Research in Motion allow you to do a remote wipe. It is just making sure you remember the number to call the number when you lose your phone because you do not have your phone.

So, what are some of the causes or some of the ways that you can actually protect against it for consumers?

MR. TUMMINIO: Correct.

MR. HENDERSON: The three main ones that I would suggest would certainly be aware and cognizant of what you put on your phone. Your phone is not a password keeper.

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

You should not be storing all kinds of manner of strange data on it. You should think, worst case scenario, if someone were to get your phone, what would they have access to and protect accordingly.

The first thing we would say to do is disable any services that you do not necessarily use. A lot of phones come on, they already have the infrared port enabled, they have Bluetooth enabled, they might have some kind of wireless capability enabled. If you are not using the service, disable it. If you are using the service, choose a secure means to use. If you are using HTTP for a transaction, intentionally try to use HTTPS.

One of the other things that you can do is with your phone, do not try to store it. We have had a lot of problems with people losing phones or laptops at conferences, leaving them on your chair. That is not a good idea. You do not save your seat by leaving your phone or your laptop on your chair. You lose your seat and your laptop and/or phone.

**(Laughter.)**

MR. HENDERSON: One of the big things that we have seen, and I think I passed some of this information to Phil, was people taking that consumer data, application data that is sensitive and storing it on a cell phone or a laptop in

transit so that they can perform testing. And sometimes the cell phone or laptop will have data it would not normally have and that can potentially be exposed. So, you have to be very aware of that.

MR. TUMMINIO: Your protection methods raise an interesting question. How secure are these devices out of the box? Last time, I got a cell phone, I picked it up, I spent an hour and a half transferring all the numbers from my old one to the new one, and then I started blasting text and making calls. But how safe is the consumer that just neglects to spend a couple minutes with the security features when they break out the new phone? Dave, I will offer that to you first.

MR. COLE: Well I think really security, it is a tale of risk, right, and what they are using the phone for. So, at a base level, if you are not using Bluetooth, as Mark mentioned, turn it off. Set yourself into non-discoverable mode. So, I think that is certainly -- is it a massive exposure? Probably not. It is proximity limited. But should you do it? Absolutely. If you are storing company data, if you are storing all your usernames and passwords, your Social Security Number, all the really sensitive PII, then you need to take more steps. So, I think the security measures that you take on your phone should be

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

the equivalent of the value of the data you are putting on it.

For example, if you are storing your Social Security Number, your credit card numbers and other sensitive information on it, at a minimum, you should be password protecting your device, which I think in most phones you can do. You should be encrypting that, which unfortunately is far too difficult today in most situations if it is available.

So, I think the level of protection that people go through on their phones, such as, in some instances, using mobile anti-virus, which we provide and so forth, really should depend upon what they are doing with that phone.

My wife's flip phone, not so important to put encryption on and mobile anti-virus. My phone, which I use for company email and I have some sensitive information on, absolutely, password protected, and I am cautious about what I do with it and where I put it.

MR. TUMMINIO: Larry, did you have any additional thoughts on the default level of danger or risk that a modern smartphone presents?

MR. RUDOLPH: Yeah, I actually wanted to respond to what Mark said, which are all great suggestions. However, I am not going to listen to any of them. I mean, I am just not. On my phone, I have all my Social Security numbers and

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

my bank stuff and all my passwords. They are on here because it is very convenient to have it on here. I have music, I have videos, I have corporate documents, I have PDF documents.

Of course, I am going to put it on here. Well, if I do not put it on here, I put it on this one. It is a little bigger.

But, yes, I have it on it.

There are -- yes, and it is great to have this service, these lock and wipe services that if you lose your phone, you call up and they are going to lock it and wipe it, provided your phone is turned on. And if I was a thief and I wanted your phone, the first thing I would do is turn it off. And then I would open it up and take out the battery and take out the SD card and now the data is on my SD card and you can do any lock and wipe you want on this thing, but I got the data in my hand. So, that is a problem.

