FEDERAL TRADE COMMISSION

MOBILE SECURITY FORUM

POTENTIAL THREATS AND SOLUTIONS

JUNE 4, 2013

Federal Trade Commission

601 New Jersey Avenue, N.W., Conference Center

Washington, DC

FEDERAL TRADE COMMISSION

I N D E X

Session	Page
Welcome, Emily Cope Burton	3
Opening Remarks, Chairwoman Edith Ramirez	6
Overview, Steven M. Bellovin	12
Panel 1: Understanding Mobile Malware	20
Panel 2: Building Security into Modern Mobile Platforms	78
Speaker, Markus Jakobsson	145
Panel 3: Extending Security Throughout the Mobile Ecosystem	160
Panel 4: Solutions for Consumers to Protect Themselves from Mobile Threats	225
Closing Remarks, Charles A. Harwood	290

WELCOME

MS. BURTON: Good morning, everyone. I'm Emily Cope Burton from the Division of Marketing Practices of the Federal Trade Commission, and it is my pleasure to welcome you to our Mobile Security Forum. I'm delighted that you're all here to learn with us and teach us as well. Since this is a post-sequester-era government event, there is no coffee or water. I just want to warn you in advance. You will have full access to the bathrooms, which are across the lobby to the left of the security desk. There is also a water fountain there if you brought your own container. We have a 20-minute break after the first panel, though, so those of who you did not come prepared will have time to get some provisions.

A few notes about the Q&A. We will not have specific Q&A sessions or Q&A portions of panels, so if you have a question, you can write it down on a Q&A card. There are a couple in each of the folders, and there are also some out on the table with the materials. Hold it up in the air, someone will come and get it and deliver it to the moderator, and we'll try to ask -- get through as many of those questions as we can. But we will be taking only written questions.

We will also, because we are very high-tech

here at the FTC, be taking questions over our Facebook page, in the Workshop Status thread, and via email to OPA, for Office of Public Affairs, @ftc.gov. And then also the FTC staff will be live-tweeting this event from the FTC Twitter account and using #ftcmobile. So, speaking of mobile, please take this opportunity to turn off your mobile devices.

And then let me just quickly run through our security procedures. Anyone who leaves the building without an FTC badge will require -- be required to go back through security, including the metal detectors, prior to reentry. So, if you're leaving for a break or lunch, please time your return accordingly.

In the event of a fire or evacuation of the building, please leave the building in an orderly fashion. Once aside, look directly across New Jersey Avenue to the Georgetown Law Center, which is our rallying point. On the front sidewalk to the right side of the building is where you'll meet, and there will be a person accounting for all of the conference center attendees.

In the event that it's safer to remain inside the building, you'll be told where to go inside the building. If you spot suspicious activity, please report it to security. And this event may be photographed,

videotaped, webcast or otherwise recorded. By participating in this event you are agreeing that your image and anything you say or submit may be posted indefinitely at ftc.gov or one of the Commission's publicly available social media sites.

With that, I'd like to introduce the Chairwoman of the Federal Trade Commission, Edith Ramirez, who will be giving us opening remarks to set the stage for the rest of the day. Thank you to the Chairwoman and thank you to all of you for participating.

(Applause.)

OPENING REMARKS

CHAIRWOMAN RAMIREZ: Thank you, Emily, and thanks to all of you for being here today. And welcome to the FTC's Mobile Security Forum. It's no exaggeration to say that we're in the midst of a mobile revolution. Today, consumers buy twice as many mobile devices as they do PCs. Nearly a third of the consumers who use their phones to get to the Internet say it's their primary way of reaching the web. And we're starting to see the rise of the mobile-only Internet user.

In the first quarter of this year, tablets and smartphones accounted for over a fifth of all e-commerce traffic in the U.S., compared to -- get this -- just 2 percent only two years ago. Smartphone users reach for their phones an astonishing 150 times a day on average, to send a text, check for email, occasionally make a phone call, surf the web, or use an app.

Today, though, we'll be turning away from our addictive smartphones and tablets, or so I hope, to consider the current state of mobile security, emerging threats, and the measures industry, government, and consumers can take to protect against security risks. Our interest in mobile security is an outgrowth of the FTC's broad mandate to protect consumers, which includes protecting them from threats to the use and enjoyment of

new technologies.

In the last decade, the FTC has been at the forefront, along with our partners at the Justice Department and in the states, of the fight against spyware on the desktop computer. We've brought a dozen enforcement actions against purveyors of spyware, from rogue ISPs that distribute malware, to computers that installed keystroke loggers that captured sensitive information, to businesses that transmitted nuisance adware that delivered popup ads.

Most recently, we brought a number of cases, including an enforcement sweep initiated last fall against marketers of PC scareware scams that operated in the U.S. and across the globe. As consumers migrate to smartphones and tablets in record numbers, we're now also turning our attention to the security of the mobile environment.

We have three main tools at our disposal: law enforcement, consumer and business education, and policy, which includes promoting industry dialogue and advocating best practices. On the enforcement front, we've already begun to address mobile security with our first case in this arena. In February, the Commission alleged that HTC America, the mobile device maker, introduced an array of security vulnerabilities in the course of customizing its

mobile devices, thereby putting at risk the sensitive information of millions of consumers.

We charged HTC with violating the FTC Act's, prohibitions on both deceptive and unfair practices. To resolve the FTC's charges, HTC agreed to establish a comprehensive security program and undergo independent security audits every other year for 20 years. Our settlement also includes a provision that is the first of its kind in an FTC order, and as far as I'm aware, the first of its kind in any other U.S. or foreign agency order: a requirement that HTC develop and release software patches to fix the vulnerabilities on millions of its devices.

But cases like HTC demand sophisticated technological expertise and tools. And to make these cases possible, we've created a forensic mobile lab to allow FTC staff to conduct research and investigations. We've brought in distinguished technologists, like Steve Bellovin of Columbia University, and his predecessor, Ed Felton of Princeton. And we've created a mobile unit to ensure that we are alert to mobile issues in all of our consumer protection work.

As to the FTC's second tool, consumer and business education, the good news is that some of you who are with us today already offer an array of innovative

technologies, some of which are free, to help users secure their mobile devices. But more work needs to be done. For our part, earlier this year, the FTC released an online business guide that encourages app developers to think about security from the outset and offers practical tips and guidance on how to do that.

For consumers, we offer extensive materials to help them stay safe and secure, whether on their home computer or on a mobile device. Onguardonline.gov, which the FTC manages, is packed with consumer tips on topics such as mobile malware, mobile security patches, and updates for mobile operating systems.

And with today's forum, the FTC is continuing its policy work in the mobile sphere. In the past year, we've hosted roundtables exploring mobile cramming, mobile payments, and mobile privacy and advertising disclosures. This series of policy dialogues reflects the high priority we place on ensuring that the FTC itself, industry, consumer groups, and other stakeholders are all fully attuned to the consumer protection issues presented by the explosive growth of mobile technology.

As part of today's program, we have with us some of the leading voices from industry, academia, and consumer organizations to engage in what I am confident will be a rich and robust discussion.

Mobile devices depend on many different players, among them device manufacturers, chipset makers, app stores, app developers, and each serves a unique but critical function in the user experience. So, I'm especially pleased to have such excellent representation from businesses across the complex -- the mobile ecosystem. I appreciate your willingness to share your expertise on this important topic, and I welcome your thoughts on how we can collaborate to ensure that mobile technology is safe.

Given the exponential growth of mobile in our daily lives, there's no room for complacency from any of us about the need to keep the mobile environment safe and secure. My hope is that our dialogue today will inspire action, encourage innovation, and engage each of us in that common cause.

We're going to begin the conversation today with an overview of the mobile ecosystem provided by Steve Bellovin, the FTC's chief technologist. Steve is a renowned expert on network security, and we're very fortunate to have him with us this year and also with us this morning, to lay the groundwork for today's program.

But before I hand the program over to Steve, I wanted to take the opportunity to thank you all again for being here with us this morning. And I also want to take

this opportunity to thank the FTC team who put this event together, including Emily Burton, Colleen Robbins, Dan Salsburg, Nithan Sannappa, and Paul Ohm. So, thank you very much.

And, now, please join me in welcoming Steve Bellovin.

(Applause.)

OVERVIEW

MR. BELLOVIN: Thank you, Chairwoman Ramirez.

So, I apologize for having slides. My years at Bell Labs and AT&T Labs have rendered me incapable of speaking without a slide that reminds me what I'm going to say.

So, again, I'll be talking about the mobile space and just what are all of the different pieces. It's not just one problem. There's a saying that the attacker can attack anywhere, the defender has to defend everywhere, which means you have to know where everywhere is. And it's not just one layer. You know, there's the old story, apocryphal story, about this 19th Century physicist presented a theory of how the universe came to be, and a woman said, well, you've forgotten my favorite and correct theory that the earth is a giant plate riding on the back of a giant turtle. Well, that's very interesting, ma'am, but what does this turtle ride on? Well, it rides on top of a larger turtle. And that turtle? Don't be silly with me, young man. You know as well as I do it's turtles all the way down.

Mobile devices can have security flaws at any layer. And it can have security features at any layer, from the chips through the applications. The layers themselves are composed of many pieces which come from

many different places. We, as the defenders, need to protect them all.

We can start with the chips. The basic chip that's in most phones these days, certainly all the GSM and LTE phones, the SIM chip, the subscriber identity module, this is intended to be a secure chip that says who you are, your phone number and so on. If someone can read this out, they can impersonate you perhaps. It's got a cryptographic secret in it.

Some of the newer phones have the NFC, near field communication, chips, which are being used to implement digital wallets. It's a lovely thought, but this means that your phone can pay for something. And if this chip is not properly designed, properly secured, somebody can basically read out your bank account number. Or it might happen by accident. You put your wallet down on the counter next to you while you take out a credit card to pay, and the merchant's NFC reader is reading your phone perhaps instead of your credit card that you intended to pay with. You pay with cash and you pay with your NFC chip simultaneously. Isn't that a great stunt?

There are many other -- there are many wireless interfaces by which attacks can enter the phone. Blue tooth for the ubiquitous earpieces where people we see talking to themselves on the streets are not necessarily

strange people these days. They're just having a real phone call. The WiFi chips for all the mobile hotspots, I see what looks like a WiFi hotspot right over there. GPS, there are security mechanisms that depend on your location. If somebody can spoof that location, bad things can happen.

And of course the over-the-air wireless interface for the long haul phone networks, whether it's GSM or CDMA or LTE or whatever other variety of alphabet soup we see in three years, these are all vehicles by which bad things can happen if they're not adequately protected.

The operating system, though, is what we mostly see, and there are, what, half a dozen different important ones today or coming in the near future. IOS from Apple on its iPhones and tablets and so on; the ubiquitous Android phones from many different manufacturers; Windows Phone, especially Windows Phone 8, a fairly new entrant; newly revised Blackberry OS; forthcoming phones with Firefox OS or Ubuntu OS from Mozilla and Canonical; probably more coming. Unclear how many the market will support, but we have learned in the PC world that it doesn't take that many instances of device to support a very viable ecosystem for malware and viruses and worms. They can spread through remarkably

low densities of phones.

We've got different hardware platforms. Of course we've got iPhones and Blackberries, which belong to one manufacturer, but, in fact, these things are manufactured very often, especially for the iPhone, by contract manufacturers. There have been security problems in the past coming from the factory. I've seen news reports of digital picture frames coming with viruses on them. When you plug them into your computer, it spreads the virus to the computer. Accidental, no doubt, but it's a concern.

Many other manufacturers of hardware, especially for Android phones, with many different companies manufacturing different varieties of Android phones and Windows 8 phones still very new, it's hard to say how it's going to develop, but, again, there are different manufacturers.

The user interface. A remarkable number of security problems start because the user is confused. Often by an inadequate design, they don't understand what they're clicking on, tapping on, agreeing to, what have you. We have many different operating system interfaces. We start with the ones that come from the OS vendor, whether it's Apple or Google or Microsoft or whomever. But different manufacturers, especially in the Android

world, add their own changes, enhancements, what have you to them. This is their product differentiation. This is what -- yeah, the problems allegedly caused by HTC came about from HTC's changes and, they thought, improvements to the Android phone to add new features.

Carriers have their new features. That's part of their differentiation. And then there are a variety of call it skins, to still change it. The Amazon Kindle, the Barnes & Noble Nook are Android devices underneath. We have a new Facebook home skin on Android. All of these change the user interface in a way that may or may not be confusing. It may be better, but it's different.

Apps. There are so many, you know, what, millions, tens of millions of apps? It seems to be about that many different vendors, too. Some are very small; some are very large. The large ones, if they get it wrong, there's a good opportunity for the malware writers; the small ones may not have the sophistication to do it right.

Apps are often built using third-party libraries, and some of these are not updated well. These will have well-known security holes. Many of the jailbreaks to IOS have happened because of third-party libraries that Apple incorporated. These apps are often interacting with remote servers, if these connections are

not adequately secured, and a lot of them have not been, researchers have shown. You can have bad things happening that way, and, again, coming from many different places: the app stores run by Apple and Amazon and Microsoft and Google, and a lot of small app stores, especially in the Android world.

And then there are all the content servers. There have been vulnerabilities in the PC world where just viewing a picture was sufficient to penetrate the machine. Think about what happens with malicious content here. A lot of information at risk: who you are; what are you doing; I won't say your keystrokes, your key taps, as you log in to something; where you are, location tracking by people who want to stalk you; what else you have done, a history that's kept by a lot of these apps; your contact list, who you talk to; your calendar; where you are; and so much more. All of this is at risk to a malicious app, penetrated operating system, what have you, especially if there aren't sufficient protections in there at every layer.

In the PC world, the laptop world, we've gotten used to patches. We have an operating system; the operating system vendor supplies patches. We have an application; the application vendor supplies patches. It's a much more complicated picture in the mobile device

world. We've got many different vendors, but they don't control the patches for the most part. Or they don't control it by themselves because they sell the phones via the carriers. Well, Apple can ship its own patches itself directly, but if a random -- if a flaw is found, say in an Android, Google will fix it, but then it's got to go to the manufacturer of that phone because it may interact with their customizations. Then it's got to go to the carrier, and it's the carrier who's ultimately going to ship the patch to the user.

The applications are distributed through app stores, it's got to go through the app store approval process for IOS to get out there, and they are built on third-party libraries and they're not always tracking the changes, updates, and fixes to the third-party libraries. So, it's a very complex and large mix of players who all have to cooperate.

Add to that the comparatively short life span of phones in the hands of a typical consumer. I've seen 18 months mentioned as the average time that someone owns a phone. And what we see is that manufacturers sometimes don't want to repair the patch because they know there's a new release coming out soon that you're probably going to buy, except if you're one of the people who hold onto the phone for two and a half years instead of one and a

half, you may have a very long period where the phone is not patched and the apps are not patched.

So, it's a very complex process, and the patch mechanism that has been working decently in the laptop and PC and Mac world doesn't work as well in the mobile device world. And given the business relationships, this is a technical problem. It's very hard to ship one patch from, say, Google out directly to the user without testing by the manufacturer, by the carrier, and by the app vendor. It is not an easy problem.

So, it is turtles all the way down. We, as the defenders, have to fix every layer, despite the complexity of the business relationships, the whole ecosystem. Thank you.

(Applause.)

PANEL 1: UNDERSTANDING MOBILE MALWARE

MS. BURTON: Okay, can we get the panelists for Panel One?

So, good morning and welcome to our first panel, which is on understanding mobile malware. I am Emily Cope Burton once again. This is the last you'll hear from me, I promise. Let me start by briefly introducing our panelists. To my left is Omar Khan, who is the Co-CEO of NQ Mobile, which is a global security company that provides mobile apps to protect mobile devices from malware, spyware, theft, and loss.

Then to Omar's left is Gareth Maclachlan, who is the COO and cofounder of AdaptiveMobile, which is another security company that provides mobile network protection to mobile and fixed network operators and their subscribers.

To Gareth's left is Dan Guido, who is from Trail of Bits, which is an information security company that focuses on enabling companies to make better strategic defense decisions.

And, finally, to Dan's left is Patrick Traynor from Georgia Tech. Dan's research focuses on the security of mobile systems and including the risks of mobile malware.

So, a printed bio sheet is available in your

folder, so please refer to that for all of the details about these panelists and all the others.

So, to kick off the panel, Omar is going to give a presentation summarizing some of the research that NQ Mobile has done on the rise of mobile malware. So, we'll turn it over to you.

MR. KHAN: Great, thanks.

Great, thanks for having me. I think Steven did a great job of setting the landscape for what's happening in the mobile industry today. I've spent probably the last 13-plus years between the manufacturing side as well as the OEM carrier application side of the mobile industry. I think it's -- you know, it's safe to say that what we're all most excited about in terms of the innovation within mobile devices, applications, within the ecosystem from an operating system perspective, is also what creates some of these vulnerabilities.

You know, we approach it at NQ Mobile from the perspective of really driving trust and enabling consumers to be empowered or enterprises to be empowered to protect themselves on these devices so that they can trust the types of things that they want to do using these devices. I mean, I think, as we head forward, it's really not fear that we want consumers to be left with.

It's really empowerment both of their data, of their devices, of what those devices are capable of.

I think as we head forward and fast-forward to the next three to five to 10 years of what these devices are capable of, they have some of the most powerful applications, processors, as Steven noted; they have very capable displays and ecosystems on the devices. As those devices become conduits for other devices, whether they're personal health care devices, whether they're mobile payment ecosystems, they themselves will be conduits for personal information, and the context that makes those devices as, you know, rich in terms of the information that they have and can provide.

You know, there's a YouTube video somewhere that somebody told me about that talked about mobile payments, and I think it was at an In-N-Out in California, that said, you know, it really compared being able to pay with your phone to being able to pay with your credit card. The credit card, I think most would agree, is a pretty killer app. I mean, the ability for you to pull out something from your wallet, swipe it in less than 10 seconds, and put it back in your wallet is fairly -- you know, it's fairly quick.

So, mobile devices, just from the perspective of it replacing a credit card is not really what's going

to drive adoption of mobile payments; it's the fact that it has context and it's contextually aware, and it provides information to payment vendors, to merchants, that makes the transaction much more rich for a consumer. And that's really, I think, what's going to drive that adoption. But it's also those environments that create, you know, create environments for hackers and malicious actors in the system to exploit consumers.

So, I'm just going to very quickly, you know, I don't need to necessarily go through each slide, but we are a mobile security company focused on endpoint. We provide solutions for consumers, for enterprises, for carriers, mostly from the antivirus, anti-malware, privacy, consumer encryption perspective. We provide solutions today that help consumers protect their devices from phishing attacks, from malware, from losing their data, as well as we provide consumer encryption solutions, so when you download third-party applications, being able to personally encrypt your own data from a context, from a communications perspective, is something we provide.

And then finally we provide a set of solutions for parents to help protect their kids on their smartphones in terms of not just parental controls and location, but also the ability to manage their

applications and their personal content and help teach responsible behavior to kids about how to use their mobile devices. And we can talk a little bit more about that on the panel.

You know, I don't think there's any argument here that from the perspective of hackers malware is very much on the rise. We've seen a huge increase just over the last three years alone in terms of the number of unique pieces of malware discovered by ourselves and our colleagues in the industry. Last year we discovered 65,000 unique pieces of malware in the mobile industry, identifying nearly probably about 33 million infected devices of which nearly 3 million were here in the U.S. alone.

So, I get the question a lot, which is, you know, are we here in the U.S. immune to malware attacks or to, you know, to hacks on our devices. We're not. There is no concept of a digital border out there. So, attacks that emanate from various countries or various environments around the world really can spread fairly quickly through mobile environments.

Just in the first quarter alone we discovered 25,000 new pieces of malware, so it is something that's growing. Today because of the power of Android, you know, it's not to say that is -- Android is an amazing

operating system, it's what's leading to the innovation that we're seeing. But it's those same capabilities that are being exposed to developers to allow folks like us that develop really rich applications that also malware that malicious actors in the system are targeting.

You know, I went through this, I mean, if we think about the sum of where the infections run most rampant, you know, China, India, Russia, U.S., Thailand, Saudi Arabia, these are some of the countries that are highest on the infection rate list. I think just if you rewind the clock four years and ask yourself why they started to happen in some of these environments, as IOS and Android really starting taking off, app stores and regulated app stores really focused on markets -- Western markets, like the U.S. or Western Europe. It left a lot of devices -- it left a lot of markets, such as China, India, Russia, and other emerging markets to have a much larger ecosystem of app stores as Steven mentioned.

We today scanned probably over 5 million applications distributed through over 400 different marketplaces around the world. So, there is a significant number of marketplaces where apps can be published and republished. And with the sources of how you can download those today, whether they be through emails, whether they be through links transferred through

text messages, it's a lot easier to get access to those as well.

Actually, one thing worth talking about is, you know, there's a lot of different threat vectors as well, whether it's, you know, root exploit, spyware, trojans that are meant to take control of devices, but also there's a significant amount of monetization happening where malware's discovered to collect and profit from users' personal data. Given the amount of information that we're collecting on our own devices about ourselves, there's a very intimate relationship between a user and their mobile device, much more so than the PC.