A simple thing that you can do, and it is just part of -- Simpson Garfinkle (phonetic) who is a PC student at MIT, did a lot of work on this, that when you format your disk under Windows or Windows Mobile and it says formatting the disk, so you think if you format the disk, you are going to lose all your data because that is what the sign says, but it does not do anything. So, if you format a disk, it does not wipe out the data, it just wipes out a little directory and you can recreate the data. That is true on

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

Windows Mobile and it is true on PCs, and you really should wipe and clean, erase with some -- certainty on your PC, some third party software. On some phones, it is very hard to get something to really erase the data that is on this SD card. It is very, very hard to even find third party software to do that. So, you maybe think you are wiping it, but you are not really wiping it.

Turning off services? Sure. Anyone here know how to turn off IR? Where is it? In the handbook? Right, right. But, you know, who reads the handbook? Turn off Bluetooth? Well, I use my Bluetooth headset all the time, so I am not going to turn off Bluetooth. Make Bluetooth non-discoverable. Gee, how do you do that and what are the implications? People do not understand that. That should be a default that is non-discoverable, but it is not. So, your suggestions are great; however, practically, they are not really sort of used.

MR. HENDERSON: Well, I think to be fair, most of the time in government space, when you have an enterprise level situation, you are going to follow a checklist and you are typically following secure technical implementation guides, and they have a STIG for cell phones, for smartphones, for laptops, for servers. And when you follow that STIG, if your device is compromised, there is a limited risk because

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

you have gone through and checked all those things.

I am not suggesting that consumers follow a STIG, but if you are not going to read the instructions, you are going to store all of your information on there, you are not going to follow security precautions, you are not going to load security software, then it is kind of like just open the door because we know the threat is potentially increasing, even though we have not seen it. We have only see like -- what was it, in the McAfee report, 10 percent of users are reporting that they have seen an infection.

So, USCERT does not see the M-commerce threat. What we see is people losing their phone, and what is on their phone, their personally identifiable information. And why is that an issue? Because in addition to their information, there are 20,000 other records from a government agency or from their human resources, information. They should not be storing that information on their phone because it is beyond the enclave where they have security controls. So, you just have to be aware of that. Try to store most of that data on the network and then it is not on your phone. If you can store it in a home PC and connect to it, you are in good shape. If it is local, that is a little more difficult.

MR. RUDOLPH: Yeah, that is a really good suggestion. I think Paris Hilton decided to follow that and

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

she put all her phone book on Verizon T-Mobile network and then she lost her phone. But, of course, Verizon did not protect that, her contact list.

MR. COLE: That's private sector.

MR. HENDERSON: Yeah, that is true. I would love to argue with you on T-Mobile security, but that is T-Mobile.

MR. TUMMINIO: I would like to invite questions from the audience at this time, preferably about mobile phones. The Paris Hilton-related, I suppose we can field some of them as well. Three ways to play, question cards, please raise your hand if you have them. We certainly welcome an appearance at one of the microphones, and you can, of course, email the questions to [beyondvoice@ftc.gov](mailto:beyondvoice@ftc.gov).

Commencing some of the audience questions, I am going to provide a question that I think was left over from yesterday, and this follows some of the discussion of the Android platform open development. When we are looking at trends or new behaviors that might have implications for the security environment, does open platform development pose any abnormal level of risk to users or to the integrity of the phones themselves?

I will start with you, Larry, and then we will give everyone a crack at this one. I think it is an important

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

question.

MR. RUDOLPH: I have mixed feelings about this.

I think one of my complaints is it is very -- and I will summarize, it is very hard to program your phone. In fact, programming a phone, even though it does look like a 10-year-old PC, is in the realm of the large companies. You have to pay a large amount of money to be able to program lots of phones. The Android is sort of a game-changing technology opening up cell phone programming to the masses.

Just the same way you would use Java and Eclipse on a PC environment, you can start using it to sort of program phones under Android, which means that kids in the garage can start doing interesting applications, which is absolutely great.

My MIT students can do absolutely phenomenal applications on that.

However, it also means that hackers can get on and do very interesting applications in their realm of what that is. It is Linux and it does have -- Google's android phone is Linux and they do have a lot of security sort of built in, but that is security for the traditional type. I mean, I cannot get into the OS to put some root kit or some traditional virus. However, you do have the access, and it is not clear if this is a security violation.

Under Android, you can locate any application, you

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

can get location information maybe for a distributed version of Pacman or something like that. It also could always go to a third party through internet access very easily and also you can use the microphone or speaker, which means that you can have a game which takes location information and voice information and sends it to a third party website somewhere to record where you are going, what conversation is going on. So, they have a built-in bug that anyone can sort of get at any place.

So, it opens up the world, but it also provides lots of challenges that traditional security will not protect against.

MR. TUMMINIO: Mark, any additional thoughts?

MR. HENDERSON: I had a Linux-embedded device like a smartphone and one of the things you can do is you can go to the OP platform, which is an open source OS for Palms and other handheld devices. One of the things they said was, when you do this, you could potentially brick your phone or your little PDA. By brick, meaning it is no longer usable.

So, if you go to an open source solution and it is not vetted and is not -- not that Google is not vetted, but Google certainly has gone through all the rigor of testing it. But if you decide to go to someone other than Google that is not tested and you brick your phone, it is no longer useful.

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

If you take it back to the vendor, they are going to say, did you load any third party applications or any other -- what did you do? And you are like, well, I went to this other site, downloaded the particular ISO and loaded it and it bricked my phone. They are going to say you violated the warranty. So, guess what, you can buy a new phone.

So, for me, I would say if you are going to go ahead and do something like an open source platform, just make sure they follow all the normal testing and security controls that you would for a major vendor. If not, try to go with a major vendor, if not, if you do not want to go with open source because they certainly have plenty of solutions that more than one person has developed security solutions for. When you have open source solutions, you sometimes have to rely on open source security solutions and those are not as trusted.

MR. COLE: Just a few thoughts from a little different perspective. First off, from a consumer perspective, I find it pretty exciting. I find Android pretty exciting. It holds the hope that Gmail will finally work on my Nokia phone.

**(Laughter.)**

MR. COLE: Which I have had non-stop trouble with. But, no, in general, I think it stands to make that market

more competitive, to provide more options to consumers. I think it is a positive thing. But from a security vendor perspective, we look at this and we do not see that the mobile security market is going to evolve in the same way that the PC security market did. It is just not. But if you look at where consumers are today with PC security, I will go back to my previous example, the storm trojan. A lot of our job now is helping people make good decisions on their PC, and a lot of it is about protecting the web space.

If you look how the mobile security market evolves and what our opportunities look like at Symantec, I think it is probably going to be a lot of the same thing. How do we help people make good decisions about the applications and the screen savers and ringtones and wallpapers and stuff that they install on their device from a safety, from a security, from a performance perspective perhaps and help them maintain a healthy device, among other things. But I think that -- it sort of evolves in sort of the same fashion.

MR. TUMMINIO: A question that has come up from a couple members of audience in writing is this: Is there a secure way to dispose of your cell phone or perhaps the example of recycling? I mean, is recycling your phone a secure way to dispose of your cell phone? I will offer this

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

to the panel at large.

MR. HENDERSON: I had this question about two years ago at a separate panel and it was quoted somewhere, at Tech Re Public (phonetic) I think. So, I have to be careful when I say my response. Within government space, because we typically do not deal with consumers asking us for particular protection for their phones, but we do give guidance. In some cases, when you buy large quantities of phones, handholds, you can get a discount if you return the phone back to the provider. If you buy a \$500 handset, you can get \$50 back if you return the handset to them. But if they are not sure that the actual data has been wiped, someone can potentially recover that information.

So, we had recommended, in some cases, actual physical destruction of the phone. We had sent that out. USCERT maintains the G-First Portal, which is a forum for government incident responders. And one of the individuals actually responded and said that is what their agency does.

They destroy handheld devices at the end of their tenure.

If you are not going to destroy the handheld device, just get it back.

I used to work for a carrier class like Tier 1 ISP and we used to give interns PDAs, and the interns would leave and take their PDA with all the company data on it. So, just

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

have an asset inventory and keep the actual handheld close to you. That is all I really got on that.