The PC has become a one-to-many relationship. It sits on your kitchen table; it sits in an environment where it is a one-to-many relationship. Over half of Americans admit to sleeping with their mobile devices under their pillow or by their bedside. We don't really do that with a PC, at least we don't anymore. So, the intimacy that we have with our devices and the dependency we have is what really creates a lot of those exploits that can happen as well. And, really, it's not about hacking for sport; it's about hacking for profit at this point.

We discovered a malware in January called Bill Shocker, which was an app repackaging, and I know one of

my colleagues on the panel will talk about app repackaging as well. It had infected over 600,000 devices. And what it was was it was deployed through otherwise legitimate applications that people were downloading, and it had taken control of the ability to send text messages, and it was monetizing from a hacking perspective the traffic associated with that to ad networks. So, there's a significant amount of profit to be made for hackers within this environment. If there weren't, they wouldn't target these devices to begin with.

You know, the other thing that we're seeing is for the first time last year it was confirmed within the industry that there was a crossover attack that happened between PC and mobile where we saw the ability for malware from a PC to be distributed to a mobile device via USB attack. So, as you're connecting your mobile device, whether it's an Android device or some other type of device, it was installing itself using the USB port onto these devices and the file systems. And that can -- you know, that can emanate and continue to propagate through a system in the same way that any other malware can.

So, what's the real risks? You know, from a risk perspective, it's not just app repackaging, but what

we're seeing from a consumer perspective is people are installing applications from third-party ecosystems. You know, it's not necessarily Google Play that's an issue; what we've seen -- you know or regulated marketplaces, because what we've seen it's the social recommendation aspects of marketplaces like Google Play are extremely effective. The fact that we, as consumers, when we go, we look at star ratings; we look at how many times they were downloaded.

And despite the fact that there may be two or three of some applications that may be distributed on that marketplace, we, as consumers, have been trained, you know, over the last several years that we look for the one that has 10 million-plus downloads or three-and-a-half or four-star and above ratings. So, there's -- while it's not perfect, the self-regulating environment of a marketplace is actually quite good, but it doesn't necessarily protect you from downloading, from side-loading, or downloading off of a link.

The other thing is that the fastest growing demographic of ownership is teenagers, tweens and teens. You know, my tween-aged son is a user of our smartphones, and we use our products to help protect him, and what we need to do as parents and as adults, you know, our responsibility is to protect our kids in these

environments, because these phones are always with them. And they're not necessarily always trained to know what the best way to use their mobile devices are. So, there's tremendous amount of responsibility on parents to secure their kids on their mobile devices.

And then I think we already talked about fragmentation of operating systems. You know, what is the harm to consumers? It's everything from bill shock to smishing attacks, which is social engineering based attacks, where hackers are collecting information through various types of attacks. I think one thing that we're saying is that phishing attacks are much more effective on a mobile device than they have ever been on a PC.

And the reason for that is the fact that URLs are obscured on a mobile device. You only have a four-inch screen. You only have a four-and-a-half-inch screen. So, the fact that most often URLs are obscured or you have this concept of tiny URLs, you're not really -- you don't know as often that you're heading off into an environment where a phishing attack is happening and so you're more prone to -- and more vulnerable to those. We scanned, you know, over 2 billion URLs last year. We found over 5 million malicious URLs out of those 2 billion. So, there's a significant amount of malicious URLs out there.

You know, rogue Android apps on third-party markets, mobile browser redirects, I think all of these are well documented at this point. I'm sure we'll discuss them on the panel.

What could happen in the future? You know, we've talked quite a bit about app repackaging and other types of attacks that are happening, including phishing. But metamorphic or polymorphic malware, you know, we, as antivirus, anti-malware makers, have very advanced engines to help discovery and resolution of mobile threats, including malware. But as apps either update themselves, both either on the client side or through server-based updates, they change very, very quickly. And we will see -- we haven't seen it yet -- but we believe we will see these types of apps continue to or start to propagate in the industry, and we have to be prepared for them from a technology perspective.

Again, you know, botnets are very well documented in legacy technology environments. We haven't seen it on the mobile device just yet, but I think with the continued deployment of IP-based networks, you know, we do expect this, you know, mobile device botnet, and I'm sure, you know, Gareth will probably give us some more insight on this to possibly start to propagate in the next couple of years.

And then reverse-engineered Android attacks, which means beyond just repackaging. It's a complete breakdown of otherwise legitimate apps and repackaging. But, you know, we use techniques such as compares and diffs to identify where an app has been hacked or malicious payload has been added because it has a difference in file size. But as you do complete reverse engineering, you can minimize that file size difference, so some of the more legacy-oriented opportunities for you to discover that malware may not necessarily be there in the future. So, it's incumbent upon us to innovate our engines to continue to foster discovery and resolution of these threats.

So, I think that gives a fairly good background of what's happening in the industry, at least from our perspective. I'm here not representing myself but 300-plus engineers that focus on protecting consumers, enterprises, and carrier networks at NQ Mobile and driving trust within the mobile ecosystem. And, you know, I'm going to go ahead and join the panel at this point. Thank you.

MS. BURTON: Thanks, Omar. I think your presentation raises a lot of great topics, but I want to start by asking you to give us a sense of how NQ defines mobile threats. You mentioned that in April you found

7,000 -- more than 7,000 mobile threats. But when you say that, what are you talking about specifically?

MR. KHAN: So, when we're talking about that specifically we're talking more about unique malware signatures, so, you know, where we are updating one of our data bases or our virus or malware data base to catch or identify and resolve some of these threats. But it does go beyond that.

And, so, while we sit here talking specifically about malware that can infect a device or target a device through distribution through the mechanisms that I talked about, whether they be third-party app stores or malicious link-based downloads, it goes well beyond that. It goes into phishing-based attacks where I talked about, which is not necessarily captured when I talk about that, you know, when you are phished for a one-time password because you've been taken off into a URL that you were unsuspecting. That's a very legitimate threat that happens, and it's something that can happen not just on Android, it can happen on any mobile device.

So, the fact that we may sit here thinking that we're immune if we're not carrying necessarily -- if we're carrying an IOS device or a Windows-based device. You know, web-based attacks or mobile browser-attacks are just as significant and just as valuable and can create

just as much pain for a consumer as a malware or an app-based attack. So, it does go beyond that, but we specifically -- when we talk about those types of quantifiable statistics it's related to malware.

MS. BURTON: Okay, so, it's malware-plus?

MR. KHAN: It is malware-plus, absolutely.

MS. BURTON: Okay. So, Gareth, at Adaptive Mobile, is that the same approach you use? How do you -- when you're looking at a threat, how do you define what a mobile threat is?

MR. MACLACHLAN: What I think for us, because we have a different approach, and we sell to mobile operators, not to consumers, and we don't sell to corporate, so we're not interested in trying to get people to buy a piece of software to put on their phone. We actually look at really what's affecting their pocket, where are people losing money. You know, for us, it's actually more important to look at situations where people might find that they're responding to SMS and signing up to premium rate services and losing 20, 30 bucks a month than something which is a pure technical exploit.

Similarly for us, the growth within spyware, the fact that you can go onto ebay now and download phones or buy phones which have already had spyware

preinstalled so you can track someone's calls, monitor their text messages, have those uploaded. All of those for us kind of come into the overall umbrella of security threats that we need to look at as an industry and protect consumers from.

MS. BURTON: And how does Adaptive Mobile identify those threats?

MR. MACLACHLAN: Well, because we sit within an operator's network, you know, we're seeing these threats at scale, we're processing about 28 billion events every day, SMS web requests, instant messages. We're seeing this across, you know, 60-plus operators around the world, so we're actually getting to see these threats as they emerge.

I think one of the key bits for us, and we often hear, you know, reports about how fast Android is growing, 600 percent uptake in the number of mobile malware out there. Android viruses are actually very easy to write. Most of them people will take a legitimate application off a standard app store; they'll spend 25 minutes adding a little routine into it; they'll repackage it and they'll throw it up on a third-party app store.

If you look at the number of individual families of viruses, there were about 450 found last

year. What we report as variants tend to be lost copies of the same underlying virus. So, we're at risk of, in my view, creating a hype that says this is growing. No, it is a problem, you know, an individual who gets infected can lose a lot of money. But in the broad marketplace, we see very low levels of actual infection. You know, you have to do -- you have to be very careless in many cases to become infected. So, there are things that consumers can do to make sure they're not at risk.

MS. BURTON: And we will certainly get to those, but I wanted to ask Dan and Patrick, in your research, how are you defining mobile malware? Both of you have looked at that in the wild quite a lot. What are you looking for?

MR. GUIDO: Sure. So, I take a pretty conservative approach to what I define as mobile malware, and I typically put the boundary at unauthorized access to data. If it's something that I installed, whether knowingly or unknowingly it tries to access data, and I've given it permission, that's more of a privacy issue to me.

But when it exploits a flaw that I didn't know was present in order to access data outside of what I gave it access to, that's what I start to determine is a piece of malware. And there's many of these flaws that

are present on devices. The ones that most commonly get exploited are these things called jailbreaks, which can be used for good purposes and bad purposes, but when they're included in a piece of malware, they give access to that piece of malware all of the data on the phone.

Many of the other threats outside of that that have been mentioned so far aren't very specific to mobile. They also occur on the desktop. They're just slightly different in flavor on mobile devices because of the difference in user interface. So, I'm a little bit less interested in those as a unique threat and more interested in the kind of app-based attacks that are very prevalent on those platforms.

MS. BURTON: So, Dan, you're looking at what it does to decide whether it's malware?

MR. GUIDO: Yeah.

MS. BURTON: Okay. What about you, Patrick?

MR. TRAYNOR: Just in the interest of time I'm going to say that I largely agree with what's been said and the research that I'll talk about in a few minutes, actually it takes what the community has defined as malware and looks for that. So, I mean, this is in many ways sort of a moral gray area, right, there are apps that do a lot for you but require a lot of your private information to do it. Are they good? Are they bad?

This is very much in the eye of the beholder.

So, when I talk about mobile malware, it will be things that others have actually as a community said we all agree that this is malicious.

MS. BURTON: Okay, okay.

I'd like to shift the discussion a little bit to the different threat vectors. And, Omar, you certainly touched on several of these, but Dan has done a lot of research into the various ways that malware gets onto a device. And, so, if you want to talk a little bit about your research --

MR. GUIDO: Sure.

MS. BURTON: -- you can step up to the podium.

MR. GUIDO: Okay, great.

MS. BURTON: And if you want to use your slides there, the only way you'll be able to see it.

MR. GUIDO: That's all right. The slides are just up there for reference for you guys.

So, as was mentioned, I'm Dan Guido, I'm from Trail of Bits. We help companies understand attackers much, much better than they do today so that they can build more effective defenses based on that knowledge. Rather than specifically focus on vulnerabilities or malware, we tend to look a little bit at a higher level and we look attacks and we look at the goals of those

attacks and how attackers achieve them. And this more holistic understanding helps us do more things like explain why certain trends are coming about, why attackers are performing one action, and what they're going to do next, so we can be kind of predictive.

So, as has been mentioned, there are many vulnerabilities on mobile devices today, and people can come up with new ones as much as they want. You can talk about apps attacking other apps. You can talk about NFC and short-range wireless being able to break into phones. You can even read data directly off chips with a radio located a couple of feet, 20 feet, away.

Unfortunately, we don't see -- or fortunately, I guess, we don't see a lot of those attacks exploited in the wild. Instead, what our analysis really provides at Trail of Bits is we try to separate the possible attacks from the probable attacks. And the way that we do that is through this kind of economic analysis, which is very similar to how maybe an MBA would help a company determine if they want to enter into a new market or if the company they work for wants to enter into a new market in like consumer product goods.

They're not chaotic decisions. They're very deliberate, made on behalf of the attackers. So, we look at things like how large is the market; how large are the

number of users that we can target; out of those numbers of users we can target, how many can we convert into users of our malware; what are the conversion rates, the capture rate that we can ensure in that given market; and then what are operating expenses in order to perform that attack, do we have the human resources to perform it, do we have the technical resources to perform it, and how expensive are they.

So, all this kind of boils down to some of the formulas that I have up here, very simple. A lot of people think of cost of attack as just ease, but it can be a lot more than that. There can be a risk of enforcement if I go to jail or if I get removed from the app store and my information gets banned, and I might have an established process that makes it cheaper.

Potential revenue can come from things like number of targets, value of data, and the ability for me to monetize it. I might collect data that's really hard for me to make a profit off of. So, you know, certain types of data are going to be more valuable than others.

So, going by this kind of economic analyses, what we see are that there are basically factories that have been set up and set business processes that are already established from being abused within the malware ecosystem. Basically, when we look at mobile malware

today, this is the process that nearly all mobile malware takes in order to abuse data on these devices.

All the new kinds of malware that you hear about, most of the new kinds of malware that you hear about are simple variations on these six steps. So, first, we just set up the malware. We've talked a little bit about app repackaging. Developing malware is very, very simple. You have to make an application that has no UI that reads a website and does something different based on what it sees. It's probably the most simple application you can write. And people can come up with thousands and thousands of variations on this in a very short amount of time.

We take that, we add it to a legitimate application or something that looks like a legitimate application. Now we have all of our capabilities set up. Now we have to scale it out. We have to put it online somewhere where other people can see it, and we have to drive installations of it. The driving installations part is really where there's a lot of variance. We can drive installations through convincing people to install apps through SMS, through putting them on an advertisement on a website, we can send them emails, we can put them in a legitimate app store, in a third-party app store, and we can game the metrics on that app store

to push them higher up in popularity ratings.

At that point, now we have applications of our creation on people's mobile devices. And at that point, that's where we want to start gaining access to data that we need and getting it back to us. So, the primary way that we do that is we break out of the application sandbox that's present on most mobile devices, and we do that with a jailbreak. These are unpatched flaws that are present in mobile devices that allow me to access data in another application's sandbox. And there are many of these come out quite frequently.

After we gain access to all that data, we need to take it, bundle it up, and send it somewhere else. And that can be a website, something that I set up to just store that information. At that point, it's just, you know, abuse. We have to take the data, do something bad with it. And that's a little bit outside the scope of this discussion.

So, I like framing these kinds of attacks in this very systematic process, because it makes it clear that if we disrupt one of these steps then the person can't get to the bottom and achieve their goal. If they can't put the app on the app store, if they can't put it online, then they can't get to the next step where they get you to install it. If they can't get you to install

it, then they can't get you to run the exploit and so on and so forth.

So, this really frames a good discussion around what are the defenses that are going to prevent this threat and what are defenses that might be outside the scope and prevent other threats that we might care about but not as much as this dominant one.

It's also nice because it evolves our response beyond just the vulnerabilities. We take a look at the whole system, and we can mitigate the kind of process that they've set up, rather than just focus on particular vulnerabilities. We can look at maybe what makes the vulnerability useful in the context of this attack pattern.

So, keeping with our kind of economic analysis, if you're in business, you might call this value chain. If you're in the military, you might call this is a kill chain. And this is kind of ideas that have been adapted from other environments to work for security.

So, to use this -- to use an example of why we see certain attacks and why we do not see others, I wanted to talk a little bit about the web. So, many people are concerned with the fact that we have web browser exploits on desktops, and that is the dominant vector through which desktops get compromised. And we

think that mobile is going to be the exact same thing. But so far that hasn't been realized, and I'm going to show why it's probably not going to be realized.

So, first, if we think about it, constructing these attacks to take over the web browser, to exploit the web browser and gain access to its sandbox, and then break out of that sandbox and access data from -- here I just have Twitter and Bank of America, but it could be any app. We need to construct a radically different chain of events in order for that to happen. We need to change how we develop the malware; we need to change how we put it online and how we distribute it. And all these things are new processes that I need to set up as an attacker that has a cost associated with it, that I need human resources with skills to be able to do, and it may affect my operating costs in a prohibitive way.

So, when we look at the mobile malware community and we ask, do they have the skills to write things, that can take over the browser, overwhelmingly the answer so far has been no. The only things they're capable of doing are using code that's been published online already by other smarter people outside maybe in the security industry that don't have malicious intent, and nobody's really publishing that code, so they're not using it. But it's more than just exploits, right? They

have to set up all this other infrastructure in order to launch these things and be able to construct a process that abuses them.

So, how does it affect my market size? Well, if I'm Facebook or I'm a normal mobile -- if I'm a normal company that wants to gain access to mobile devices, like Facebook, the kinds of decision-making that I go through are, well, I could set up a mobile website or I could make an app. And overwhelmingly legitimate companies decide to create apps because it's a much more effective way to get eyeballs on a mobile device.

So, the web browser perspective here is going to have a smaller market and it's slightly harder to reach these people because the advertising mechanisms that get me access to all these kinds of popular websites are a little bit harder to get into. They're more expensive; there are less advertisements present on mobile websites; that sort of thing.

So, it's harder, also, because when we're looking at mobile browsers -- I guess I should explain the slide, shouldn't I? When we look at mobile browsers, we have to use two exploits. So, first, we have to exploit the web browser, and then from the browser we need to break out of the sandbox that it's inside to access these other applications. So, now I've doubled my

operating costs. I need two exploits instead of just one.

So, in summary here, what I'm saying are that web exploits on mobile devices are definitely possible, and people can prove that to you at any security conference you attend. But are they probable? I'm going to say probably not, simply because the processes to take advantage of these things are not set up and the skills to perform these attacks are not widespread.

So, at Trail of Bits, we have a very conservative estimate around the development of mobile malware. We think it's going to be very app-centric for quite a while. And when we think about the mobile malware community, we think of it more like enterprise software development than we do like Silicon Valley startup. It's very deliberate; it's very slow; and they're not quite doing a lot of innovation. They're looking at business patterns that scale and that work well that they can profit off of effectively and repeatedly. And that's all I have to say.

MS. BURTON: You're not done yet.

MR. GUIDO: Oh, am I?

MS. BURTON: You can have a seat.

MR. GUIDO: Okay.

MS. BURTON: But I've got some questions for

you. So, we have all seen Batman movies, and hence we know that there are bad actors out there who are not motivated by profit, who are motivated by, you know, political motives or something else. Is it -- your argument seems to be we should focus our efforts on what's -- you know, from an economic perspective what's most likely to happen. But would it be appropriate for security companies to sort of ignore the crazy bad actor who could do something really bad?

MR. GUIDO: Sure, so I guess the elephant in the room is Anonymous or something like that.

MS. BURTON: Uh-huh.

MR. GUIDO: Yeah, so, groups like that are technically not very sophisticated, and they tend to create very simple tools that can be distributed on a wide scale so that nontechnical people can perform these attacks and aid these kinds of denial of service attacks. I actually liken it to kind of an open source scenario, where a couple -- 10 years ago, we all thought open source was going to take over the world, it's going to be a threat to all commercial software. But it all depends on people's free time to add to this kind of development, and you have to have a very charismatic personality in order to convince all these people to give up their time and contribute it to your project and make it successful.

So, we haven't really seen a lot of these open source -- pure open source, not commercially supported open source take over the world. And it's the same kind of thing with threats like Anonymous and other people that are not financially motivated. They have less incentive to construct the elaborate and sophisticated, highly reliable, dependable attack patterns that other groups do. So, the kinds of things that I see from people that are not financially motivated tend not to be very sophisticated and not very much of a threat at all.

MS. BURTON: So, Omar and Gareth, are you seeing attacks that you would -- that sort of fall into this category maybe of not financially motivated? And do your products protect against those? Are you looking for them? Are you finding them? Are they out there?

MR. MACLACHLAN: Well, I think one of the big questions for all carriers is do we have mobile botnets and how do you detect them and who's running them. Now, botnets are out there, and some of those are being used for financial gain. Now, there are others we've detected, and you can't see an immediate financial return from them. Now, that could be that actually it's just a badly set up organization who hasn't quite got their business model right, and so are missing the opportunity to make money.

But there are situations where we've seen devices under the control of a command and control service sitting outside in other countries. And, so, from a critical infrastructure protection perspective, you immediately start looking at those in more detail to start to understand, well, if you do have mobile devices sitting on a network, which are waiting for commands from China's MMA and servers in Southeast Asia, for example, at what point could those be used and what could they be used for?

MR. KHAN: I mean, I would agree with that. I mean, I think have we seen attacks that are not financially motivated? Yes. And we actually saw the most dramatic decrease we probably saw was, you know, I think initially it started and I think it speaks to the evolution as well as the lack of sophistication. You know, the highest instance was at some point, you know, taking remote control or this concept of, you know, trojan horses, but that's significantly decreased.

It's being much more motivated now by, you know, financial gain or gaining access to personal information. And I think it also has to do with the fact that it's not just a single collection effort that can be monetized. Oftentimes it's a multi-pronged effort that has to take place to be able to create something that

from either a premium rate service perspective as well as a data dump where I've collected enough personal information that I can monetize, you know, on the black market. It takes -- it takes some collection effort and some social engineering effort as well.

So, yes, do we protect against it, but I do agree with the panelists. I think where the industry is headed, as well as where the majority of the effort, if not more the sophistication is going as more towards financially motivated attacks.