MR. RUDOLPH: Flush it down the toilet. Water does really destroy it.

Part of the problem is that certainly the failure mode of phones is that the input does not work, either the screen is broken or the keyboard is broken. So, anything that you can -- you know, you sort of cannot wipe the data off and the data is sort of sitting there.

Clearly, if you have an external SD card, you take that out. But lots of them are built-in and there is not a whole lot that you can do once the phone stops working. So, physical destruction might be the only solution.

MR. TUMMINIO: I will note that if you choose recycling, we do have an FTC pamphlet on safe recycling outside. Is that a question from the audience? Please, and if you could identify yourself before asking.

**(Individual off microphone.)**

UNIDENTIFIED FEMALE: Sally Mund (phonetic) from the Council of Better Business Bureaus. Thank you for teeing up my question (inaudible). It is really interesting to me to hear our statistics coming out where the individual end user is really the one who is responsible for protecting themselves.

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

MR. TUMMINIO: Ma'am, if I could ask you to speak a bit louder, it does not seem like the microphone is picking up.

UNIDENTIFIED FEMALE: Okay. The end user is key. This has been talked about in ID theft and fraud prevention for a long time, usually it relates to paper because people lose paper documents and the IDs are stolen that way.

What I find really interesting, I would love your perspective on, with the rise of environmentalism I think there is a strong awareness or a strong awareness from consumers that these PDAs are environmental hazards. So, people are less likely to throw them away. But they are not up to speed with understanding all this personal data that they are carrying on this device.

So, I am curious what the industry has in mind or what their thoughts are, how to close that gap, that the environmentalists have done a great job at making people sensitive to the environmental hazards and not just throwing them in the garbage. What is the mobile industry doing and plan to do to help raise awareness of the private information on the devices as well? So, you can kill two birds with one stone.

MR. TUMMINIO: Dave, perhaps you could take a crack at that first?

MR. COLE: I think I am sort of the wrong guy to answer this one and maybe all of us are. But, in general, I think -- yeah, there we are. Stand up and be counted.

MR. DIGGS: My name is David Diggs with the Wireless Foundation. In 1999, we began the first consumer takeback program that was nationwide in scope. So, two comments, one to the environmental one and the other to the security issue. What we recommend that donors do is exactly what you suggest. Please wipe out the memory in your phone.

I am not going to stop and we do not presume to try and stop the NSA from cracking what is on there. You are right. The directory is deleted, but the data are still there. But for most purposes and for what most of us keep on a simple phone, that is pretty benign data.

In the four million phones that we have collected, I can count on one hand the number of times where we have had an issue where data that was stored on the phone came back in some form. These were all benign. These are the number of calls I have gotten.

As to the environmental piece, what has happened is there has been an awful lot of work on making the phones -- notably driven in Europe, and I am a little rusty on this. But the phones themselves, the kinds of things that were

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

considered problematic from an environmental standpoint are gone from phones that are manufactured now. These are chemicals, I cannot really name. Chlorinated -- I do not know what they all are, but they were in there as well as the battery technology, which has gotten a lot more benign from the days of the NiCads.

So, we would recommend -- and I do not want to take off the table the option of recycling your phone. Not only is that an environmentally sound thing, all the responsible recyclers, and that that includes everything that the wireless industry is currently doing are -- again, yeah, right. So, there is an economic incentive for consumers to give this back, it helps out on charitable organizations, what have you. So, I would just add that comment.

MR. TUMMINIO: Dave, I have another question from the audience that you may be the right guy to answer. The question is this: How easy is it to install mobile security software, and then once it is installed, how is the software properly updated?

MR. COLE: I will own up to the fact that it is not as easy as it should be. There are things we have done, for example, we have had mobile security solutions, I believe, for about six, seven years now. They are in their fifth generation. But largely for the enterprise. That is where

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

the demand has been is in the enterprise, for folks like Mark and so on, protecting enterprise PDAs and keeping that data secure.

Having said that, we introduced the first Norton smartphone security this year aimed at a high-end consumer who also has valuable data they want to protect. It did not change dramatically from the enterprise version. But what did change is it auto detects your operating system whether it is Symbian or Windows Mobile and loads the right version.

Having said that, I would argue that -- and what we have seen from research is that people want the security software to come pre-loaded on the phone and already be there and be part of a stock offering for a phone. So, ultimately, I think as this market emerges, as I said, it is going to be a little different than the traditional PC security market.

In most cases, hopefully, the user will not have to install a security software. It will already be on -- the device will come with the security software needs already loaded.

MR. TUMMINIO: Larry, you had some thoughts?

MR. RUDOLPH: Yeah, I completely agree with that.

The only thing I want to add to it, though, is that while this might be a ten-year-old PC, the security threats are broader and the traditional way of saying, well, I am going

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

to put in virus protection software so I do not get a virus, protects you from viruses, but it does not protect you from all these other threats.

So, what I advocate is the opening up of the phone to allow, just like the Google phone will allow, third party high school kids or whatever, someone in their garage figuring out new security models or virus protection or security protection models to allow them to sort of play with them.

Then maybe they get taken over by a company like Symantec.

But, today, all the development is sort of left in the hands of the big guys and I think that is a problem ultimately for security for consumers that we are protecting against this threat, but the threats may be coming from someplace else.

MR. TUMMINIO: While we are discussing viruses and PCs and comparisons between phones and PCs, I wanted to bounce a statistic off of you that was in the presentation yesterday from M:Metrics. That is that 77 percent of music on mobile phones is actually transferred there from consumer's PCs.

Mark, does this kind of side loading -- is this going to be the greatest vector for an infection of a smartphone increasingly connected to the internet?

MR. HENDERSON: Well, I think that is one of the things that we caution consumers about and certainly federal

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

agencies. When they have a device like a laptop or a smartphone, they tend to plug it into their home network if they want to put on specific MP3s, they want to load particularly a USB thumb drive, they just got out of a conference with a guy's new business card and they jam that into their smartphone. After a while you begin to deal with cross contamination. Somewhere, somehow, you are going to get something malicious potentially on your phone, so you want to limit that capability.

And I think from where we are talking, from USCERT's perspective, we are always concerned about what exactly users are doing with their phones making sure they are operating, so there is limited risk. One of the ways they can do it is there are guidelines out there that can actually tell them, these are ways that you can protect your phone and some of the best practices as far as what they can limit adding to their phone and some of the secure applications that are available to them.

MR. TUMMINIO: We are running out of time, but I see we have one more question from the audience. We will take this question and then offer each of the panelists an opportunity to provide some closing thoughts. Yes, ma'am?

MS. GRANT: Thank you. Susan Grant, Consumer

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

Federation of America. I wanted to ask about phones that are equipped as contactless payment devices. I guess there are a couple of different technologies, at least, that enable that. But can you talk about that in terms of security? Can that information be intercepted in transmission? Can it be gotten just carrying your phone around if you have the right technology?

MR. RUDOLPH: There is something called near field communication, which is we are talking about centimeters of distance. They come in the back of phones and they are beginning to appear in lots of phones. People love them.

Absolutely love them. Because you just -- that is your credit card. And credit cards have -- your cards have RFID cards inside of them, but they are not active, they are passive. So, the ID you have in your RFID card is fixed and it is the same ID when you put it up to any reader anywhere.

The ones that come on the back of phones are active, meaning that they are actually getting power from the battery, so they actually have the capability of doing computation and giving a new number each time and doing challenge and responses.

So, that is the good news. The bad news is that this stuff can be read since it is active and it is broadcasting, it can actually be read from a mile away with

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

a tube-like gun that can read this information. So, the man-in-the-middle attack, there really can be someone standing right next to you as you hold up your phone to do it and, bam, you get hit. We have seen RFID attacks numerous places, lots of -- in Amsterdam, the whole transportation system was built on RFID cards, and within a half a day of them coming out with the cards, that system was cracked. So, it is both good and bad.

MR. TUMMINIO: Comforting. And on that, parting thoughts, Dave, please start.