MS. BURTON: Okay. So, I was reading last night some colleagues of Patrick's at Georgia Tech have created an iPhone charger that can inject malware into a phone when it's being charged. And I think we're going to hear more details about this at the Black Hat conference, but are these types of infections something that, Omar, your security product could actually protect against as well? Like how would you know if a device was infected through hardware? Or is that something that's kind of -- there isn't a protection against that at this point?

MR. KHAN: I mean, in terms of the incursion itself, that's not -- I mean, you know, that's not something that we would necessarily identify, whether it came from, you know, through a USB or whether it came

through, you know, through a web-based or IP connection, et cetera. It's really, you know, as an endpoint security company, you know, we're looking for, you know, once the payload has either been delivered, comparing it to what, you know, what is known to be malicious -- you know, a malicious payload or a malicious software attack or if a user is headed off into a web environment.

Again, you know, I agree with Dan that highjacking the mobile browser isn't really what's happening. It's more from a web perspective the phishing attacks, but it's not necessarily the delivery mechanism today, which is why from our perspective a lot of it has to do with education to the consumer of, you know, turning on -- turning off WiFi, turning off blue tooth when you're not using it, as well as teaching folks the safety of connecting to various third-party sources. You know, those are some of the things that from a consumer education perspective are paramount as well. But, no, not necessarily what Patrick's colleagues have done.

MS. BURTON: Okay.

MR. TRAYNOR: I just want to add something.

MS. BURTON: Yeah.

MR. TRAYNOR: I think that we're leaving out -- we're very focused on the mobile device, but if we're talking about an adversary who may or may not have a

financial interest, say a state actor, we haven't talked about the networks at all. And the networks are full of vulnerable, unauthenticated protocols. So, if that's the kind of adversary that we are worried about, I don't see a state actor necessarily trying to shut down the network by infecting a huge number of devices when they can with a single device, you know, talk to specific nodes in the network and shut down all traffic. So, you know, I think we need to be sure that we consider the network aspects as well as the end devices.

MS. BURTON: Right. And, Gareth, is that where you come in?

MR. MACLACHLAN: I completely agree. From the network perspective, you actually don't care whether an application was written for malicious purposes or whether it was just badly written, you know, something which just sits on the network and starts to, you know, is too chatty, sends too many requests through the cell towers can have as much of a problem for an operator as something which is designed to actually cause problems itself.

So, an operator is always concerned about the fact that, you know, any application could potentially use up all of the resources within location. If that was in, you know, downtown DC, it would start to have a major

impact upon the revenue for that particular carrier.

MS. BURTON: Okay. Patrick, you've provided a perfect segue to your own presentation. So, maybe we'll hear from you now.

MR. TRAYNOR: Funny how that works out.

So, I want to start off by telling you a story about why it's wonderful to be a professor. And that's one of the really great things is that I can have random and arbitrary projects, and I have an army of students who will help me do those things. Let me tell you about it. So, a couple of months ago I stormed into my lab, and I said, everyone, drop what you're doing. For the next 30 minutes, I want you to find the most outrageous news stories you can possibly find. That's the job. Come back to me in 30 minutes.

So, we got back together, and the students provided me things better than I could have hoped for. For example, it turns out the highest number of Bigfoot sightings occur in Ohio. And if you ask local police in Scotland, the Lochness Monster, absolutely real. In fact, if you're from the West Coast, the chupacabra often suns itself on the beaches in San Diego.

Now, we can all laugh at this, of course, because these are extraordinary claims and they require absolutely extraordinary data to support them. And we

don't have that data, so we laugh. So, the next part of the assignment was, okay, I want you to go out and look for news stories that are related to your research, that have similarly large claims that we can't necessarily address. And they came back with some of the headlines that I'm sure you've all heard. Android malware is exploding 1200 percent this year. My favorite article, to cut right to the punch, was that Android has become the ultimate platform for malware. Okay, imagine this: as bad as Windows 98 was, we haven't learned anything in over a decade since then; Android far worse.

Here's where the cognitive dissidence comes in, though. I don't know anybody who's ever been infected. And when I give this talk at universities and to companies, most people say, oh, well, yeah, I knew a friend of a friend of a friend who was infected. So, how can I provide people with good advice when I can't really measure the problem, and how do I know that we're doing better without measuring it.

So, that's what we at Georgia Tech set out to do. We partnered with a major cellular ISP in the U.S. who asked to remain nameless, but we'll say that about half of you in the room are probably customers. And what we did was we sat at their DNS resolver and watched traffic for about three months. Now, if you're not

familiar with DNS, this is what turns CNN.com into an IP address. Okay, and we know a lot about DNS as a means of identifying malicious domains, malicious hosts.

And, so, we had a couple of very interesting findings that I'd like to share with you. Yeah, as a professor, I'm going to have a couple of graphs and numbers, but I'm going to hit the high points as quickly as I can. All right, the first thing is, so, what is this mobile web, all right, what are these apps, what are people's browsers talking to. And when we compared the hosts that were hosting these -- the, you know, the apps and so forth, it turns out that we see almost 99 percent of those hosts in traditional wired ISPs, which means that all of the reputation data that scientists like myself have spent their careers amassing, and many companies do this as well, we can also use to reason about maliciousness. So, great, the mobile web is the web. It's not terribly surprising, of course, that people who have web pages reuse many of those servers to support their mobile apps.

The second is this: Did we actually see mobile malware? Okay, mobile malware in general is going to resolve some domain so it knows -- or some host so it knows exactly who it should talk to, even mobile malware, by the way, that's involved in SMS premium number scams.

What it will often do is go out and say, hey, are we still using this short code to rip people off, and the response will come back, yes, we are, and then it will send off the message.

Okay, so, we went and we opened up all of the mobile malware that was available to the community a year ago, and we also then went to antivirus providers and said tell us the domains, the hosts that you've extracted from mobile malware. That way we can get the community consensus on what's malicious and where it's talking to.

And here's what we say. We actually saw mobile malware at work. You can see for some of these, for example, we saw a few thousand devices, 5-, 6,000 devices, that were infected during our three-month study. Okay, that's bad, except for when you put it into context, okay, that over the course of our study it turns out that less than 1/111,000th of 1 percent of devices in this provider's network were infected with what the community agrees is mobile malware, malicious applications.

To put that into context, the National Weather Bureau, I apologize, says that the chances of being struck by lightning over the course of your lifetime are one in 10,000. Okay, so, during the course of this study, you would be far more likely to have been struck

by lightning than to have been infected with mobile malware.

Okay, that's not the end of the story, though. We looked at all that reputation information that we had, and it turns out that mobile devices are talking to a significant number of malicious hosts. The column that I want you to care about is the middle one with these 8 percent numbers. And I break out IOS here separate from all other, but I can give you a breakdown. They all roughly end up at 8 percent.

And what we show here is the following, that 8 percent of all devices in each population, if you're an IOS user, you're an Android user, if you're a Windows Mobile user, go and talk to known malicious servers, servers that we don't have information on in terms of mobile malware. Okay, so, the thought that IOS is somehow magically safer than any other device or that Android is somehow automatically worse than any other device, don't stand up to our analysis from the network perspective.

Okay, so I want to finish my time here with the following: I'm not saying that maliciousness is impossible. What I'm saying is that for all of the downloads, for all of the variance that people say that we're seeing, from the network perspective, we don't see

infection happening all that often. If you'd like to know more details, of course I'm available after this and the paper and our methodology are public. So, I encourage you to take a look at that and judge our measures. Thank you.

MS. BURTON: Thanks, Patrick.

Omar, I think NQ's estimate was something like 2 percent of devices in the U.S. are infected. This was not in your presentation, but I think when you and I spoke earlier that was the estimate you gave me. How do you explain the difference between that statistic, or you can give me a different statistic, I don't want to put words in your mouth, between that statistic and the numbers that Patrick's seeing in his research?

MR. KHAN: Yeah, I mean, those are -- the statistic that you mentioned is correct. I mean, that is what we are seeing within the environment. And it's -- the prevalence rate, I mean, is significantly higher outside the U.S. than it is in the U.S., but the infection rates we're seeing versus the libraries that we maintain are on that order, obviously primarily on -- within the network of devices today. But the reason we're also seeing it specifically is because I think the fragmentation of operating systems or fragmentation of updates that was mentioned earlier also creates some of

these vulnerabilities.

You know, we'll definitely follow up with Patrick and his team on collaborating on the libraries and making sure that the data correlates, but, you know, from our perspective we've got, you know, eight figures of installations in the U.S., so a tremendous amount of data, and nine figures of installations around the world, so a tremendous amount of data coming in around what the infection rates are.

I would agree that generally the propagation rates are fairly low. So, when we do see -- I mean, even the 600,000-unit attack that we saw happen in the Asian market, that was significant, you know, by and large -- far and away the largest infection rate. Generally, the infection rates are lower. They don't propagate as quickly. And the instances are significantly focused in markets where third-party application marketplaces are a source of distribution.

I think if you were to walk around this room or just do a show of hands of folks who have IOS or Android devices and who had performed an installation outside of Google Play or outside of iTunes App Store, it's probably very low. How many of you have actually installed an application outside of IOS, iTunes, or Google Play, and outside of the industry that we're in, right?

MR. TRAYNOR: Now, put your hand down if you're a technical expert or on a panel today.

MS. BURTON: And don't admit it if you're from the FTC.

MR. TRAYNOR: My statistics professors would be upset about sampling error here.

MR. KHAN: So, yeah, I mean, it's probably a curated sample here that we put together. But I think that's what it speaks to, right? It speaks to the fact that the instances of third-party app downloads, third-party marketplace downloads are significantly higher outside the U.S. It doesn't mean we're immune here, but, you know, we'll definitely follow up. So, yeah, 2 percent is the right number based on our network statistics.

MR. TRAYNOR: One of the things I want to add to this is that I think the picture of third-party apps as -- or third-party markets as sort of always polluted, always bad, is changing. And two years ago I think that this was very much the case, but third-party app stores realized that they'd like to make money too. And you can't make money, or it's harder to make money as a legitimate app store, if you're known for hosting a lot of malware.

So, many of these that we've looked at have --

since our initial studies have partnered with some of the big A/V companies and really tried to clean out their markets. So, I think the picture is changing. By the way, the whole concept of marketplace really changes this space. I think it's actually significantly more difficult to infect user devices, if you're one app in a sea of a million others. I mean, how do you pull people in without attracting the attention of Google or whoever is, you know, doing the auditing of this third-party market without advertising? Right? I mean, if I know how to write an app that was going to get 10 million users, I could probably come up with a better way to monetize it than steal their data, because I'd like to remain in the app store long enough to make some real money. So, I think the app stores really changed the dynamic of maliciousness in this space pretty significantly.

And I do want to say that that's not to say again that people like Jon Oberheide can't get lots of malicious apps into the market, it's just that they don't last for very long, or he gets blacklisted.

MR. KHAN: No, app store scanning is definitely -- you know, has been implemented. I think the app stores are cleaning up. We're seeing the same thing. But we're also seeing a rise from distribution directly

from servers as well, so I think the concept of that being replaced is definitely happening out there.

MR. GUIDO: So, that kind of analysis leads you to think that a lot of the malware that is incredibly malicious is very bursty in nature, so it comes out, it infects a lot of people, and it goes away as quickly. Could it be that a lot of the historical data you have doesn't overlap exactly with the period of burstiness of the malware that you're looking at?

MR. TRAYNOR: So, the great thing about this is that all of our methodology is public.

MR. GUIDO: Okay.

MR. TRAYNOR: And I will point you to the paper. But the answer is of course it does.

MR. GUIDO: Okay, just checking.

MR. MACLACHLAN: So, coming back on the point about advertising, to Omar's point, we're seeing a large growth in terms of directly linked malware, so malware which isn't being hosted on well-known third-party app stores. And you've got to remember, outside of North America, the majority of users will go to third-party app stores. As an example, a Russian malware group in March this year pushed out SMS messages to over 2 million subscribers, all of which directing them through to one of 98 variants of a new piece of malware. And all of

that was just hosted on servers; it wasn't on well-known app stores.

So, I think people are realizing that app stores are starting to become a hard place to set malware up. But it means that we're now seeing lots of people being promoted through links in games, through SMS through to their phones, and people just have to click on that, and it immediately starts downloading, if they've already given approval to download things from third-party stores or off-market sites. They've removed that one key piece of protection that they have on the device.

MS. BURTON: Dan, do you agree that -- I mean, that --

MR. GUIDO: That fits the pattern. It's just when we look at the step, you know, when we want to take the app and we want to put it online, we can put it on our own server, we can put it on a third-party app store, or we can put it on a first-party app store. And it just affects how many people you can potentially reach, because you can still advertise something in a first-party app store with an SMS. You'll probably have a little bit of a larger market that way, because you'll get additional installations through other means, through people just downloading it because they see it becoming popular. But all three of those are essentially

equivalent.

MS. BURTON: Okay.

MR. KHAN: I think it also speaks to consumer behavior as well, right? Because, I mean, here in the U.S. we're not as prone specifically to SMS-based marketing as emerging market consumers are. When you land in Thailand, when you land in India, when you land in China, when you land even in Mexico, the instance of SMS-based marketing is significantly higher than here in the U.S.

I think that, you know, it's -- so, the receptivity, as well as the likelihood for a consumer to click through on an SMS-based marketing scam or whatever it might be in terms of an attack it initiated is much higher in markets outside of Western Europe and outside of the U.S. than it is -- than it is here.

MR. MACLACHLAN: I've got to disagree with that. The U.S. is the biggest source of SMS spam, not just for Americans but for other countries around the world.

MR. KHAN: No, I didn't mean the location, but specifically users clicking through.

MS. BURTON: So, we're the source, but we're not consuming it.

MR. MACLACHLAN: Oh, okay. Well, that's good.

MS. BURTON: You can be proud of that.

MR. KHAN: No, no, you're absolutely right. We see tremendous sources coming from the U.S., but in terms of consumer behaviors, in terms of click-through, some of the incident rates or the click-through rates are higher in markets outside the U.S.

MS. BURTON: So, Patrick, you said that over 8 percent of people in the U.S. are visiting these malicious sites, but infection rate is incredibly low. And I think we've talked about as consumers we're a little bit better educated and maybe aren't clicking on things, but the 8 percent of people who are clicking on things aren't getting infected. What is the reason for that?

MR. TRAYNOR: So, I should add a few caveats. The first is that because we look from DNS I can't tell you if they clicked on it or how they got there, just that they go there. All right. I actually find this sort of encouraging. So, strictly speaking, with my technical hat on, that if the operating systems are -- and of course there are vulnerabilities -- but if the operating systems are hard enough to break that you can't do it automatically without having to trick the user, boy, I wish we were in that -- in that sort of standing in the desktop space. I mean, that would be amazing.

So, the fact that most -- a lot of what we see is really very much social engineering oriented, from a technical perspective is great, it means that we're actually doing our job. Now, the other panels today will, of course, talk about where we can improve what we're doing to reduce that. But spam click-through rates have been going down. And, yes, some people still do click on them, but compared to a decade ago, the percentage of the population that actually follows spam is decreasing. If we can continue to decrease that, I think that mobile will continue to be in much better shape.

MS. BURTON: And you think that's specific to U.S. consumers, or is that for those of you who are looking more globally, are you seeing a decline globally as well, or?

MR. MACLACHLAN: If I may, so, to echo Patrick's point, the mobile malware today is not a technical issue; it's social engineering. Most of the drive is because people want something for free, and if they can go find a game and get it for free off a slightly dodgy link, rather than paying 1.99 in Play Store, then they go and try and save the two bucks and not realize what they're losing.

And I think that's the same in every territory.

People are always going to look for something that's free and lose money that way.

MR. GUIDO: I think we need to differentiate a little bit between what we're talking about, because we're saying that a lot of this is based on phishing and social engineering, but that's the access into the device. Once it gets on the device, there are technical risks that are present inside the, you know, Android, IOS, Windows, whatever devices, and that's the jailbreaks, because without that, the only data that they're able to abuse are things like sending SMSs for toll fraud and, you know, bill shock, however you guys phrased it, as well as collecting data that's available to every application.

But if they want your banking credentials or if they want your Twitter credentials or social media credentials or other kinds of access, they need to break out of your sandbox. And that's a technical attack, and it's based on a technical weakness in a device that it's been installed upon. And there are certain, you know, manufacturers that are better at handling that risk and certain ones that are worse, and that creates a real difference for consumers.

MR. TRAYNOR: I totally agree, but I just wanted to again differentiate that if the user has to

click 17 times, I really want to download this, yes, okay, okay, okay, and then it jailbreaks the phone, it really is a social engineering issue, yes, but the user said yes. So, after -- a much more dangerous attack would be if the user said nothing. And, so, we're in agreement that, yes, there are absolutely problems with all of the platforms, with all of the pieces of technology, that software has bugs. But what I'm saying is that the vector in -- seems to be primarily requiring the user to do something.

MR. GUIDO: So, I'll add one thing. There's a lot of, like, folk advice that people give about not installing malicious applications on Android that's incorrect. A lot of it centers around permissions and looking at whether the permissions that a given application asks for are asking for too much, but when we actually look at what jailbreaks require in terms of permissions to be able to run it's nothing.

So, the kinds of things you need to click through are actually quite minimal, and the app is going to ask for very little. But the permissions that it can gain by itself through an attack is actually very large. So, that mismatch makes it more of a risk because consumers aren't going to be able to tell.

MS. BURTON: My question cards are building up

into a large stack. So, first of all, I'm supposed to remind everyone that if you do have questions for the panelists, please write them on a card, hold them up, for those of you who may have come a little late.

And I do want to get to a couple of these questions. One is via Twitter: What can cellular providers do to detect mobile devices infected with malware and prevent delivery of malicious traffic? And that seems like a Gareth question.

MR. MACLACHLAN: I didn't send that in myself, honest.

MS. BURTON: I think it's from the CFTC.

MR. MACLACHLAN: So, operators from where they sit can do a lot to find out which devices are infected. And one of the things we do by looking at the traffic that are actually flowing through the network we can identify which devices are compromised and what they're compromised with. And our stats end up being somewhere between Omar's and Patrick's and kind of closer towards Patrick's end, I think, than Omar's. You know, we don't see a lot of infections in networks today.

The key bit for an operator and the reason they're looking at this it's not necessary to try to stop people from becoming infected. You know, there are so many different ways you can infect a phone, but an

operator can't actually keep people safe all of the time. But the concern for them is, you know, the public are aware of mobile threats.

Talking to my mother the other day, who just got an Android smartphone. She was nervous about what she downloaded in case it got -- you know, she got a virus. And what happens is every time a consumer finds that they've got a charge on their bill they're not quite sure about or their credit's disappeared or their battery's run down, the first thing they do now is phone the operator to say, oh, it must be a virus, I've read about them. And that call costs the operator $10 to $15 every single time. So, the actual fear of mobile malware and the fear of infection can be a much bigger and much more costly problem for the operators than the actual number of incidents that are happening today.

MS. BURTON: Omar, are there certain groups or populations within the U.S. that are more vulnerable than others? I mean, I think you identified teens as one of the really vulnerable populations because of their behavior. Are there others that you've identified that particularly need to know about this?

MR. KHAN: I mean, I think, you know, other than specifically identifying teens or kids who are also, you know, more likely from a -- you know, as Dan said or

as Gareth said looking for ways around getting games and getting other types of applications and downloading free -- you know, free tools, free applications, for us that's behavioral. We haven't necessarily segmented, you know, from a personal information down because we don't collect that level of personal information down to specific demographics that are more at risk versus higher at risk. So, we haven't gotten down to that point.

But I think in general you would assume -- you would make the assumption just based on our panels or focus groups that we've done, it tends to be in environments that are less tech-savvy, you know, that are less -- necessarily less aware of what they're doing or what a specific click or what a specific permission set is that you're giving access to on a device. But beyond that, we haven't necessarily gone down to the demographic study.

MS. BURTON: Okay. One more question from the audience: What is the majority of malware designed to do?

MR. KHAN: So, I mean, the majority of malware still, I mean, based -- I mean, and I showed it on page, you know, whatever it was, you know, page 19 of the presentation, it's still even today, despite the fact that financial benefit or financial gain is where it's

going, but in our identification 65 percent was still root exploits, spyware, you know, pervasive adware or trojans or remote control of devices. And --

MR. GUIDO: They'll steal data later.

MR. KHAN: Yeah, exactly. So, I mean, those are the exploits that we still see as the highest majority, although that's been on the decline.

MS. BURTON: Okay.

MR. TRAYNOR: Just one thing just to add to that is, by the way, there seems to be a much lower rate of SMS fraud here in the U.S. than abroad, and one of the reasons for that is actually regulation of the way that short codes are managed here in the U.S., as opposed to in Europe or the former Soviet Union. So, having good regulations is actually a very good way to deal with this problem. It's a policy problem.

MS. BURTON: Thank you, Patrick. I'll pay you later.

(Laughter.)

MS. BURTON: I wanted to be sure that we had time to discuss emerging threats, because I think all of you are paying attention to what's on the horizon. And I guess one of the ones that we've talked about, at least amongst ourselves, is back-door apps, or they go by lots of different names. But I'd like to get a sense from

each of you sort of where you think we should be focusing our efforts in the future, so we can -- we'll start at the end. Let's start with Patrick.