MR. COLE: So, I think it is very easy to overhype the digital threats facing mobile phones today. And in doing so, I think you kind of cloud out the bigger issues today, which is largely fraudulent payments and loss of the phone itself and all the valuable data we are putting there. So, the threats today really, there are software remedies out there like we offer for providing easy encryption and so on and so forth. Again, I think consumer interest is relative to the amount of valuable information you are putting on that and that should be the consideration point.

But longer term, as we look at things like fixed IP addresses potentially for phones with IPv6 and so on, as we look to phones being one of the main, if not the main, platform for accessing the web, things get a lot more

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

interesting. So, do we expect it to follow the same PC model with self-propagating threats barraging people's phones? No, not really. We expect it to look a lot more like the threats base looks today, which is focused on deception and tricking people and fraud and so forth. So, we do see it taking a little different model today.

Really, again, the remedies, I think, are a lot more along the lines of protecting yourself from the dreaded taxi attack. But having said that, in the future, I think things are going to get a lot more interesting.

MR. TUMMINIO: Mark, parting thoughts and advice where to find USCERT's mobile security tips.

MR. HENDERSON: Sure. I will start there. So, we partner with the Computer Security Research Center with NIST, and NIST has two documents that you might be interested in. One is 800-97, which is on wireless guidance, and the other one is 800-101, which is on cell phone forensics. Both of those documents are going to have, at the end of them, recommended other resources that will be very valuable to you.

As far as some of the trends, we publish a general trends that goes out to consumers and any individual in the public sector. That is quarterly. I think that is actually every three months. We also maintain current activity, any

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

new threats that potentially would be targeting mobile consumers. I am going to take away from this, maybe it is time for us to update some of our material that we have had that might be stale on our website, which is certainly available. We do have documents and publications that cover security.

I would say, in parting, user behavior is certainly something we need to focus on and users need to be aware of some of the things that they need to do to protect their phone for information that is processed or transmitted on it. But we really need to partner, both the public and the private sector, to come up with secure protocols, do some analysis on some of the threats and go against the bad guys or the criminal-to-criminal gangs per se. There is lots of material out there and we are just trying to help individuals get access to it and coordinate with the right authorities.

MR. TUMMINIO: Larry, we have maybe a minute and a half, two minutes left.

MR. RUDOLPH: Okay, due to the fact that I am a New Yorker, I am going to talk fast. The first point, I think the biggest threat that is going to be in the future is this over-the-air update. And, right now, we are sort of trusting the carriers and the handset manufacturers and the like to be able to sort of regulate that. The day that someone breaks

*For The Record, Inc.*

*(301) 870-8025 - www.ftrinc.net - (800) 921-5555*

that code and they can do over-the-air upgrades to people's phones without the manufacturer's knowing about that, we are going to have massive kinds of viruses that we never have seen before. It can happen like that. It is not there yet, but someone just has to crack it.

The second thing is that this may be different, but it is lots of people who do -- PC penetration in the U.S. has not increased in the households very much. People are bypassing PCs and using the phone instead of PC. When you take your phone home, it has WiFi capabilities and it is just a PC. Put a big screen next to it and a keyboard and this becomes the brains of the PC with WiFi, so it goes over the WiFi networks and not just allowing the carriers to do all the protections.

So, every threat that we had from the PC world, we are going to see that again when this thing really starts acting as a PC.

The thing that I really -- transparency I think is the key. We heard the previous sessions today that, do not worry, the network is going to protect you. And we are going to check things for you. No, I am sorry. I want to see all this stuff. I want to see what my kids see on their phones. I do not completely trust the network to sort of make sure that my kids are not buying stuff. But whenever

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

they buy stuff, I do not want to just see a number of how much it was. I want to see what was displayed on their screen.

Somehow I want that ability. I bought the phone. I want that ability to be able to see that as a parent.

In terms of really I want to be able to do third party applications. I said I am a stakeholder in this phone, I cannot put a device driver in here. I cannot snoop on which internet sites my phone goes to via third party application.