MR. TRAYNOR: So, actually, I agree with Omar in many ways. I actually think mobile browsers are quite difficult to understand your security standing, even as an expert, and this has been shown by lots and lots of folks. While I agree that it does take multiple steps to break out of them, which by the way is why we haven't seen a fully automated breakout, if someone is able to do that, that's actually the area that I would worry about the most, again, with an "if."

MS. BURTON: So, that kind of raises the questions for Dan. Where do you think that falls in the probably versus possible -- is that something we should worry about?

MR. GUIDO: Well, I think it requires a large change in capability and a jump in capability from the kinds of people performing these kinds of attacks today. And what I see as a more natural progression is people shifting to back-dooring applications that are legitimate because desktops are compromised all the time, as well as developers of mobile applications, and all you need to do is go to one of these services that searches through data that's already been collected and find developer

certificates and developer credentials that allow you to upload your own repackaged application in the place of a legitimate one.

And we've seen this start to emerge where in the last few months there have been cases where people found these developer certificates and then back-doored legitimate applications in the app store. And the nice thing from an attacker's point of view is that it doesn't require them to do any new -- to have any real new skills. They take advantage of all the things they have already, and it doesn't really cost them much extra.

MS. BURTON: So, just from a consumer's perspective you're clicking -- you're downloading an app that actually is a legitimate app but without your knowledge it's been changed on the back end --

MR. GUIDO: Right.

MS. BURTON: -- and it is now a malicious app.

MR. GUIDO: Yeah, you would get an update and it would have something else inside of it.

MS. BURTON: So, it could have 10 million downloads and it could have five stars, but it's been changed and is now malicious, right?

MR. GUIDO: That's the risk.

MS. BURTON: Okay. And you've seen incidents of that? There have been incidents of that in the past?

MR. GUIDO: There have been incidents reported in the media in the last three months that took advantage of several legitimate applications on the app store through that method.

MS. BURTON: Okay. Gareth, where do you see things headed?

MR. MACLACHLAN: So, there's probably three areas that we're tracking. The first one is naturally back to a point from the opening comments by Steve. It's actually on the SDKs that are used to build apps, actually looking at how organized groups can put together new SDKs and make those available to developers so they've already got something with a back door included in a range of applications.

We spend a lot of time, also, looking at kind of the machine-to-machine environment that's out there because, you know, we come from a network-centric perspective. There are so many devices which now rely on SIM cards and cellular data as ways of communicating between each other, so rather than a consumer or an individual being attacked, it's looking at the security of the services, whether it's home automation, whether it's flood control, et cetera, that could be compromised.

And I think the new area is actually the new services that the operators are desperately trying to

launch. You may have heard of RCS, rich communication services, which is really the cellular industry's approach to dealing with WhatsApp and Vibram, and all the other over-the-top messaging services.

Now, those offer huge great opportunities in terms of ways in which devices can interact with each other. They can talk to each other, find out which devices are potentially vulnerable for attacks and carrying new types of attacks. So, that's an area that we're focused on very heavily with operators at the moment.

MS. BURTON: Okay. Omar?

MR. KHAN: So, I think we -- I mean, I agree with my colleagues that those are all emerging threat vectors. I do agree that, you know, the mobile browser is probably an emerging opportunity, although much more complex. I think what's going to end up happening, especially as we head into the next generation of mobile browsers as more and more device-level APIs are exposed within the browser for browser-based applications, you know, you'll see quite a bit more activity from a sophistication standpoint, because I think as we head into the future environment today, largely I think everyone agrees on this panel that it is really app-based distribution because of how easy it is to deploy apps,

because of the number of APIs that devices -- device-level APIs that apps have access to, that's where the vulnerability is, that's where the threat vector is.

As we head forward, where you have -- where applications and functionality starts to migrate back towards the browser and browsers become more and more powerful on the mobile device, you'll start to see more and more APIs being exposed to that direction. And then you'll see this native -- sorry, this hybrid environment develop, where you have native wrappers, but then you have browser-based code that's embedded within applications, so it changes the landscape quite a bit. It doesn't mean that's exactly how it will emerge, but I think that is -- that evolution will drive a new level of attention from hackers and create some exposure out there for us.

MS. BURTON: So, you think that there will be a shift back to browsers and how people use their mobile devices, and that's going to mean that that's where malware will shift as well?

MR. KHAN: It's already happening, right? I mean, it's already happening in terms of more and more functionality going back towards the browser. It doesn't mean that native applications are going away anytime soon; they're not. But there's more and more

functionality embedded within the browser-based applications or browser-based functionality being exposed to users, and within that, you know, browser redirects, whether it's, you know, just phishing or other types of incursions will increase in frequency as well.

MS. BURTON: Okay. Well, Omar, Gareth, Dan, Patrick, thank you so much for being here today. I'm sure people would appreciate it if you stuck around a little during the break in case they want to harass you with questions.

And for everyone else, please be back at 10:55 for our next panel. Thank you.

(Applause.)

PANEL 2: BUILDING SECURITY INTO MODERN MOBILE PLATFORMS

MR. SANNAPPA: Well, thank you, everyone, for joining us. We are really excited to have a great second panel consisting of a lot of the folks who design the systems that are built to protect consumers from malware and really getting a, you know, sense of how they're building security into their mobile platforms and what they're doing to address the threats that we discussed in the first panel.

So, we have here William Enck, who is an Assistant Professor at the Department of Computer Science at North Carolina State University. He has focused much of his research career on mobile system security.

We have Adrian Ludwig who is the Manager for Android security at Google. We have Michael Coates, who is the Director of Security Assurance at Mozilla Corporation. We have Geir Olsen, who is the Principal Program Manager for Windows Phone Engineering and deals with Windows Phone security at Microsoft.

We have Adrian Stone, who is the Director of Security Response at Blackberry. And we have Jane Horvath, who is the Director of Global Privacy at Apple, Inc.

And to give you a little background in terms of how I decided to seat the folks in this order, so, if you

see here Google and Mozilla with Firefox OS are, you know, open-source platforms, and with -- who have multiple partners that they work with in order to create the hardware that their operating systems run on.

Geir Olsen from Microsoft, you know, Microsoft Windows Phone is a proprietary operating system, but he, too, you know, deals with multiple partners in creating devices for Windows Phone.

Blackberry and Apple, however, are proprietary and integrated systems, meaning that they control both the operating systems itself, as well as the hardware. And, so, we thought this would be a good way to give a sense of that spectrum visually in terms of how these various operating systems fall and, you know, how they need to deal with different parties within the mobile ecosystem.

So, to get us started, I've actually asked William Enck to give us a brief overview of various protections and various mechanisms that are being used by the platform providers today in order to really define the very -- the terms that we're going to be discussing throughout the panel's discussion.

So, Will, do you want to take it?

MR. ENCK: Absolutely. Thanks, Nithan.

So, being the academic of the group I feel a

little obligated to teach a crash course on different terms and concepts that you might hear as we're discussing a lot of these defenses and protections that are being built into these new platforms. So, I think these slides are either available now online or will be soon, so I'm going to give just a high level of these things, and there is some more content on the slides themselves.

Now, a quick disclaimer, most of my research on smartphones has been targeted towards Android, and so that might bias my descriptions of this a little bit. We have a lot of great experts on the panel who can maybe give you more details on those different aspects. And of course I don't want to overstep Adrian on Google-specific things.

So, here's sort of an abstract view that I use to describe the platform and the scenario that we're dealing with. All right, we have an application market or an app store like Google Play, the Apple App Store, and this is the primary means of delivering these apps to phones. But this also provides us a mechanism to do some sort of security analysis of those applications. And, so, part of the platform security isn't just on the phone itself but also within the market of how we analyze these applications.

Once you get it on the phone, we have these apps, they're running on top of some very specific middleware for the different platforms, but below that we have a more traditional operating system, primitives and the kernels that's there. So, on the phone itself we have various protection systems that are going to help protect that phone. So, we have sort of two phases that we can perform protections in.

Now, when these new platforms were built, there was a redesign in sort of how they were architected. We no longer try to separate between different users. If you look at your PC, you have your login account and it's trying to protect from another login account on that. But that's not the case. There's really one user of this phone, and so now what we do is we separate between applications, and we're going to run those applications in sandboxes. And what this means is we're going to give it a limited set of access to different information and resources to every specific application.

Now, from there, we're going to gradually add access back. And these are what are commonly called permissions or capabilities to access this different information and resources, whether it be your address book, your location, the microphone, the camera. These are all permissions that are added back to applications.

Now, each platform deals with permissions a little bit differently. Some of them prompt you at runtime, do you want to access, if you think about IOS if you have an iPhone, allow access to the location, right, that's a runtime permission.

On Android, as you see in this slide, when you install an application, you get a list of permissions that once you've decided to install the application that application has access to all of those.

Now, there's lots of discussion of what is the value of permissions, do users understand permissions, what's being presented to them. There's various aspects and dimensions to this discussion. There are some great things that come out of permissions from just sort of a research side. They allow researchers to hone in onto which applications are potentially dangerous.

If an application doesn't have the ability to send SMS unless it has a root exploit as we've heard about in the previous panel, it's not going to be able to send that SMS message. So, this can help some investigations as well. And it helps experts become whistleblowers to find maybe sketchy applications.

When applications are ordered over the phone, it's typically signed, and so code-signing has been around for decades in the PC world. This is basically

the idea where you're going to encrypt or sign with a private key some application, and then anyone who has a public key can then verify that only you were able to sign that.

The platforms deal with this in different ways, again, some of them more centralized like IOS, where if Apple doesn't sign that application it can't run on an iPhone. Now, it's a little bit different in an Android where developers sign those different applications, and there's no centralized notion of who can decide what can run on your platform or not.

But there's different values to this model. One of the primary things that the signature model Android provides is that once you've gotten that Bank of America app and you try to upgrade to the new Bank of America app, well, that same developer is the one who's giving you the update, and so this is a valuable sort of primitive to provide.

You also hear about something called IPC, or inter-process communication. And this is just a term that we used when applications on the phone are talking to one another. And, again, this is different and varies between the different platforms. Android has the most feature-rich form of communication between apps, and there's some terminology specific to that that may or may

not come up in the discussion. These are called intent messages on Android, and they're sent to these action strings, which basically sort of addresses for the messages that are automatically resolved by the platform.

These are used for integration between the user part of applications and also the background parts of applications, and it can be used to start applications automatically. This can trigger malware, for example, malware can start when you get a new SMS message on your phone. But it's also used for these interactions between apps. And because of that, these applications can re-expose privileged API, so you have an application, it can make a phone call, and it has interfaces for other applications to work with it and interact with it. And it might re-expose that ability to make the phone call.

And, so, this can produce vulnerabilities. And, so, one of the points that I want to make here when discussing IPC is that it's not just the platform and the code that is created by the manufacturer of the operating systems, but also the developers of applications that you run that can provide and sort of cause vulnerabilities on a platform to be created.

Now, it's not just Android. I don't want to pick on Android too much, it's just that's where my research has been. But IOS also has forms of IPC. There

are URL protocol handlers that allow one application to send data to another, and there was an instance in Skype a couple of years ago where you could start a Skype call automatically.

Now, in terms of malware, we had a great discussion on malware in the first panel. I think we sort of settled the fact that, you know, malware on smartphones is just like on PCs, incentive-based and it usually boils down to some sort of monetary incentive. We're generally not going to see malware that's just designed to drain your battery, because then your phone is pretty useless.

Two main types of malware that we've sort of seen come out on Android, that which gets root access, sort of administrative access on the phone, as one of the panelists was discussing. This is the really dangerous stuff. It's hard to detect; it's hard to remove once it's on there. And, so, this is a primary thing that the platforms want to protect against.

There's also malware that works within the permission system. You install an application; it asks for the ability to send SMS message; you've granted it that access; and then it does it. All right, a lot of -- when you look at sort of the sheer number of different types of malware, a lot of it is working within the

permission system, but we are seeing some which gets root access as well.

Now, protecting that, there's efforts in sort of in the cloud, in the market. We use different dynamic and static analysis techniques, which I'll mention shortly. And then on the phone itself we can install antivirus software just as we've done on PCs. Now, a point I like to bring up here is that there is a discussion within the communities whether or not this on-phone antivirus software actually gives you a value-add, and I hope this is one of the things that we're going to get to talk a little bit more in-depth on the panel.

From the platform side, protecting against these nasty root exploits, technologies from the PC world have been migrated and adopted by the mobile platforms. Terms you might see here with respect to this one is address space layout randomization, or ASLR. The basic idea here is when you want to mount an exploit, often you have to guess where in memory are you going to jump to execute code. And if you move the pages in memory around to a different location and randomize that, it's much harder to guess, and this provides some protection.

The other type is DEP, or data execute prevention. And the idea here is that often when you want to go and execute some exploit, you've delivered

that code down to the application, it puts it in its stack, which is sort of a scratchpad for doing operations, and it executes from there. Well, there's no reason for that scratchpad to be executable, and so we've added some hardware bits to make sure that that scratchpad isn't executable, and you'll hear various terminologies like NX bit or no-execute bit. But the different architectures give it different names. You might hear XD bit, XN bit. It's all sort of the same idea of making sure that this scratchpad isn't going to be executable.

Now, when it comes to the markets and what's happening in the cloud of how we can analyze these applications, two broad sort of techniques: one is static analysis; the other is dynamic analysis. If you don't remember anything else about these techniques, remember that static analysis is going to look at an application, not run it, and it's going to figure what are all the possible things that can happen. All right, what are all the possible code paths that can execute, but not necessarily what actually will happen if there's dead code or some configuration that's not turned on, it may not do that. And, so, that's where dynamic analysis can be used to run the application and see what happens.

The limitation there, though, is it's very hard

to automatically go through and tickle all those potentially dangerous parts of an application to see what is going to happen when your users go and run them.

The last sort of topic to bring up here is this idea of jailbreaking or rooting. They've very similar sort of concepts and are often conflated with one another. You can think of them sort of the same. There's some subtle differences between, well, jailbreaking is really opening up restrictions, opening up and installing new applications. Rooting is much -- sort of a super set, more powerful, getting administrative access.

And there's a whole community out there who loves to tinker with devices and technology. And phones are an exception. And, so, they've taken these phones and for their own purposes have figured out ways of putting their own firmwares on them to get enhanced capabilities from there. And, so, it's not just bad guys trying to do this, but hobbyists as well. And, so, these hobbyists have been creating the mechanisms that some of the malware authors are going and taking.

And there's lots of different motivations for this. In the end, doing this jailbreaking and rooting, often makes the phone less secure, which is less desirable for enterprises who have their employees using

their devices. And from my perspective, at least, I think removing a lot of these motivations can, in the end, help increase the security on devices.

So, that's my crash course. Hopefully that will give you some terminology as we talk about these different topics on the panel. So, I'll give it back to Nithan.

MR. SANNAPPA: Thanks, Will. I see some confused looks in the audience, but hopefully people were able to follow along. And hopefully, you know, the panel will still be able to illuminate us as we continue the discussion.

So, Will, you know, discussed the fact that the mobile operating systems all, you know, use some kind of sandboxing, which means that the applications are limited to their own space within the device and, you know, have limits on how they can interact with other applications, as well as how they can interact with the various system resources. And one of the issues that Omar brought up on the last panel was that, you know, Android in particular, you know, makes many different APIs available to applications.

And one of the things that I want to discuss is how we create or design secure APIs. You know, what are ways in which you can create APIs so that you allow

legitimate applications to use really compelling functionality that creates great apps and great user experiences but still ensure that malicious applications can't abuse those functionalities for nefarious ends.

And, so, you know, to that end, I'd like to pose a question to Adrian, and, you know, part of how I am going about the panel is to bring up, you know, challenges that each of the platforms have had in the past and really try to discuss, you know, how they responded to those challenges and how they made changes potentially to the platform in response to, you know, things that they saw were potentially being abused.

So, Adrian, with that, can you discuss a bit about the read_logs API and Android? And for those who don't know, the read_logs API allowed applications to access a central system log on Android devices. And, you know, according to reports from researchers, a lot of apps were writing potentially sensitive information into those logs, which could then, you know, be accessed by other applications, including potentially malware.

So, Adrian, could you, you know, give a background on the reasons why Google decided to include that kind of functionality in the system and what -- the reasons and the thought processes behind eventually deprecating that API.

MR. LUDWIG: Yep, I'd be happy to do that. Before I dive into that, I want to start off by thanking you for having us here, folks in the FTC. I'm actually really excited to be here for a variety of reasons, but not least of which is I think this is the first time I've seen a panel in the mobile space that has all of the OSs at a table, well, in the same room probably, much less at the same table.

(Laughter.)

MR. LUDWIG: The panel that we saw earlier today similarly was probably one of the most impressive panels that I've seen discussing malware in terms of the range of information that was brought to bear. So, this is really, really impressive. And I think it's great to see this kind of visibility being introduced into a space that historically has been extraordinarily closed. Android has focused on openness from the beginning, and I think we've seen the other platforms, regardless of what their model looks like, also bring a lot of openness to the mobile ecosystem. So, it's very, very exciting to see that.

And we're also starting to realize that these aren't just technological problems. These are really problems that have some technology element but have policy elements and really require a lot of engagement

among all the parties. So, it's exciting to be here to be able to sort of participate in that and to build that up.

With respect to specific platform decisions, they're very, very challenging. And I think this is true no matter how open or closed you want to make your platform. You know, we've built a multitiered security model. I think William did a spectacular job of describing it. And what's interesting is I think it's very consistent across all of the platforms. Almost every one of the platforms to a T has been very successful in taking the learnings that we had from previous environments, whether it be the desktop or we actually learned an awful lot, even earlier when there weren't desktops, when we were building security models for UNIX and the server infrastructure, taking that and then building services and building platform-level security models that protect users.

For Android, that comes in the form of reviewing of applications that are submitted into Google Play, previously called Android Market. Similarly, we've extended that capability to provide integrated into the operating system the ability to use that to check applications that you might be installing, even if you're getting them from outside of Google Play.

So, we're building the knowledge using the data that's being provided in Google Play, an awareness of who the developers are, the types of applications that are being built, what are legitimate activities versus maybe not-so-legitimate-looking activities, and then applying that knowledge to applications that are being delivered through other places as well.

At the same time, we started at a platform level with the foundation of sandboxing, which is to get to Nithan's original question, where we provided a very select set of APIs that are available to developers to build their applications. And with every single one of these APIs, there's a very lengthy discussion. I was in a meeting the other day with the frameworks team, talking about a specific API that I was advocating for. And I was told every mistake we've ever made started when we provided an API.

Well, he's the frameworks team, that's what his team does, right? So, it's true, every mistake they've ever made started with providing an API. And read_logs is a very interesting example where our expectation for how it was going to be used changed. We learned from data that was introduced and we changed how we provide it to developers. Specifically, early on in the Android platform, we were very focused on making the platform

open and flexible for developers. And this was an API that was designed to allow developers to monitor the environment around their application to see where bugs might be introduced. And that's what we saw early applications using it for.

We then saw a broadening of the usage of it. One of the dominant users of it was the security community, because it gave them the ability to see what other applications were doing on the device. Well, that seemed like a good thing. Well, then we started to see instances where that visibility presented the possibility of the accidental leakage of information. And that's actually what we saw happening more recently. And as we started to see accidental leakage of information, then we made a decision to narrow down the scope of the read_logs permission to protect the user's privacy.

And, so, at this point, the API exists. It's provided to developers so that they can monitor the behavior of their own application and view that data, but they aren't given the ability to monitor or view data that's put into those logs voluntarily by other applications, because we saw application developers who just didn't realize how many other applications were looking in those logs.

MR. SANNAPPA: So, it sounds like you're saying

that this is, to some degree, a reactive process where you watch what applications are doing and make adjustments accordingly?

MR. LUDWIG: Absolutely. It's critical, and I think this is true for any platform provider, you look at what your applications do on your platform. You add new APIs; you adjust APIs that already exist. And, ultimately, security comes down to that. It comes down to looking at the data and making decisions about where to add, adjust, or course correct.

MR. SANNAPPA: Thanks. So, Michael, let me turn this to you. Do you think that there is the potential as a future operating system, I think you guys are still, to some degree, developing and getting your policies into place. Do you think that there is the potential to be more proactive in thinking about security and API design? I know that you guys have stated in your documentation that you are not going to make, for example, the telephone API available to third-party applications. Can you discuss that and the reasoning for that and potentially any tradeoffs that you see in doing that?

MR. COATES: Yeah, definitely. And, again, before I start, thank you as well. I think it would be remiss for any of us not to start with that. This is a

great opportunity to chat about these issues.

One of the benefits of where we are developing the Firefox OS now is looking at what have we learned, what have other people tried, what's gone right, what's gone wrong. Before we get into the details, one of the different things about the way we built Firefox OS, to set the stage, is it's all built from the web. It's all web technologies. So, everything you see on the home screen, your home screen, your dialer, it's all built with HTML, with JavaScript, with CSS.

And, so, what we're doing is taking a lot of the lessons we've learned over the last, you know, 10-plus years with Firefox and bringing those to the mobile device. So, we're not necessarily reinventing the wheel, but we're translating things we've learned into a new paradigm.