I do not have that ability. Even though I bought the phone, I do not have the rights to put a device driver on here to stoop network or SMS traffic. I think that is an absolute mandatory thing. Since I bought this machine, I should be able to have root password on it. So transparency, device drivers.

The last thing I want to talk about is privacy, which is my own sort of thing. And even though my mother, bless her soul, probably would hate seeing this, I believe privacy is the right to lie. Everything is -- wherever I go in the light, the phone company knows where I go. If you go to my website, though, however, the last three days I publish where I have been outside. You will find out that I took the train from New York by going to my website at MIT, because I believe that if I publish where I have been, I have the right to lie. And I can sort of have plausible

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

deniability. So, I want to be able to put information out there that competes with other information, so that people cannot really tell what is true and what is not true. Because there is privacy, people know information about you, I want to know the equivalent information and present it out there.

MR. TUMMINIO: Unfortunately, that is all the time we have. We have covered a lot of ground. I think it is good to learn that the threat has not been tremendous in terms of number of attacks so far, but it sounds like there are a lot of places that we can get into trouble if we are not careful.

I would like to thank our panelists, remind the audience and everybody watching over the web that the deadline for comments and research or anything you would like to submit has been extended to June 6.

If I could kindly ask everyone in attendance here to stay in place because closing remarks will follow immediately. Thank you, and a nice round of applause for our panel.

**(Applause.)**

**CLOSING REMARKS**

MS. RICHARDS: I will be very brief because I know I am the only thing between you and going home.

So, Phil stole one of my two announcements, which was that the comment cycle will remain open until June 6,

*For The Record, Inc.*  
*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

and we encourage you to file comments based on what you have heard over the last two days.

For those who would like to learn more about contactless payments and RFID, I wanted to announce that the next in our series of town halls, following from the tech aid hearing, will be a town hall on contactless payment systems and RFID. That will be held July 24th in Seattle, Washington. We will be co-hosting with the University of Washington Law School. There we will explore contactless technologies and how and to what extent the technologies are being deployed in the U.S. and around the world, and also the potential benefits and threats, some of which you heard within the last couple of moments.

The last thing I wanted to do, this is my Grammy moment when I get to thank the people who made the event today and yesterday possible. And a lot of work goes into putting on these town halls. First of all, I would like to thank all of the panelists and everyone who gave so generously of their time to come and be part of this.

I would also like to thank the staff that worked very hard to put it together, and if you would indulge me, I will go through a list of some of the people, starting with Ruth Yodaiken, who spent an awful lot of time and is kind of the ringmaster of this. I wanted to point her out. Phil

*For The Record, Inc.*

*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

Tumminio, who was just up here and manager Lisa Hone and Lois Greisman from our Division of Marketing Practices. From Advertising Practices, Mary Engle who heads that Division and manager Rick Quaresima and staff attorneys Jim Trilling and Stacey Ferguson, who have been your hosts at some of the panels throughout the day.

Special thanks to our FTC Honors paralegal Julia Flanouski (phonetic) and the law clerk Alissa Zigler, paralegals Conner Macavoy (phonetic) and Haley Zernich. I am getting close to the end. And also to the other staff, Peder Magee, Robert Schoshinski and Phyllis Marcus and to our media team, to DCBE, Cali Ward and Ashley Vo, who did all the logos and websites and print material that is outside.

The security team, all the attorneys and the different divisions who worked on this, the honor paralegals who have been in the back and out front.

And last, but not least, Commissioner Leibowitz who started us off by referencing Maxwell Smart and Get Smart and I think that has been successful. I think all of us are a little smarter having sat through two days of panels and hearings, and I thank you all for coming.

**(Applause.)**

**(Whereupon, at 4:08 p.m., the workshop was adjourned.)**

*For The Record, Inc.*  
**(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555**

C E R T I F I C A T I O N O F R E P O R T E R

MATTER NUMBER: P074403

CASE TITLE: MOBILE GROUP

DATE: MAY 7, 2008

*For The Record, Inc.*  
*(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555*

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MAY 21, 2008

---

ROBIN BOGGESS

**C E R T I F I C A T I O N O F P R O O F R E A D E R**

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

---

ELIZABETH M. FARRELL