And on the APIs front, one of the main items we're focusing on is protecting user data, and that's, of course, not to say that anyone else is not focusing on that. But what we want to do is really look at how does a user make the decision of when to share data with applications and what do they understand when they're making that decision. And, so, we felt that one approach that's been tried is prompting users with a list of permissions at install time. And from our perspective,

that's challenging for users to understand what they're exactly agreeing to. They see -- they want to install an application; they see a large list of permissions; and, unfortunately, I think a lot of users just click okay, let's get this application running.

And, so, what we've done instead is our APIs will prompt users at runtime for sensitive data. So, if you're using an application and you're looking for restaurants in the nearby area, it would make sense that that application would say, I'd like your geo location, I'd like to know where you are. And you would, of course, most likely, say yes, that makes sense.

But at the same time, if you're playing a video game and the video game suddenly says, to go to the next level, I'd like to access your contacts, I'd like to send your mom an email, you would most likely say no. And that decision makes sense to the user. And, so, that's kind of the paradigm shift we're trying to do is for APIs that access sensitive information, geo location, camera, video, contacts, present it to the users in a way they understand so they can make informed decisions, and then let the market evolve from there.

So, that's one of the larger issues that we're looking at at this point.

MR. SANNAPPA: Okay, so, let me -- but going

back to the original question on the phone dialer --

MR. COATES: Yes, on the phone dialer.

MR. SANNAPPA: I'm not going to let you get away with it that quickly.

MR. COATES: No, so, for the phone dialer -- very good point. So, we have a notion of different permission levels for applications. Something like phone dialer would be restricted to the most privileged applications that typically are put on by the OEM. And the reason we do it that way is the phone dialer is so sensitive that if someone was to make a mistake there and you lose phone functionality you have a big problem. So, those apps are thoroughly reviewed to make sure we're doing things correctly.

Now, if an application wants to provide a phone-like functionality, we expose that to the app through something called web activities. And, so, imagine you want to make a phone call. In a different app, you would click on some sort of number; it would use the web activities technology to then populate the number into the dialer. And at that point, you are using the phone dialer built by the OEM and reviewed that we know is secure, where you can then dial the number through there. So, the technology we're using is web activities to expose those more sensitive items to other

applications.

MR. SANNAPPA: Okay, that makes sense. So, it's a trusted UI mechanism?

MR. COATES: Exactly, exactly.

MR. SANNAPPA: And, Adrian, has Google experimented with more trusted UI mechanisms in terms of being able to expose functionality without necessarily creating direct access to discern APIs?

MR. LUDWIG: Yeah, I think there are lots of interesting analogs you can draw that are nomenclature-based. I wrote down here web activities equal intents. And I think -- I believe that's actually a fairly good representation. We have different mechanisms for APIs to be accessed. So, a good example is telephony, you can send an intent to the dialer, and that would allow dialing of that phone number using the built-in phone application.

But we found that there are lots of instances where there are very valuable applications produced by third-parties that modify the dialer. Generally don't like to name specific examples, but the Facebook application was very prominent quite recently. It was an excellent example of the types of innovation that are capable when we provide APIs to those developers. It's one of the reasons that we're so excited to provide an

open platform, so you can see that kind of innovation.

MR. SANNAPPA: So, going back to this question of, you know, permissions and whether users are actually paying attention to permissions, whether this is an effective security mechanism, Will, can you give us, you know, some background in terms of what's been shown in the academic research on that question?

MR. ENCK: So, there have been a few user studies looking at sort of whether or not users comprehend whether the permissions that are provided to them, and I think the general consensus of the academic community is that general users do not -- so, they look at the permissions, and if they do, they don't necessarily understand what a permission is going to do in and of itself.

Although, I think that there is a good reason to sort of take that in a broader perspective as well into what is the actual value of these permissions. As I mentioned briefly when I was giving you the overview, one of the really sort of valuable pieces of showing the user permissions is it enables whistleblowers, right, people who are a little more experts in an area to see what an application might do and maybe investigate that a little bit further.

There was a very interesting study at a

conference earlier this year that looked at the same application in both Android and IOS, sort of looking at sort of the free versions of these applications. And they went and looked at what are the APIs, these are the APIs to sort of sensitive -- either privacy-sensitive or security-sensitive interfaces. And they found, on the whole, that the IOS applications accessed more privacy-sensitive APIs.

And the speculation you can make from that, I don't know that you have sort of causation, there's definitely correlation, is that having the permissions there gave a level of transparency that may have disincentivized the Android versions from actually using those APIs.

We're seeing those sorts of correlations again. Whether or not there's causation for that, we don't have evidence of, but I think that there are sort of second-level advantages to -- even though the users might not -- all users might not understand them.

MR. SANNAPPA: So, Michael brought up this point of, you know, what he sees as the advantages of run-time permissions compared to install-time permissions, and I note that, you know, three of the platforms up here are actually using install-time permission: Windows Phone and Blackberry. Blackberry

actually went from run-time permissions to install-time permissions.

Do you, Adrian Stone and Geir, have, you know, opinions on -- as to which is more effective? Are users -- you know, do they pay attention either way? Or are the benefits of permissions really more of the second-level benefits that Will was talking about right now?

MR. OLSEN: Want me to go?

MR. STONE: Sure, go ahead.

MR. OLSEN: First, let me thank the FTC for putting on this event and inviting Microsoft to attend. I'm happy to be here to represent Windows Phone team.

We've talked quite a bit about prompting and have quite a bit of experience from our desktop solutions and asking users are you sure.

(Laughter.)

MR. OLSEN: And we have found that it is not very effective. There's typically something we do that's a last resort, kind of it's legally required. It's not something we like to do, and the numbers that we have -- we collect regularly show that most users just basically tab through those dialogs. They want what's on the other side. I compare it to, you know, getting between a mother bear and her cubs kind of thing.

(Laughter.)

MR. OLSEN: So, we're looking at trusted UI and what Michael was talking about before as better ways of making users understand what's going on.

MR. SANNAPPA: And can you give a couple of examples from Windows Phone as to how trusted UI has --

MR. OLSEN: So, for contacts access, for example, instead of just giving access to the APIs we show a user experience that shows -- the user has to actually pick the contacts from a list.

MR. SANNAPPA: Okay, so, there's no way to automatically upload all the contacts --

MR. OLSEN: Yeah, we like to do that more progressive. We see that that's the way forward.

MR. SANNAPPA: And, Adrian Stone, any thoughts on Blackberry's transition from --

MR. STONE: Sure. You know, again, in line with my other colleagues here, definitely appreciative of all of us being able to be at one table to have a really in-depth conversation. Like Adrian over here, it's the first time I've actually had that opportunity, so thank you.

Echoing your thoughts, I mean, we've seen the same thing. Yeah, our data shows us that users will almost Pavlovian style click through things. So, you can debate the efficacy of the dialogue, if you will, without

being able to set context. And, so, you know, when we look at -- as we've, you know, reinvented our platform with Blackberry 10, you know, you bring up the change from run-time, but at the same time, we've tried to establish more context in terms of what the applications are doing, and in many ways, make it in a way to the user that is seamless.

So, when I think about, you know, sandboxing and I think about app containerization, well, with Blackberry Balance, for example, we have taken our trusted areas of the operating system, specifically for our business -- you know, business-type environments, where we've said this style of application that is accessing certain trusted APIs, we just won't allow to function there. Or we won't allow the copying of data from one application space into another. So, for example, if I'm running Facebook on my Blackberry 10, I don't have to worry about the information that is being -- that would typically be accessed for my corporate data to be accessed in the -- your user space, personal user space, versus the -- what we call the work space.

So, you know, really it's about context for us. I also think, you know, another point that Adrian made that I think is absolutely on target, which is you have to go back through and do analysis, and you have to trim

the way that you're doing things. And as we look at the threat curve over time, we'll go back through and we reevaluate, and that's exactly what we did here, because we didn't see a return that would have been expected by having it at runtime.

MR. SANNAPPA: All right, thank you.

So, Jane, turning to you for a minute, you know and both of the Adrians now have discussed --

MR. LUDWIG: Very rarely consent.

MR. STONE: It's kind of weird talking about yourself in third person.

(Laughter.)

MR. SANNAPPA: Both of the Adrians have discussed, you know, going back and, you know, putting in, you know, limitations on API access. And this was, you know, something that IOS recently did with IOS 6, there were, you know, increased limitations on access to things like the address book and the calendar database. And I think that, you know, one of the issues that we want to explore here is, you know, what can you do purely through, you know, a review mechanism of apps and what do you really need, you know, hard, you know, built-in, technical fixes for.

So, I think a lot of people, you know, expected that Apple was doing, you know, an intensive review that

would catch any, you know, potential misuse of an API. And, you know, Apple's introduction of a more robust permission system in IOS 6 seems to indicate that you guys ended up deciding that you needed a technical mechanism there to help stop these abuses. Can you discuss that a little bit and the thought process there?

MS. HORVATH: Yeah, first I want to also thank you for inviting Apple. I'm very pleased to be participating with all the other platforms.

I would say that we implement a multifaceted security system. First, we have our developer program, so in order to even put an app in the App Store you have to go through the developer program and agree to the Apple Store guidelines and the developer agreement. And in that agreement, we have certain requirements with respect to the collection of user data.

And about two years ago, we decided that we would do what we call isolate the location API, which meant that we popped up a consent box, a just-in-time notice, so at the time that the location was being collected, the user would have the idea of why the location was being collected. And we found that that was a really effective way of communicating to users. And the beauty of this is it's blind to the app. As we rolled out these permissions in IOS 6, we could do this

for contacts, calendars, reminders, and photos at just the time of access.

And the other thing that we rolled out with IOS 6 to improve the understanding of users was the purpose string. So, it doesn't just say that this app would like to access your photos, the app has the option of actually saying why they want to access your photos, so it makes it much more clear to the user. And for us, it was the beauty of the operating system. The operating system could do it without any additional coding by developers.

MR. SANNAPPA: Thanks. I think that's a really interesting point that you bring about the purpose string. And I think that, you know, Michael, Firefox OS is going to implement something similar, I believe.

And am I right that in Firefox OS, I think, Jane, you said that in IOS it's an optional string. But in Firefox OS it's actually going to be a mandatory string?

MR. COATES: Yeah, it's, again, terminology. Ours is called Data Intentions, but the exact same thing. And the idea is to strengthen that context that when you get a dialog box asking to grant access to camera or photos or what-have-you, that the developer has a chance to say why, because it can be a bit misleading if the box pops up suddenly, even if totally legit. If you don't

understand the context, that can be confusing.

And that would be -- that is a required piece of information that we use both so the user experience is strong, but also so we as the review process in the marketplace can look through and say this is the intent of what you're doing, let's see if we can help you. If you're trying to accomplish it this way, let's make sure you're doing what you actually say.

And if for some reason you're being malicious, that will also give us information that will help us track down, you say you're doing one thing, but you're clearly doing something totally different. Let's dig in here and make sure we're not letting an insecure app or a malicious app into the store.

MR. SANNAPPA: Geir, do you have any thoughts on the efficacy of, you know, these data intention strings? Do you think that that's a useful mechanism either for, you know, users to understand what an application is going to do or as a review process, especially in terms of, you know, detecting actual malware?

MR. OLSEN: It could be. I think, you know, one of the biggest threats to security where I find most security issues is often when there is inconsistency. Like inconsistency to me is kind of the root of a lot of

security issues. And inconsistency not only in -- like within the platform itself, but then across the application space. So, I think if we're looking to developers to self-declare, then, you know, I think you're going to see a varied result. There's going to be developers that are fully capable of doing that, and it's going to be very beneficial to the end-user, but then there's going to be others that are not going to be that good at it, and it's going to end up confusing users.

MR. SANNAPPA: So, you see it as really an issue of whether the developer can communicate the message appropriately to the end-user?

MR. OLSEN: I do.

MR. SANNAPPA: And, so, but, you know, with both Geir with Windows Phone and Adrian, both Adrians, with Blackberry and Android, I think that, you know, this isn't something that you've really implemented into your systems. I know that with Android if an application creates its own permission then it can, you know, provide information on what that permission would allow access to, but otherwise there's no actual data usage intention ability.

What's the reason for doing that? Is it something that you would consider putting into place? Do you think it would be useful? Anyone can go first.

MR. LUDWIG: Do you want to go first?

MR. STONE: Well, I mean, from my perspective, I think part of the real question is how do you incentivize the developers to be able to be clear and concise in their intent, and how do you make it clear for users to be able to make that choice, again, going back to this context part that we've talked a lot about.

And, so, I always use my Dad as the perfect litmus test in what I think a user would do that could go absolutely wrong. And, so, if my Dad goes and installs a flashlight app, you know, we've got five or six or 10,000 flashlight apps, how is he going to know which one to get. So, how do I go incentivize the developer who is not malicious, and I think lazy even is an incorrect term, right, it's they're as efficiently as possible trying to go produce their application and they're using all of the permissions that they have available to them.

So, how do you incentivize that developer, you know, under a well-known security concept of principle of least privilege? What's the least amount you need in order to be able to develop your application, and then how do you take it to the next step of that which tells the user this application is trusted because it's also developed with that in mind? And, so, from my perspective, and I know where we're doing a lot of

investment is trying to work with our developer community to help them to understand that if you're going to go write a flashlight app here's what the baseline behaviors of expectation should be, and here's how we expect for you to be able to communicate that to the user, and here's how we are looking not just on the device but also with the app store of being able to go communicate the behaviors of that application.

And there's a lot of things we're working on there, but, you know, whether -- you hear terms -- Brad Arkin does a great job at Adobe of talking about the gamification of Adobe's own in-house developers, right, to want to embrace and understand security. And that's one of the things that we're looking at, how do we do that type or take that type of an approach in addition to the platform protections that we're building in to incentivize developers to do the right things. And a lot of times it's purely out of ignorance, not maliciousness.

MR. LUDWIG: So, I'll take it then as well. One of the things that we focused on a lot with Android is increasing transparency to consumers about what the behavior of applications are going to be. One of the reasons that it's very important to -- for us to provide permissions prior to installation is that's the point at which the consumer is making a decision, do I want to

install this thing or not.

We like to think of this as the type of information that would be on the back of a movie when you go to rent it, right? Who is the actor? What is this movie about? What information do I have available? The key being that it's something that's trusted because it's provided by the platform.

I'm fascinated by this idea of the purpose string. It's actually something that we've discussed repeatedly within Android. I didn't realize there was a platform that was implementing it. I apologize for my ignorance on the subject. But it has all kinds of interesting complexity to it, and so I want to take the rest of the audience through some of the complexity just to give you a sense.

Android is delivered on hundreds of different devices, in hundreds of different countries, supports dozens of languages. Every string you see has to be translated. I had the great pleasure of writing one of the permission strings not too long ago, and then having six different people tell me that what I had written couldn't be translated into their language, which was on top of the fact that we went through multiple edits in order to get it to work in English.

(Laughter.)

MR. LUDWIG: And to expect that a developer could do that and then reach a global audience with their application, it's an extraordinary opportunity for that developer to learn a lot about their customer base and to learn a lot about some of the smaller countries and et cetera, et cetera, regulatory restrictions on what you say. So, it's really, really interesting what comes of increasing transparency.

That said, to take Geir's point, it could be good. And I'm really looking forward to seeing data that comes out, you know, is this an effective additional measure, the idea of knowing more about what the developer states they're going to do with data or what's going to go on in their application, that kind of transparency to us a platform provider and then subsequently to the user who's about to install an application could be incredibly valuable.

But at this point, we just don't know. So, I'm excited to see that there's somebody that's going to do some experiments for us and we'll find out whether or not that's a net positive to transparency or whether it creates complexity and confusion. I honestly am very excited to find out.

MR. SANNAPPA: Great. So, Adrian Stone, you had mentioned, you know, the idea of list privilege

principle, that every app should have the list privileges that they need to perform their functions. I think the idea behind this is that it reduces attack surface so that if another application tries to take advantage of that app, you know, there are going to be fewer possible vulnerabilities that would be exposed.

So, Geir, I want to discuss something that you tried to do in Windows Phone 7 and that perhaps didn't work because you changed it in Windows Phone 8, and that was the automatic detection of capabilities when an app was uploaded to the Windows Phone store. Can you discuss, you know, what was the purpose of trying to implement that and the challenges and why you decided to back off?

MR. OLSEN: Sure. List privilege is also one of my personal favorites as well as that, but true. I just feel like that's kind of the motivating principle behind a lot of the work that we do. And one of the things we've done on Windows Phone is not only built sandbox for third-party developers, but we also use the sandbox very heavily internally. Windows Phone 8 ships with over 100 sandboxes for different applications and experiences on the phone. So, we feel very strongly about that principle.

In Windows Phone 7, it was possible for us to

do static analysis on applications as they were ingested to our app store because they were managed -- managed code, I'm using technology terms now, but the way the language the applications were written allowed us to -- run code and analyze the apps, and we could determine which capabilities were needed. And because we could, we allowed us to kind of accurately determine exactly, which is optimal for this privilege.

On Windows Phone 8, we moved to allow different languages on native code, which makes it a lot more complicated. So, it was more of a technical challenge that we couldn't overcome rather than something we backed off of. I would like to do it now, also, but we're not really accurate enough with our detection logic at the moment to be able to pull it off.

MR. SANNAPPA: Interesting. So, generally, how often do I guess all of you meet with that challenge where you want to do something security wise but it's too difficult technically to actually pull off?

MR. STONE: Well, I'll jump in here. You know, I think Dan in his previous -- on the previous panel did kind of a great job of enumerating the costs for an attacker, and so they're always going to go -- or typically -- go to the area that provides the most amount of return for the least amount of work. And, so, there

are a lot of things as a security team that my organization will look at and come up with great ideas. And oftentimes we will get those implemented.

But then when we -- what we realize or oftentimes when we reevaluate that decision, similar to what Geir was just enumerating, you go back through and you realize, well, either the complexity of what we originally assumed was higher or is higher, therefore, attackers are not going that route and there are other areas we have to prioritize for in our development process. Or simply the threat curve doesn't exist, and the platform has matured in other ways that really is resulting in a degraded experience to users or developers or enterprise customers.

So, I think it's part of a mature secure development process that you go through, you analyze, you trim, you go back and you say, wow, this is exactly what I want to do in this iteration of software delivery, but when I go back through and I also focus on what the real world attacks are, how the threats are evolving, I'm just going to go -- I have to prioritize where the technology is not there yet or the community is not there yet.

And I think that's just a natural part of the evolutionary process, and it's something we do with every design review when we develop our -- you know, we roll

out code and develop our product, and let's do that analysis.

MR. COATES: So, I kind of want to take that question in a little bit of a different direction, talking about technical challenges. One of the things we've seen -- so, as many people know or maybe some don't, Mozilla is a nonprofit, community-based company, so to speak. And the interesting thing about that is we've seen some really technical difficulties and challenges around security, and the way we've tackled that is by reaching out to the community at large.

And we're going to do the same thing with Firefox OS, working on both exposing our marketplace via APIs so we can have security researchers analyzing the applications that are in there, looking at the permissions, looking for interesting trends or patterns that we might not be able to see, and also looking at something called the Bug Bounty program, which we started with -- we started that with Firefox, actually, in 2004. And that's a way where we invite the best and brightest community researchers for security in the world to find mistakes.

You know, we do the best we can and we do a lot of great things. What's the newest thing you're thinking about? And if you find that, bring that to us, let's

work together and fix that to make the world safer, you know, instead of other options with that.

So, the technical challenges, they're definitely there, and I think it's a matter of, you know, what sort of creative solutions do you come up with to reach the best and brightest minds to try and tackle them.

MR. SANNAPPA: Right, so, yeah, you raise a very interesting idea with the Bug Bounty program. This is something that we've seen used by a lot of companies in the web space, but not so much in mobile. And I was wondering if the rest of you can, you know, give a sense as to why you haven't thought it was appropriate in mobile or, you know, some of you may not think it's appropriate with any of your products, but if you could, you know, discuss that and, you know, the reasons for or not harnessing the power of, you know, researchers around the world. Anyone?

MR. STONE: I'll jump in. So, you know, I think the Bug Bounty programs definitely serve their purpose. And they definitely provide value. I also think there's a multitude of ways to compensate, you know, bright, like-minded individuals who are committed to improving the security of customers.

I think when you look at the mobile environment

it really -- there are some unique complexities to that equation when you talk about if the end goal is to go address a vulnerability on the platform. What are you paying for and how do you get down to that last mile in terms of securing your customers?

And, so, I think, you know, when I just look at the entire patching equation today, for, you know, from my perspective, a vulnerability that impacts, you know, Adrian's platform may very well impact my platform. A vulnerability that impacts Apple is very likely to impact mine, because unlike what we've seen in kind of the traditional desktop environment, we all share code to some extent. So, I think that's -- that's kind of one inherent challenge that a lot of us are potentially noodling over. I think the other is getting to that last mile of update delivery.

And, so when -- you know, when you make that commitment to a researcher to accept their bug, to pay their bug -- pay for their bug, you also want to honor that commitment of being able to secure the customers as a result of the bug that they reported. So, I think there are some very unique complexities when we start talking about mobile environment that aren't necessarily a one-to-one mapping in the desktop world.

MR. SANNAPPA: Thanks. Adrian Ludwig, I know

that Google especially, you know, the Chrome program has been really big on Bug Bounties and we haven't seen the same in Android. And would you echo Adrian Stone's concerns that -- you know, the thinking there?

MR. LUDWIG: I think he definitely described some differences between the desktop environment that are really significant, the intertwining of the platforms in a variety of different levels of the stack, very low in the stack, as well as much higher in the stack, especially into the web browser. So, I definitely think that's an issue. And delivery of those updates is also different from the model that was set up in the platform, on the desktop.

The one thing that I would emphasize is the desktop environment has a dependency on updates. It is in many instances the vast majority of the safety that users have for those devices. The add-on security solutions they have haven't protected them. There are no services built around those platforms to provide them with multiple levels of security. They do not have the app store or integrated solutions as part of the platform provided those additional layers of security.

So, I think in some ways the fact that we have built those additional protections into the platform, and this is across the board, gives us greater flexibility

when thinking about vulnerabilities. We have data. Is there an application currently exploiting this vulnerability? No. Do I need to urgently get a patch out right now for that, or can I make sure that no apps that do exploit it get introduced into my market?

So, those are the kinds of tradeoffs that we are able to make now that we were not able to make previously. And I've worked at multiple companies in the security space, and it's really invigorating to be in an environment now where we have data and we're making those tradeoffs based on data. So frequently the security community is driven by a fear that there could be someone who's going to exploit this, but then you have someone like Patrick in the earlier talk come up and say, yeah, but there aren't any apps that are doing it. So, maybe it's more urgent that we have a really systematic response. Maybe it's more urgent that we build broader based protections. And, so, that's a lot about how we're thinking about it.

An example of one of the things that we're doing on my team is when we find a vulnerability, don't just fix that one line of code that is a buffer overflow, which is sort of the classic operating system buffer vulnerability, but ask yourself, have we turned on ASLR? What could we do to make ASLR more robust in this

particular situation? What could we do with data? You know, is this a place for fortified source, which is another kind of protection that Android has put in place, could be employed. And we, where we can, make sure that we put two or three or four defenses in place every time we find one of those kinds of vulnerabilities.

So, that doesn't fit well into, you know, a vulnerability rewards program which ultimately is motivated at finding and patching as quickly as possible as opposed to doing it in a robust manner. That said, we talk about it quite a bit.

(Laughter.)

MR. SANNAPPA: Did you want to chime in, Geir?

MR. OLSEN: Yeah, so, we share a common kernel now with Windows and we get -- obviously Windows has a decade worth of experience handling security issues and have built tools around it and processes and infrastructures, but we're also getting tons of metrics that we use to base our decisions on.

MR. SANNAPPA: So, Adrian, you made the point that, you know, you can tackle this from, you know, including new features like ASLR or DEP. You can tackle it from, you know, actually fixing the specific buffer overflow vulnerability. Or you could tackle it from entering that -- the apps that are trying to take

advantage of this vulnerability don't get into the app store at all.

So, I think that was a good segue into discussing app review processes. And, you know, the benefits and the limitations of these processes and what exactly the platforms actually are doing to prevent the -- to prevent malware from entering into the marketplaces in the first place. So, I'd like to start with Jane, actually. This is something that, you know, I think consumers understand Apple to have been at the forefront of this and, you know, really implementing these processes to ensure that malware doesn't enter into the app store.

And there was an interesting issue in 2011 where, you know, this renowned research, Charlie Miller, was actually able to sneak some malware proof of concept app into the app store that was taking advantage of a bug in that where he was able to undermine the code-signing mechanism and, I guess, get -- you know, jailbreak the device. And, so, you know, he claims that he was doing fairly obvious things with his proof of concept app, that he was trying to download a file, trying to, you know, use function pointers and do pointer manipulation.

And, so, you know, this ended up on the app store. Charlie, I guess, later, you know, informed

Apple. They quickly took it down, banned him as a developer, and but, you know, what I want to ask is what did Apple learn from that situation in terms of, you know, potential weaknesses in the app store review process and, you know, how you recalibrated those processes and, you know, whether this is, you know, indicative that at some point, you know, a sophisticated enough attacker would be able to get through any review process.

MS. HORVATH: Well, first off, security is definitely an arms race, and we've deployed a number of things that we think protect users better through our platform and it's not just one thing over another, it's not just app review, but it's a number of different things that we have done to protect our platform. And there's seven different things that we've done.

The first is the real-world identity of each developer is determined when they apply to be a developer with the Apple developer program, their identity is actually confirmed. And that acts as a real deterrent toward submitting malicious code because if we can find you then you can be terminated from the store. As an a app developer, being removed from your distribution platform is like a product being removed Walmart, it's a pretty big stick.

The next thing is is -- once a developer applies, they're given a certificate. And that certificate allows them to submit apps. And then once the apps are submitted, we review them. We basically run each app to determine whether they run as -- they operate as they're supposed to operate and whether they have any bugs -- any obvious bugs, of course.

And then the next thing, at runtime, we have code signature checks of all executable memory pages that are made as the pages are loaded to ensure that an app has not been modified since it was installed or last updated.

And then we deploy sandboxing, as has already been discussed on the panel. And then after an app is launched in the store, we actively monitor for any threats. And any developer who maliciously tries to harm a user or an IOS device will be terminated from the app developer program.

MR. SANNAPPA: Great. So, those are, you know, the overall processes that Apple uses. And I think that, you know, one aspect of that that I find really interesting is the developer identity issue. And, you know, do the other platforms think that is a high -- you know, something that creates a high barrier of entry to malware developers? Do you guys also, you know, make

sure that you've identified every developer who is submitting apps to your stores?

MR. STONE: We work through a process to identify developers on our side. Like to your original question, do I believe it's a high barrier of entry, not necessarily. I think really, you know, kind of reframing the problem, which is how do we go and ensure that our app ecosystem is free of malware and even broaden that to take it another step, you know, based on the data that we saw, malware may not be the most prevalent -- you know, prevailing problem in the app store ecosystem. It may actually be about privacy-infringing applications. And what are those applications doing?

So, you know, in that instance, even being able to validate the identity of a developer doesn't solve that problem necessarily. So, you know, when I look at kind of our approach to app vetting, we, you know, at a high level, number one, the app vetting team is embedded within my organization for security response. And that gives us a couple of interesting options. One, when we're actually exploring vulnerabilities in the platform, we can look at how can we go protect the app store, to Adrian's earlier point, because the main vector or the main point of introduction for exploiting that vulnerability may be a newer app store. So, regardless

of who the actor is or where they come from, how do we protect customers and ensure that it doesn't get leveraged.

Two, we've also partnered externally. You know, our platform environment is pretty diverse. We do support ported Android apps on our platform. We do support native apps on our platform. We do support HTML5. So, a pretty wide and diverse, you know, area that we got to -- we've got to look at. And one of the things that we pretty quickly identified is we are not necessarily experts in Android malware. So, let's go partner externally.

And we made an announcement earlier this year around our partnership with Trend Micro. And not only did that -- again, not only did that get us mileage in terms protecting the app store from malware but also privacy concerns as well, because they do deep inspection on advertising frameworks and stuff like that. So, you know, better able to leverage that as well.

So, I think the identity is definitely one part of it. I think it's something that, you know, you look to go make sure that real people are actually submitting the apps, especially when we start talking about cutting checks at the end of the day to developers or making sure that developers can earn money. But I think that's one

part of the larger equation, and you got to walk through how you get there.

MR. SANNAPPA: So, going back to the actual, you know, static analysis, dynamic analysis, all of this stuff, you know, what are -- you know, are consumers -- consumers trust that process to be able to, you know, capture every piece of malware? Is there -- you know, we know with the most recent outbreak of malware in Google Play, which was I think called Bad News, that the malware was actually, you know, I guess, you know, changing after, you know, it had gone through the review process, that it was -- there was some kind of trigger-based mechanism where it was then, you know, downloading other code from the server.

I'm not sure exactly what the issue was, but how do you, you know, address those kinds of issues when, you know, malware authors probably know that, hey, you know, bounters are going to be running me for, you know, 24 hours, you know, the Apple app review process, you know, apps usually get out of there in two weeks. Yeah, how do you deal with the fact that there are, you know, things like code obfuscation, things like, you know, trigger-based mechanisms that can try to thwart these review processes?

MR. LUDWIG: I think I'm probably the one that

knows the most about Bad News, so the question wasn't explicitly directed at me, but I'll take this one.

I made some promises to people that I wouldn't provide statistics that were not public, but I'm going to provide one here. Bad News is a really interesting application. Functionally, the way it behaves is it is a SDK included into applications. We saw it across a number of applications, not a very large number of applications. It was downloaded by a fairly significant number of people. I think the reports -- I don't remember what the numbers were publicly, low millions numbers of people.

The behavior of the application is it display advertisements. And some of those advertisements allow you to click within that advertisement if you want to download an application. You would then install that application. And it was reported to Google that there was the possibility of some of those applications being -- misusing the SME permission, abusing SMS to commit toll fraud is one of the words that gets put out there.

We reviewed the application; we determined, based on other characteristics, not the behavior of the application, that it appeared to be a violation of Google Play's policies, and it was removed from Google Play. At no point, and including right now, has anyone said that

Google says this is malware, spyware, or malicious. I'm not saying that right now.

What I will say is we've reviewed through all of the logs that we have access to, and no means comprehensive, but they're substantial, and we have not seen a single instance of an SMS application that was abusive being downloaded through Bad News, none. And we looked at a lot.

And, so, there were reasons it was taken down from Google Play, but I don't want to lend credence to the idea that because something comes down from Google Play it is malware, it is malicious, it is bad. I read a lot of reports like that. I have a particular view of the news, I realize, but a lot of those reports do go out.

So, I just want to make clear that something coming down from Google Play, and we never -- this is probably a little bit too strong -- very rarely confirm the reason why something gets taken down from Google Play or comment on a specific developer, because, frankly, we don't know what the intention was, was it an accident, was it a mistake, we don't know. And, so, it's important for us to be able to retain the ability to have a conversation with the developers of the applications to make sure that there's an understanding of what it was

that was going on.

So, specifically to the question of, you know, what are the types of things that we do, verifying the identity of the developer is an important first step in the process, right. In order to upload an application to Google Play, you need to have a valid credit card; you need to create a developer account; then you can begin to upload applications.

So, that is an identity verification process. It's a fairly robust one. Needless to say, every identity verification process has mistakes and flaws that get made. Creation of fake IDs for state governments in order to get into bars is a long established pastime, right?

(Laughter.)

MR. LUDWIG: So, no matter how much your robust your identity verification process is, there are going to be mistakes that are made. And, so, it's absolutely critical to have additional reviews that happen after the fact. It's absolutely critical to maintain good relationships with the research community that's looking at those applications, that can provide insight into what it is that they're seeing, that can give you an early alert on an application that maybe was going to become bad, even it hadn't yet, and even if we hadn't been able

to see that yet. So, there are a lot of those kinds of things that we do.

It comes down to identification; it comes down to a static review of applications; it comes down to looking for patterns of behavior between different developers, between different applications, when are they signing on, do they normally sign on at that time. There are a lot of different complexities. I won't go into the specifics, but absolutely it's the case that every single day we're learning something new and adding new capabilities into our automated systems to make sure that we can, you know, really find what at this point are like quarter-needles in a haystack.

MR. STONE: Well, and I think Adrian's point there's two key things, right, that we need to look at as a community, which is, one, intent, you know, what was the intent of that application when it's moved into your store. And that's extremely hard to determine. So, you know, I echo Adrian's statements about really working with the developer to try and understand that intent. I think at the same time, you know, that we have to also work when we believe that the intent is non-malicious but potentially can have negative consequences to the user or negative impacts to the user. We need to respond to that.

And we, also, to, you know, to varying degrees across the panel need to also be able to clearly communicate that back to our user community once we have enough understanding. And that's, you know, that was one of the reasons in the last year we launched our privacy notification service. You know, we -- again, the previous panel before, the question, what is malware, what constitutes malware, you saw a wide variety of answers, but, you know, again, the data doesn't show what I think we see or hear in the news, and at the same time, when we refocus on privacy, that's the area that I'm very concerned about, right, and non-malicious apps that have privacy-infringing implications through non-malicious intent. And, so with the privacy notification service that we launched earlier this year, when we identified an application as potentially far-reaching from a privacy concern, we do reach out to the developer, we do initiate a dialogue with the developer.

When we believe we have a solid understanding of what that application's intent is as well as its behavior, we then publish a comprehensive document to help communicate that out to our user community. So, that's, you know, intent and understanding of that behavior and maintaining that relationship both with the developers as well as the security community is

invaluable there. Cuts through the flood.

MR. SANNAPPA: Geir?

MR. OLSEN: And, so, we do some other things. We have a sign-up process for vetting the developers. We scan the apps with all major anti-malware engines. But we're, frankly, not finding much malware. So, we -- and I would also say that our number one goal for securing Windows Phone is end-user safety and privacy. Number two is earning developer trust, so we also try as much as we can to respect developers and their IP, intellectual property. So, when something is suspicious, we don't automatically yank the application from the store. We do typically reach out to the developer and that typically resolves the situation.

MR. SANNAPPA: So, we've touched a little bit on, you know, some of the limitations of review processes. And, you know, one big question is scalability. When we have, you know, 700,000, 800,000 apps in a market, are you -- I mean, that must be an intense, you know, computing resource and, you know, human resource in order to actually, you know, scan and review all of those apps. Can you, you know, talk a little bit about that, about those challenges and whether you think that, you know, this is something that's really scalable?

MR. OLSEN: Well, one data point is that, you know, the majority of the apps are not downloaded ever. The majority of the apps in the store are not ever downloaded.

MR. LUDWIG: That's not true for us.

MR. OLSEN: In any significant numbers. The vast --

MR. LUDWIG: It might be just the AP companies.

MR. OLSEN: There is about 500 to 1,000 apps that are downloaded a lot. So, that's another data point that allows us to invest our resources where we think is most important.

MR. SANNAPPA: Okay, so that's actually something that you use to say, hey, you know, this app is getting a lot of traction, we should probably look into it a little bit more carefully.

MR. OLSEN: Mm-hmm.

MR. LUDWIG: Yeah, I mean, I'll answer the scale question. Google is about scale ultimately. The ability to read basically all information that's ever been written, parse it, make it accessible, make it open, make it available worldwide in whatever language you want translated, that's a hard problem. Looking at a million applications and trying to get a sense for what they do and whether or not it's within the bounds of normalcy,

that’s -- I mean, I don’t want to dismiss it, but that’s not a hard problem in the scale of things that Google worries about in terms of processing information.

That said, you know, we have over 300 security engineers within Google that are focused on security and countless people who are not in a security role but that are in some kind of anti-abuse, anti-spam, anti-phishing kind of role, where they’re looking to understand what kind of social engineering is going on and then do -- make sure that there’s policy complaints. And what’s interesting from my perspective is that this didn’t come out of -- you know, the review of applications didn’t actually come from the Android team.

We kind of knew it was necessary, but it turns out we already had a team that had taken it upon themselves to protect the entire world from the Internet in the form of safe browsing, which is a product that we make available for free. It’s an API, that there are a number of browsers that use it, Mozilla uses it inside of Firefox, we use it inside of Chrome. There are actually a number of other devices that use it integrated into their platforms to protect users, because it’s the kind of thing that Google does, right? Put our computing resources to bear to then protect users across the entire Web.

And that's really how we think about Android security is in the context of all of the ways that people want to access information, making sure that it's safe. So, it's not just about Android and us protecting this platform. It's about whether they're connecting to a Google service or connecting to something on the Web, making sure that there's confidence and safety and they're just not afraid and they don't have a reason to be afraid. So, that's really how we came to think about it and how we came to focus on it inside of Android.

MR. COATES: So, you may be thinking to yourself for a company that's not as large as Google what are we going to be doing to tackle a very similar issue. And, so, I just want to throw a few thoughts out here as we're kind of wrapping up. We're tackling this in the way that we've tackled a lot of things, and whether or not you know it, Firefox is actually almost half developed by community people around the world, just volunteers that like the mission, you know, are smart individuals and want to contribute.

And we're going to take that same thing for mobile. We're going to have them as part of the review group. It's going to be review-driven through the community, just like we did for add-ons for Firefox. And, so, that combined with, you know, static analysis

for quality, making sure apps function, but also reaching out to the community, we think, is going to be, you know, a different way of looking at that problem, but one that's been very successful for our organization in the past.

MR. SANNAPPA: Great. So, you just mentioned, you know, static review to see whether apps function, and that's, I think, an interesting question as to, you know, what -- to what extent does content review in itself decrease the threat of malware. Is it, you know, possible that malware authors, you know, aren't creating sophisticated apps and that's why, you know, they wouldn't get through Apple's review process, for example. And maybe I'll, you know, throw this to Jane.

MS. HORVATH: I'm not exactly sure I understand the question. Are you saying that they don't get through the process because we actually run every app that comes in to app review and that would be a deterrent to submitting malware because malware is generally simplistic? Is that the question?

MR. SANNAPPA: Well, I mean, I think that people generally understand, you know, Apple's app review process to include some kind of a content review in terms of, you know, keeping apps at some standard of quality. And, you know, is that a contributing factor in, you

know, decreasing the potential for malware because, you know, malware authors may not be invested in creating high quality apps?

MS. HORVATH: I'm not certain I can answer that. I think that, you know, holistically speaking the entire -- all the processes that we put in place help to deter malware on the device and on the platform.

MR. ENCK: So, I just wanted to add the -- sort of the scalability discussion, and I think your point about right now malware being very simple I think helps scale the identification of the malware, but as the malware becomes more tricky or as it's trying to use different obfuscation techniques, polymorphism, very, very delayed sort of execution and logic bugs, the types of technological sort of analysis techniques need to become much more deeper and they become much less precise than accurate.

And then scaling up those approaches where you can throw a bunch of computation at it becomes limited to some extent where you do still need to throw a number of actual human analysts at this problem to identify the new sort of issues, and so there is scalability in sort of different aspects of how this is going to evolve.

MR. SANNAPPA: So, one thing that we haven't touched on yet is, you know, Apple really, you know,

created this model of a single app store in which, you know, you only get apps from one source and Blackberry and Microsoft have built -- moved in that direction with, you know, Blackberry 10 and with Windows Phone, you can now only access apps from a single destination. Can you, you know, explain, Adrian and Geir, the reasoning for that, whether it was really related to security benefits or, you know, whether there were other considerations like, you know, usability and, you know, ease of distribution for app developers?

MR. OLSEN: I would say not only have we moved in that direction, that's where we are. So, and I think it was all of the above. We saw that as a way to improve discoverability of apps for users and then a simple way for developers to reach a large market. And it has definite security benefits.

MR. STONE: Well, from our side, I mean, it's easy for me to point to what Geir said and say "what he said," but I would also build on top of that. You know, yes, we do now, you know, have a curated app store that is -- we expect to be the central distribution point for apps in our ecosystem. At the same time, and, again, the previous panel touched on it, so I'm going to bring up the term again, you know, when we look at situations like jailbreaking and the unintended consequences of

jailbreaking a device, a lot of times users want to have to some degree a greater choice in terms of their user experience or the apps they want to install.

So, you know, one of the things that we did was we've provided a mechanism today where users could side load apps to their device. Now, they have to make willful and conscious decisions. They have enter in a secure password that puts the device into that state. The device has to be tethered.

So, my point in all of this is about reducing the threat. Yes, we want a -- you know, a very refined positive customer experience with all of our apps. We recognize at the same time that especially the developer community needs a little bit more access or a little bit more capability or even to some extent individuals would like greater opportunity in their device, so how do we -- how do we segment the risk that that could potentially present from an app perspective, and so we've created the -- you know, what we believe is a safe mechanism for side loading of applications in that way.

So, it's just one of the ways that we can help try and minimize risk while still at the same time giving users a safe option.

MR. SANNAPPA: Great. So, I think our time is up, but if you guys are willing to bear with me, I think

we're hitting on an interesting discussion right now. And, so, you know, with IOS and Mac OSX, you guys have instituted two different types of security mechanisms there. In IOS, obviously, you can only get the, you know, apps from the app store; whereas in Mac OSX it seems like you can choose -- the user can choose whether to only get stuff from the Mac app store or to allow downloads from other sources. And can you give us a sense as to Apple's reasoning for making that distinction? Is it something about mobile that you think, you know, creates a greater risk?

MS. HORVATH: No, we've -- IOS is based on our experience in developing the Mac operating system, and the Mac operating systems actually comes with Gatekeeper, that similar to what Adrian was describing on Blackberry, it in a sense allows users to determine -- the default in Gatekeeper is that you can download apps that either have a developer certificate or come from the Mac App Store.

We do have an app store on our Mac now. And that's the default, but if you try to download an app that does not fall within that range, then the user will be prompted, and the user has to override Gatekeeper. You can also set Gatekeeper up to the most secure mechanism, which is to allow only apps to be downloaded from the Mac app store; or you can turn Gatekeeper off

altogether.

MR. SANNAPPA: So, do you see a reason for making a distinction between mobile and desktop in terms of the flexibility given to the user? You know, and vis-a-vis Android where, you know, it's a similar mechanism, I think, Adrian, right, where you have to check a box to say "allow downloads from unknown sources?"

MS. HORVATH: I can't comment on that. It's just the two different mechanisms that we have.

MR. SANNAPPA: Adrian, do you think that, you know, having that setting there in Android gives enough protection? We've heard a lot from the previous panel about how, you know, a lot of the malware is coming from third-party app stores.

MR. LUDWIG: Yeah, it was interesting listening for the last minute or two. I heard the word curation. What I didn't hear was choice. What I didn't hear was the idea that the user should be the one that gets to decide which things they want to consume and where they want to consume them from.

And, ultimately, I think one of the basic principles that Google espouses is that the user should have a choice, that the reason you make information open and accessible is so people can go out and find the things they want. And we view applications as something

like that.

There are many instances where a single provider won't be comfortable with a particular application that lots of people want. And, so, we did not want Google to be in a position where it could impede users from having those kinds of choices. Which ultimately is what closed markets do, and a review process that involves curation of those applications is they prevent users from having that kind of choice.

So, we focused on transparency. We focused on providing users with information about what those applications are going to do. And, so, that's the direction that we've taken.

MR. SANNAPPA: All right. Well, that was an interesting point to end on. I have a ton of other questions that I wasn't able to get to, but I think we had a really interesting discussion and I want to thank all of you again for participating. It was great to have such a wide variety of perspectives and to have, you know, all the major platforms participate today. So, thank you.

(Applause.)

(Whereupon, a lunch recess was taken.)

SPEAKER, MARKUS JAKOBSSON

MR. OHM: Hi, everyone. Welcome back. My name is Paul Ohm. I'm a Senior Policy Advisor here at the FTC. I will be moderating the third panel. I hope you all had a nice lunch. We are such great hosts, I hope you enjoyed the full banquet that we provided.

(Laughter.)

MR. OHM: And my panel will start in a few minutes, but it's my honor, in the meantime, we thought it would be nice after lunch to invite someone who's been around the field and has thought a lot about it, and who can reflect on not only what has happened in the morning but hopefully set up and engage the discussion for the rest of the day.

We think we found the perfect person for this, Dr. Markus Jakobsson. You'll notice that we kind of have a mixture of academic types, people who work for big companies, people who have started small companies. Well, Markus, in one human being, encompasses all three of those. A former professor in computer science at Indiana, is now both at PayPal as a principal scientist and is also the CTO and co-founder of a company called Fatskunk. I just like the name Fatskunk.

And Markus, in many ways, has had already a long and illustrious career thinking about security and

privacy issues across different technologies and is all-consumed these days thinking about them in the mobile sphere. So, please join me in welcoming Dr. Jakobsson.

(Applause.)

DR. JAKOBSSON: I'm not quite sure how to operate the Windows product. Can anybody help me start this?

(Laughter.)

DR. JAKOBSSON: So, the name Fatskunk suggests how difficult it has become to get the domain name these days.

(Laughter.)

DR. JAKOBSSON: Also, it is about to, you know, it's about making it memorable, so those are the two goals here. But that's not the goal of my talk. I'm going to speak about what I see the threat view of -- in terms of mobile devices, with an emphasis on malware, but not a sole emphasis, because things flow into each other, as you know.

So, first of all, the question is is malware the same as mobile malware. And for a long time, people did not acknowledge a difference, and consumers, of course, didn't acknowledge that there was such a thing as mobile malware. They argued that a phone is a not a computer, whereas computer scientists said a phone is a

computer, nothing but a computer. And it turns out both are wrong, of course.

A phone, in the context of threats like this, is not just a computer. It has a more restricted user interface. For example, it's harder to type long passwords. It has a screen that is such a precious thing that we allow scrolling away URL and address bars, which of course means that it's harder for the consumers who do care about, not that there are so many, who want to see where are they actually going. It's harder for them because I can scroll off -- I can have an app or web app that is a vicious one that it scrolls off the address bar and then it could even replace in the content portion and say Bank of America, whatever you want, and it makes it much harder for the end-user to know where they are and why.

Those are not the only ways in which malware and mobile malware are different, of course, but there are also limitations on power, for example. With a small battery, you cannot compute all the time. With restrictions on how to patch in a particular (inaudible) patch, you can't expect for things to be fixed quickly. And, so, we're facing an entirely different situation. And this doesn't even take into consideration how people -- how people use these devices in a different way. And

I'm going to touch on those things.

But first I want to talk a little bit of what I think the problem is. And this is something we often forget. I want to talk about who is attacking whom, how, and why. And without that background, it's very hard to talk about things in a meaningful way, I argue.

So, these are the three threats as I see them: root kits, jailbreaks, and trojans. And I'm going to argue that these are not at all the same, and we cannot group them into one bunch. So, first of all, root kits and trojans, they attack users, whereas jailbreaks typically attack service providers. The service provider, for example, being a content provider, a jailbreak could make tethering, that is against terms of service, possible for the end-user. It could allow access to apps that are not desirable by the carrier; or maybe that aren't desirable by the end-user, just that they don't know it.

They are different in terms of how they get in there. Root kits and jailbreaks, of course, they rely on privilege escalation, in other words, technical vulnerabilities; whereas trojans, it's based on user actions. And it's about social engineering, and it's about things in the marketplace. Now, that doesn't mean, of course, that you can't have root kits and jailbreaks

that start out using social engineering, but that's not the sole way of getting on the device.

And there's also a big difference in terms of why. Root kits do it for the money or for espionage, depending on who is being attacked. Jailbreaks, that's about control and piracy. It's the user who wishes to control his or her device, typically his, I think, and who wishes to use it for things that are not acceptable by the content providers. And trojans, the main reason is snooping, getting access to information.

And really the worst case there is to get access to SMSs, at least in the context of financial service providers, that is the worst case, since they often rely on SMSs for second-factor authentication. So, anybody who could subscribe to SMS events can therefore read those and use it in order to get access to an account.

So, I argue these are very different animals, and if we treat them as the same, we're doing ourselves a big disfavor. And, in particular, if we group in other things, like phishing and Nigerian scams and things like that and call it threats under the very same umbrella, then we become less credible and we confuse the issues to those who need to know what they're about.

So, I'd like to make sure that we're very

honest about what are the threats we're speaking about, not to say that one is more important than the other, just to distinguish them from each other and make sure that we all understand what are the threats that are being addressed.

So, now, a few more words about whom are being attacked. In some cases, just anybody. In the context of click fraud, for example, it does not matter to the attacker who the victim is, or at least who the person whose device is infected. That is not necessarily the victim, but it's the advertiser, of course, in that case. A second possible target is anybody with financial access. So, it doesn't matter whether it's you or it's me, as long as its access -- you or I have access to a financial service provider and have some reasonable amount of money in the account, the attacker couldn't care less.

Then there are people with access to a particular resource. So, for example, if you are familiar with the case in which RSA was attacked some time ago by not just malware but by people gaining access through social engineering, they wanted access to servers at RSA in order to gain access to information held by these servers. And, so, there, of course, it's necessary to get to those people. And, so, this is social

engineering that is targeted. Also, you got a very targeted person. If you want a person who's got a particular kind of information or a person of interest to an organization, then it's that person, and nobody else, who is the victim.

And as the last one, an organization. If you wish to either cause money -- cause loss of money to an organization or get access to resources and information about an organization, it doesn't quite matter whom you're getting there, as long as they have the right privileges or it leads to the desired result. And, so, if we don't distinguish about whom are being attacked, again, we're forgetting something important here. So, these are all considerations that are worthwhile in some contexts.

Now, I'd also argue that if you can understand what's happening, you can predict what is going to happen onwards. So, and this is not only from the perspective of what the costs are and what the technical difficulties are in order to implement a particular attack; it's also, at least when it comes to social engineering, about just how gullible are people in the context of a particular attack and how easy it is going to get in there. And you could think of that last thing as not their peak abilities but their average abilities to avoid being

attacked. And if that is rather low, then you've got a good opportunity; whereas if it's much higher, of course, there's less of an opportunity.

So, understanding the social vulnerability is also helpful in order to understand where are the attackers going to go. The attackers are going to go where it's most green. And, so, if you could identify the place that is most green, whether it's the easiest, the most desirable from a financial payoff point of view, or the way in which they're most difficult to be booted out, those are the ways in which we could classify areas as being more green than others.

So, it's important for us if we want to predict what's going to happen next to understand from the perspective of all of these aspects that I've described where is it desirable for the attacker to go, to put ourselves in the shoes of the attacker and say, here's where I would have gone. And if we don't, we address the wrong problem.

Now, one particular entity that is often forgotten is the end-user, at least among technical people, and there are many technical people in this room. They think of malware as something that is strictly technical and it doesn't have anything to do with the end-user. And that's absurd. If we don't take the end-

user into consideration, we're missing one incredibly important part of the picture.

And, so, this is a graph that you could imagine is the propagation graph of malware. It isn't, it turns out; this is a propagation of a human-borne virus. And the reason I took this is that we know much more about human-borne viruses than we know about computer viruses, in spite of the fact that it should be so easy for us to measure malware. It's just very hard to get to, even when you work in a large organization that has access. And the reason is simple. Human-borne viruses don't try to hide; malware tries to hide, and it tries its best to hide, and there are lots of unintended consequences, and it's hard to understand exactly what's going on.

But, anyway, back to the user here. The user and the speed with which the user can perform actions is very important. If you on a desktop read email every morning and you have an email-borne virus and you may, as a result of reading email, activate it and have it being propagated to some of your contacts. Think Melissa, to make it simple.

Now, that is going to happen at a certain speed, whereas if you have access 24/7 to the same -- to a device, a handset now, and it's a very similar threat, but where there's 24/7 access, of course, the speed-up is

going to be dramatically different, both because you can access it more often and because the people who are receiving it from you can access it much more faster.

And this is of importance because the way the marketplace reacts to malware typically is to detect it somewhere along this ramp-up, and then it takes a while to churn out an anecdote and then to deploy it. That means that the vulnerable time from the point of view of the attacker is the ramp-up. Anybody who among the attackers can speed up ramp-up is going to be more successful, and that's one reason why handsets and mobile computing in general is more desirable to attackers, the ramp-up is faster.

Now, also, I want to make sure that we don't stick to phones only in this discussion. If we're going to predict the problem, we should also think about nonexistent but emerging platforms. For example, think Google Glass. There you truly have users who are on 24/7. Once it's in their face, I'm sorry for the pun, it is going to be much faster, right? So, we -- in order to anticipate where things are moving, not only would you have to look at the attack surface from a technical point of view and the social implications of how people use technology, but also where, socially speaking and in terms of deployment, are things headed. And that's going

to be important for us in order to predict the next step.

So, this brings me to one thing: What do people want? And there was talk about this morning about what we should do in terms of communicating with users and how we should make sure that they do the right thing. Well, this is what users want: They want one big button that says make me happy; they press it; and they get happy, really.

(Laughter.)

DR. JAKOBSSON: A few years ago, it was very common to provide user education by financial institutions, for example, where the financial institution said make sure you turn off JavaScript and don't use it. And, of course, that's a ridiculous piece of advice in a world that is dominated by JavaScript and where you can't do anything without using JavaScript.

Similarly, maybe users should not be told to turn off bluetooth and WiFi because it's an instruction that is kind of contrary to their wishes. They wish to communicate; they wish to receive information; and they don't want to switch back and forth. You know, that's a complication of their life. They want things to be transparent and automatic and safe.

And to the extent that there is a problem, they want to be able to have a day-after-pill button, so that

they say, you know, everything is fine now. And to the extent that is possible, we should try to provide that.

So, when we do communicate to the user, how do we communicate with them? This is an example of the traditional approach. Are you sure that you want to install the unsigned application named, and then the name of it, which happens to be “Click yes to proceed” in capitals. And, of course, people read “Click yes to proceed” and they click yes. Now, that’s how we deal with security.

Now, what we shouldn’t do -- instead do is just say drag the skull to the computer to install and to communicate that this is not a good thing to do and you don’t want to do this and are you really going to do it anyway, then you’re on your own. So, in order to distinguish between threats we need to, first of all, know what the threats are and, you know, the magnitude of them. And then we -- to the extent that it’s possible and meaningful to communicate it, we need to do so. And when it isn’t meaningful to communicate and we know that this is not desirable, we should simply make it impossible to reach.

Now, there are a bunch of technical approaches, and you’ve heard about many of them this morning. You could harden the device. Everybody understands how data

execution prevention and ASLR works, and you could do code signing and code obfuscation. And this is good in order to make it harder and more expensive to attack.

Filtering in the marketplace is great, and, now, that protects against some forms of attacks, but not all, of course. And, in particular, it doesn't protect against attacks that didn't show up in the marketplace. And you could filter during runtime on the device, which is the traditional antivirus approach, use signatures or behavioral approaches, which isn't the greatest on a device with limited battery power. Or you could do the same thing on the web and instead look for access to command and control centers and look at the velocity with which the things spread and so on.

Or you could audit before any sensitive event. And that's something that I believe is helpful to say you are about to enter your banking application; we're starting up SSL; now we're going to check that you have no malware. And, of course, as well, you could patch. And this is a natural thing to do, when you notice something that isn't so good, then you patch. Now, unfortunately, patching is complicated and not so affordable, and it comes with all kinds of technical complications because of the number of versions out there. So, these -- I'm not saying that one is better

than the other. They complement each other. But we should understand that these are technical approaches that we have to choose between.

Now, the question is who cares and why. First of all, we have users. They want their simple life. They don't care a lot. You have the relying parties; they want to avoid losses. Government wants to control crime. Carriers, they want to avoid losses, of course, and at the same time sell services. And OEMs, they want to be competitive and sell services.

Now, why do we rely on those most who care the least? That's a really unfortunate situation. We need to start providing security that isn't necessarily demanded before we supply it, because users don't know that they could have the security until we present it to them.

And in question of where the focus should be, you have today's threat, which I represent by this ag here, or tomorrow's threat as it could turn out. We need to look at both. If we only focus on the ag, then we are really fooling ourselves.

And, now, in order to get context for my beliefs, I'm speaking as a representative of Fatskunk, which is a software company that allows at the station on devices to determine that a device isn't infected. And

it's based on physics, so it's not based on patching or detecting code. It's just saying there is a piece of code running on the device and, therefore, since the operating system said to all routines to stop executing, this must be a bad piece of code. And, so, that is a nontraditional approach, and it could be used, for example, to determine that environments such as TrustZone are truly to be trusted, because today we're relying on code hardening and code signing and things like that, which we know are decent but aren't foolproof.

And, so, what I believe has to be done is to understand all the attacks and all the countermeasures, and then figure out how to put them in place. And that concludes my presentation. If anybody has a question, I'm very happy to answer. Thank you so much.

(Applause.)

MR. OHM: If I could have the panelists for the third panel please join us.

Thanks, Markus.

DR. JAKOBSSON: Thank you.

PANEL 3: EXTENDING SECURITY
THROUGHOUT THE MOBILE ECOSYSTEM

MR. OHM: And I should have mentioned at the outset that Markus is also participating in the fourth panel, so you'll get to ask him questions at that time as well.

All right, so, once again, my name is Paul Ohm. Thank you very much for joining us today. I've learned a ton already, and it's been a really, really interesting mix of people. Before I begin, I wanted to give you two of the ground rules that we've already talked about today.

First, please, like, find the little question cards. They're still floating around; they're still in your folder. That's one way to get a question to me as the moderator, and I'll try and do it justice. We're also getting a lot of questions through Twitter, so, hi, those of you who are doing nothing but watching a webcast all day and not doing your work. We're glad -- we're glad for your dereliction because it's been a lot of really interesting questions.

The second thing I wanted to say at the outset, which has been said before, is we don't have the time and we're not using the time to go through the long and impressive bios of everyone that we've invited. I really

do urge to you, at some point during a break, study the bios of these people. They're really impressive.

On this panel in particular we decided that you had to be named Alex or John to participate.

(Laughter.)

MR. OHM: So, when I ask questions, if I get lost, I'm just going to say "Alex," and hope that one of them has something to say about this. But I did want to briefly go over job titles: Alex Gantman, Vice President of Corporate Product Security for Qualcomm. We have John Marinho, Vice President for Cybersecurity and Technology at CTIA. And by the way, you saw Justice Scalia's snark about the CTIA last week. We can talk about that later. That made no sense.

Jon Oberheide, the Chief Technology Officer for Duo Security, but really has worn many hats in the mobile security space. And Alex Rice, Head of Product Security for Facebook.

So, here's the setup for this panel. At one point, we were going to have -- sorry, I'm pushing my notes around. At one point we were going to have what we were calling the industry panel, and this was going to be members of the many pieces of the complex mobile ecosystem that Steve Bellovin started our day with.

And, frankly, we had this rare event, this

embarrassment of riches, where many, many, many different people agreed to participate. That's a nice problem to have. And at one point we realized, well, the solution here is to break that panel into two. And a natural line seemed to be let's have one panel with all of the platform people.

The questions will basically be fairly uniform to a bunch of people who ask and answer the same questions. And then after we've absorbed and learned what they do, we're going to invite other people who represent a whole panoply of different positions in the ecosystem to make things complex, right, to take those lessons and then build on. And, so, that's what we've tried to do.

Now, that's a tough thing to do. It's a little incomplete. You'll notice we don't have a company that does nothing but builds handsets, yet we do have the CTIA, who has many of them in their membership.

And, so, what we want to do with this one is really talk about the rest of the ecosystem, put the parts in motion. And, so, that's my first question. Oh, no, actually, I take that back. John Marinho of CTIA, and by virtue of having a membership that represents two-thirds of that ecosystem, maybe more, we thought we'd invite him to spend a few minutes with a few slides

talking about kind of his reflections on the early morning. I said you should do it from your chair, but I think you need to be standing to advance the slides. And let me make sure that -- these are the right slides, right? We're good to go? Okay, great. So, John, take it away.

MR. MARINHO: Thanks, Paul, really appreciate it. And let me just make sure I know how to drive.

So, again, good afternoon, ladies and gentlemen. And my name is John Marinho. I'm with CTIA, and I'd like to first of all thank Paul, as well as the FTC, for this opportunity, because I have to say that I really enjoyed the morning. It was a great set of panels. And, in fact, the speakers have made my job a lot easier with regards to this part of the agenda.

So, I promised Paul that I'd keep the comments very brief, and, so, in the spirit of that, let me begin by first highlighting some words that kind of struck me as we listened to the panelists from this morning, because we heard words like static analysis, dynamic analysis, social engineering, polymorphic and metamorphic malware, jailbreaks, root kits, gatekeepers, app stores, curation, chips, LTE, a series of statistics about the malware infection rate in the United States, from as little as, you know, one -- one-ten thousandth or less to

something on the order of 2 percent. And, indeed, we saw and heard what the layering effect is of the mobile ecosystem, particularly as described in the layer of turtles that I really enjoyed.

But, indeed, one of the kind of interesting things when you reflect upon all of that is that we're dealing with complexity; we're dealing with a very dynamic ecosystem; we're dealing with an ecosystem that's very rich and robust; we're dealing with an industry that is acutely focused on the importance that security has to the end-user. So, that, to me, really struck me from this morning as a great story, particularly when you look at the diversity of players that we saw, again, on panel number two, when you look at that particular dialogue, as well as even before then in terms of all of the complexities of what we're dealing with.

And, so, the good news is that the industry is focused; the ecosystem is focused on doing the right thing for the end-user; and the good news is that it seems to be paying off in terms of malware infection rates. And I'll talk a little bit about that as I go through the material.

So, indeed, mobile cybersecurity is a top priority, and I think we saw that from all the speakers this morning, and I can reinforce that. At CTIA, we've

got over 250 members. We've created a cybersecurity working group. That working group has representatives from almost every element of the ecosystem, including the players that you saw on panel number two are part of the cybersecurity working group. And it promotes an open and diverse ecosystem, which has given us 150 million smartphones in the United States and growing, and growing very, very rapidly.

So, what's the key to cybersecurity? And I like to describe it as it's a team sport. Everybody has a vested interest in ensuring that cybersecurity is addressed, regardless of whether you're providing an OS, whether you're providing an application, whether you're providing the service, whether you're providing the device. Indeed, everybody has a vested interest in a highly competitive market. So, that's a very important attribute to keep in mind.

And then, indeed, there is no quick fix to cybersecurity. Often when I talk to folks up on The Hill or I talk to folks at different government agencies, they always ask me, well, isn't there a lock you can put on the door, and unfortunately there isn't, because you're really dealing with something that's much more complex than just a simple lock on a door. And I liken it to the analogy of a house in the sense that a house has many

things that are impacted by security, from the foundation to the doors, the windows, the roof, the chimney at times. And, indeed, there is no silver bullet; you have to really focus on all the different elements that impact it.

Consumer education, we heard that over and over again, and we're trying to do everything that we can through CTIA to drive consumer education. You'll find on our website everything that we recommend for consumers in terms of how to be safe online with their smartphone. We've published a series of cyber safety tips. Some of that material we actually brought along with us and is available on the table outside the meeting room. But, indeed, it is a focus because you can't dictate or mandate that people have to put locks on their door, even though it's a good idea. So, at the end of the day, again, consumer education is important because, again, it's a team sport, everybody has a role to play, including the consumer.

And, lastly, I always like to bring up privacy, just because they're not diametric, cybersecurity and privacy, because I like to describe it that privacy is about what data you protect and cybersecurity is about how you protect that data. And, so, the two have to work hand in hand. And, indeed, it supports the whole notion

of the ecosystem, how the ecosystem has to work collaboratively when it comes to privacy.

So, this particular chart, there's going to be a test on this later in the afternoon, but, indeed, what I try to do here is to kind of really highlight how the consumer is really at the center of our discussion when it comes to the ecosystem. Because they're individuals, they're professionals, when they work with an enterprise, they could also work for the government. But, indeed, they're at the center of the entire discussion, but there are a lot of different players in the ecosystem that touch the device, from the application to, let's say, the aggregators, to the application marketplace.

I won't bore you with the details, because we heard a lot about that earlier today, but, indeed, that's why it's so important for the ecosystem to come together and to look at what are all the different things that each player needs to do so that you can deliver on the promise of security and in some sense maintain the integrity of that house that I described earlier.

So, what does that all mean? What it means is is that the U.S. has one of the lowest smartphone malware infection rates in the world, and I have to thank the previous speakers, because they made my point for me. But, indeed, just to compare and contrast these numbers,

and this is based upon industry reports that we scanned on the order of about 16 reports from companies like Symantec, TrendMicro, NQ Mobile was one of the reports.

And they're amazingly consistent when you look across all those different reports, and this was a study that we did late last year, but what you find is is that in countries like Russia and China malware infection rates are in excess of 40 percent. I'll repeat that: excess of 40 percent. When it comes to China, that's a really big number. That's on the order of over 100 million smartphones that are infected with malware. And these are based upon numbers at the end of the first quarter. Whereas in the U.S., again we heard from Patrick Traynor and we heard from NQ Mobile, and the number is dramatically lower. And, indeed, we have some indications that the numbers are even getting better in the first quarter of 2013.

So, at the end of the day, when we look at all these different studies, what we find is is that there are two things that really drive that, which is that, indeed, the industry in the U.S. in particular has standards and practices that they follow. There are a wealth of standards, we heard about a lot of them earlier today, but, again, it's a wealth of standards that are actually being implemented.

And the second element is curated app stores. The previous panel talked a great deal about that. They're curated in different methods. They are curated by different business models and approach to the marketplace, but at the end of the day, when you look at the research, it basically says that, indeed, within the U.S., the app stores are curated and then outside the U.S. that's not necessarily the case. And we see that in the numbers that I mentioned earlier.

So, at the end of the day, what I'd like to bring up is the fact that there are a wealth of security solutions across the mobile ecosystem, but that doesn't mean to say that we're done, because we're not. And, in fact, if you go to our website, what you will find is material that talks about what are the solutions that the industry has available today, but you'll also find a blueprint in terms of what are we looking at in the future, what are the things that we're targeting because we're trying to stay ahead of the threat, we're trying to stay ahead of the bad guys. That's part of our effort and why we do a great deal of research.

And then, lastly, we also look at mobility in terms of how it fits into the bigger trends of the Internet, because you can't look at mobility in isolation because, as one speaker said earlier today, you know,

there is no distinction between the mobile web and the web, they're one and the same.

So, again, I'd welcome that you visit our website. In the supplementary information and my material, I highlight some of that, as well as the URLs in which you can try and track down that information. And you're also free to, you know, contact me if you have any trouble in getting that information.

So, with that, Paul, I'll turn it back to you. Thank you.

MR. OHM: Can you flip back two slides?

MR. MARINHO: Sure.

MR. OHM: I think this is a good backdrop for the first question. With the setup in this room, the only people who can't see the slides are those of us on stage, but suffice it to say it's a complicated map of the ecosystem. If all you knew about mobile security was what you learned in the last panel, you would think it begins and ends with the platform, the operating system developer, in the case of some of these platforms, integrated companies that do more than one thing in this ecosystem map.

But, indeed, there are lots of other players. And, so, the first question, and I'll start with you, Alex, is what do other individual parts of this very

complicated graph -- what are their obligations with regard to security and what are some examples of what they've done? And, you know, the more specific you can be. And in your case in particular, I think of you as like the biggest turtle at the bottom, right, perhaps? Or is it the smallest at the top? Maybe we could have had someone who mines silicon for a living talk about that. But other than that, right, you're where it kind of begins. What does a chipset manufacturer, what does a processor manufacturer, what do they do to ensure mobile security?

MR. GANTMAN: Absolutely. So, yeah, so on this slide where the like -- I think it's the little green box up at the top and some of the other slides were the little gray box at the bottom, so if you think about a modern mobile device and think about the processor that's on it, it's really not a single processor, it's more like, you know, a system of a dozen or so processors that are packaged under a single chip. So, you know, and the dozen processors do different things. You know, they run the operating system and the applications; they run the basement software, you know, in a sea of bluetooth, a lot of the turtles that Steve talked about.

And, you know, before even the operating system and the applications make it on there, there are, you

know, 10 million-plus lines of code and firmware that are running on it, and that's what we provide, right, this foundational piece for a lot of these mobile devices. And the job of my team is to make sure that that core component is secure, that we're properly addressing the attack surface that it presents that if we're enabling the security features that the partners downstream can use, that the OEMs and carriers and content providers and app developers can use, but also the primary focus of my team is making sure that the software and hardware that we contribute into the ecosystem is secure.

So, as others have said, you know, we do static analysis, dynamic analysis. We make sure that the modern countermeasures are enabled, like DEP and STK, and we're working on ASLR. It's the same things everybody's doing.

MR. OHM: Well, and just to make clear, I'm sure there's a lot of variance in the room on what people know. So, where is the code in particular that you're contributing? I mean, are you doing this at the kernel level? Are you doing this higher up in the stack? Are you offering STKs for end-users? All of the above?

MR. GANTMAN: Yeah, so, for the most part, so there are some drivers that go into the kernel level, but for the most part it's code that's either, you know, even below that or to the side of it that's running on the

processors that are not running sort of a traditional OS but that are still on the same system and chip.

MR. OHM: Okay. Okay, so, then, John Marinho, and I don't know if you're contractually allowed to do this with your hat on at CTIA, but I would love for you, the provider we don't have on the panel right now is someone who works just for a carrier. A lot of your prominent members are carriers, and, so, same sort of question: kind of what does the carrier see as its role in the security ecosystem? What does it do, not do? What's someone else's problem, et cetera?

MR. MARINHO: So, you know, let me begin by maybe answering the question at a high level, and then I'll try to, you know, get into the specifics. But at the end of the day, when you look across the entire mobile ecosystem, it's in everyone's interest that all of you continue to use your smartphones, right? Because, you know, that drives the ecosystem, that drives the value proposition. It drives the significance that it has for every player in the ecosystem, so it's a shared interest. It's a common objective. All the players have different roles to play, and that's why we have what I described as the cybersecurity working group where we all get together. So, the carriers are there; the OEMs are there; the platforms providers; so on and so forth.

And what we try to do there is to really look at, again, what are the nature of the threats and what are the kinds of things that are working effectively, what kind of countermeasures are working in the marketplace, and what are the threats that we need to anticipate. Now, every player, including carriers, just like you heard this morning across the different platform providers, you know, carriers have different models, they have different scales, there's small, there's large. But they all have as a priority security, so they're all trying to do everything that they can to secure the network, secure the capability that they're delivering to their consumers, but there are things that they don't have visibility to.

So, for instance, I'll give you a very clear example, and we highlight this in a lot of our white papers. A carrier may have visibility to information that traverses their network that's going to a mobile device, particularly as it relates to, you know, information that could be through an SMS or through other sources. However, if that device is tethered to a PC or it's tethered to a WiFi and now you're using the WiFi connection to go to the Internet, the carrier has no visibility to that, number one.

Number two, it's the end-user that decides what

applications are downloaded onto that device. And if they choose to jailbreak it, if the consumer chooses to download information from a suspicious website, it's really up to them. And, so, there are those elements that the carrier doesn't have visibility to, and in some sense is something that, again, there's very little that they can do. But at the end of the day, when it comes to "the" network, that's what the carrier is focused on is securing "the" network to ensure that nothing mischievous or malicious happens vis-a-vis the services that are delivered via the network.

MR. OHM: So, you couldn't have set this up better. I have a question from the audience, and I really do want to get the audience engaged. And a member of the audience asks a question exactly about the point you just made or something related, closely related, which is, you know, I'm a customer of a carrier who's one of your members, and I got the email that said, You should turn on WiFi all the time, it's going to help you with your battery life. It didn't say, oh, and it's also going to probably help us with some of our traffic management.

But the question is how does that overlay the issue, so as the carriers are encouraging users to use WiFi more often or in some cases actually building

systems that take advantage of public WiFi or open WiFi --

MR. MARINHO: Great, great question. And I'll give you -- I'll use myself as an example, just because I happen to be on one of the large four carriers that are here in the DC area. They like the color red, by the way. But what they do offer is they have a for-free security application that I can download from the carrier's store that will monitor and check on anything that's on my device.

Now, that's not to suggest that it's foolproof, because there is no system that's foolproof, regardless of whether it comes from the carrier or it comes from a security company, but at the end of the day, those things are in place and the carrier is taking those extra steps to provide those capabilities to the consumer so that, indeed, even if they are using WiFi and something malicious happens over the WiFi network, at least they have a recourse, number one.

Secondly, they're also providing advice and tips that in the eventuality that something bad does happen, this is how you recover. And there are a series of tips that CTIA has offered, as well as the individual carriers have it on their websites in terms of things like if your phone gets infected, make sure you've got

everything backed up so that you can restore it to factory settings and then restore the information from your backup being either your PC or it could be a cloud service.

But, again, my point is is that the carriers are doing everything that they can to protect their customer, but there are things that are outside of their control, number one; and number two, no system is foolproof and so you've got to be prepared for the eventuality and how to recover.

MR. OHM: Great. So, Jon Oberheide, your company actually -- and correct me if I've got this wrong -- focuses more on kind of what the topic of panel four is, two-factor authentication, and yet you're with us because you've done so much kind of analyzing just about every piece of the ecosystem. So, maybe kind of if you can take the 25,000-foot-level view of this map and talk about where you think security is happening and maybe where it isn't happening like it should, kind of reflections on what some of your copanelists have said.

MR. OBERHEIDE: I think that's a good way to frame it. I'm very good at putting on my attacker hat or my devil ears, whichever you prefer. And when I see a picture like this that's up on the slide right now, I see complexity. And complexity is the archenemy of security.

So, each of these little boxes, and I think more importantly the lines between the boxes, are sort of implicit or explicit trust relationships. They're all areas where if I'm an attacker I'm going after each of these participants in this software supply chain. I'm trying to compromise, you know, these small independent software houses that are providing the drivers for the chipsets for the devices that you're using. I'm also looking at it from a perspective of, you know, the delay that comes along with complexity.

So, if I do report a vulnerability to Google or some other mobile software provider and they have to go through this ecosystem, this chain of operators, whether it's platform provider, the OEM, a bunch of third-party developers, the carrier who's responsible for finally pushing out that over-the-air update, all I see are enormous lengths of time measured in the months and years where I have the ability to sort of cut -- I could draw a diagram that's from the attacker's perspective, which is I have an exploit, whether that's something I developed in-house myself or it's something that's been published publically.

There are some very rich jailbreak communities that will happily give away, you know, privilege escalation, other client-side exploits for free in order

to support their jailbreaking activities. I look at the path from an attacker to the end-user, and I see it's much simpler. And the time line from, you know, that attacker reaching the end-user is probably measured in hours or days, even for unsophisticated attackers, whereas the time line from a vendor like Google, who receives a report of a vulnerability and passes it through the relevant parties, eventually reaching the user's device again is measured on a much larger time scale.

And when you're talking about, you know, sort of the window of vulnerability in terms of security, the attacker in many cases in that kind of, you know, several orders of magnitude difference in those windows, the attacker will win that race every time. And I contrast that with the desktop world where we talked previously on some of the panels about, you know, very proactive companies like Google pushing out Chrome security updates in a matter of hours. And on the mobile side we're talking about months and years.

MR. OHM: So, let me follow up really quickly, because one of the things we kept hearing in panel one especially but also panel two was, you know, the importance of separating the possible and the probable, the, you know, just because it can be done doesn't mean

it isn’t going to be done, and also looking at incentive models of attackers. I didn’t hear you weaving those into the story you were telling. What do you think about that approach generally, and then how does it apply to the attack model?

MR. OBERHEIDE: I think that’s a really good point. If we bring back Dan’s sort of kill chain, where we’re talking about how they, you know, create their malware, how they get on the device, how they escalate privileges, and then how they monetize or, you know, complete their attack, you have to look at each of those stages and look at the feasability of solving some of those problems or like, you know, what -- how do we affect the conversion rates between, you know, those different stages of the attacker funnel, if you will?

And I see that, you know, yes, there’s several ways you can get on the device, whether it’s, you know, malicious mobile apps that apparently affect nobody or everybody, depending on who you’re talking to, they’re drived by exploits that no one thinks exists except for, you know, very targeted attacks against executives where, you know, these are nation states attacking high-profile individuals.

I look at the patching process as the place where we have the most macro optimization, where we

understand the problems in all aspects of mobile security. We know what they are; we've dealt with them in the desktop world. I see the most optimization and the most impact in that stage, and I think it kind of ties back to some of John's discussion, where I don't think carriers are in the security game. They're here to provide service; they're here to, you know, sell you some pretty awesome voice plans and data overages, if you happen to be in Canada like I was a few weeks ago. That's not their business, and I don't think it should be their business. I think we have fairly efficient markets.

I don't know if there's any efficient market theorists in the audience, but I think that, you know, the wealth of security companies in the desktop world and even the mobile folks who are trying to get on this game somehow are kind of hamstrung by the control that the carriers have maintained over the platform. So, you know, I think there's a big opportunity if carriers loosen that control and really open up the platform to the market so that third parties can provide these security services.

MR. OHM: I'm a big believer in the ready reply. Alex, you got --

MR. GANTMAN: Yeah, so I'm not going to reply

on behalf of the carriers, but I am going to say I think it's -- I think saying that patching is either solved or sort of a problem with a known solution is a vast oversimplification. I've yet to meet a person that really understands the depth of the patching complexity in the mobile ecosystem.

MR. MARINHO: So, I'll make a few comments, and I will say this on behalf of the carriers, because it's fair to say that the industry has invested hundreds of millions of dollars in security solutions. And, again, I think the carriers have put their money where their mouth is, but they do it for reasons that are important to them because it's important to the consumer, it's important to the subscriber.

But, again, the ecosystem has given us the wealth of diversity that we have, because there was a point in time where all telephones were painted black. But that was a long time ago, and, indeed, the marketplace has grown very dramatically. And I don't think we would have seen all of the players on the previous panel that we see today if we were still in the same paradigm. And I don't think it's reasonable to say that we're going to turn back the clock to an environment where, you know, there's one particular entity that decides how security is architected in an ecosystem like

this because it's the strength and diversity of the ecosystem that makes it very hard to attack.

And the numbers speak for themselves, because, again, if you have a single point that controls security, it's very easy for the hackers and the attackers to figure out how to target that, and most military strategists would explain that to you. And, in fact, Keith Alexander is a good person that has spoken about that particular issue on a number of occasions, so the diversity of the system is actually one of its strengths.

The carriers are doing their part. All of the different players are doing their part, because I see that every day. And, indeed, the numbers speak for themselves. So, to say that, you know, there's a problem and, you know, a solution in search of a problem isn't necessarily where I think the industry needs to be focused, because the risk of focusing on something that's not the problem is that you're diverting resources from what the industry is doing to stay ahead of the bad guys, and that's actually going to backfire and have unintended consequences.

And, so, again, we can't oversimplify this to a large extent because I think it loses sight of what the real issues are, and the real issues are, again, taking the metrics that we've seen reported and in the industry

based upon real stats that they've pulled from what they see in the wild and actually focusing on what do we need to do to keep those statistics where they are or improve upon them.

MR. OHM: So, I don't have Twitter in front of me. I'm guessing some people are saying, well, let's just talk about patching for the entire hour. I'm not going to take that bait just yet, but I do want to come back to it in a little bit. But let me make sure I finish this first round, and then we'll get back to that topic and others later.

So, Alex Rice, in many ways when I watched that last panel it was interesting because they were the platforms, talking all about everything they're doing for the app developer and then also to scrutinize the app developer. I think you bring a totally different perspective, right, the opposite perspective. You are the app developer. And not only that, I think it's probably fair to say, although I don't have statistics so I can be even more confident saying it, but your company engages probably in as vast a diversity of different approaches to app development on different platforms, in different ways, than almost any company on earth.

And, so, what does your company think about its role in security? I mean, John Marinho just said it's

everybody's business, and that's kind of the military model. So, what does Facebook think about its role when it comes to securing the apps that you're designing and deploying?

MR. RICE: I'm happy to get on a soapbox about patching if we decide to go down --

MR. OHM: Yeah, we'll talk about that later. I know you have opinions about that.

MR. RICE: For the role that I'm here for is really to represent the largish app developer. I'm not going to make any claims of the largest --

MR. OHM: I've already done that, so you don't need to. Yeah, go ahead.

MR. RICE: And I really want to try to narrow the scope here to things that an app developer cares about on mobile versus the desktop world. We could fill up several panels talking about the amount of stuff that goes into normal secure development life cycles around applications in general, but narrowing it down just to the things that are dramatically different for us on mobile versus the web.

And one of the biggest things that we struggle with as an app developer is the -- one of the primary security mechanisms that exists on these platforms out there, which is the sandboxing that exists between

applications. And Windows -- sandboxes have holes in them for whatever reason. You end up with information disclosure vulnerabilities, also called privacy vulnerabilities in our context specifically. And those are a very well understood and tackled problem on the web. We do not have a lot of information disclosure vulnerabilities on the web. We have a lot of experience dealing with enforcing the same origin policy on browsers, and I think most large websites have matured to that point. You know, there's still plenty of work to do there at the same time.

But in the mobile space, these sandboxes end up being a lot more -- slightly different, whereas when you're dealing with Facebook on a desktop, it's very common for us as the app developer to kind of cede control to any software running on the machine. We're really only protecting Facebook from other websites, other domains, but it's not something we consider. It's unfortunate, but it's not a security or a privacy vulnerability in Facebook if there is -- happens to be malware running on a desktop computer.

We spend a lot of time fighting and minimizing that because it impacts us, but it's not a vulnerability that we fix on our side, whereas when you start approaching mobile devices, there are a large number of

ways where something from Facebook can escape the sandbox, and that introduces these information disclosure vulnerabilities that I'm talking about. So, that's the first major category of issue that's different for us.

And as a -- I'm trying to find the right word here -- but also being a platform developer, platform developer on a platform on a platform, we integrate with a large number of applications within the mobile device, which means we are intentionally escaping that sandbox in order to interact with another application. And, so, the effort that we end up focusing on, when it comes to information disclosure vulnerabilities, is not just from within Facebook's application sandbox but from within all the other application sandboxes that are interacting with Facebook that the user has chosen to export the data over into. And the type of vulnerabilities they're talking about here are unintentional, almost always.

The read_logs example that a panel earlier touched on is a really good one, where it's just some application logging into the system log. The most basic type of privacy disclosure that you'd have there from Facebook's case is just a user ID, which is very -- it is the key. It's in every API call, it's in just about every page that you view when you're doing anything social, and it's very easy for any developer who's doing

some very legitimate logging or debugging or even just basic exchange in their applications to include that API key as a part of it.

So, we had -- I think I can confidently say it, we had more -- the read_logs permission was a source of more single privacy vulnerabilities in our ecosystem than any other issue. It's really great to see Google scaling that back and, like, really making that easier for developers. And to clarify, it's not just our application writing into the logs; it's any other application out there, you authorize it to interact with your Facebook data, and that developer is debugging into their logs.

And those are the type of privacy vulnerabilities that are really hard to tackle as an application developer, and you really end up depending on your relationships with the platform one step beneath you to try to help clean those up, while at the same time recognizing that that takes time, it takes a long time to deprecate an API like read_logs, and so you -- you end up really trying to guide other application developers at the same time to continue on with that.

The second piece that I want to talk about -- touch on, it's slightly different for us in this ecosystem is the social engineering piece. It's just

kind of a bit outside of the realm of application security, but we -- it was a common trend across a few of the other panels earlier where most of the action is being taken by users where as a result of something that the user wanted. And we end up being the source of a number of those schemes of what the user wants.

Let's try to pick an example. As a lot of users out there, or a large percentage of our users, who don't like the color blue, or maybe they just really like the color pink. And, so, if you go to just about any open app store and search for pink Facebook you'll find a large number of just complete clones of Facebook, except for every instance of blue is replaced with pink. The developers creating this pink Facebook are not doing it out of the goodness of their own hearts, and those applications come along with quite a few other surprises. And that doesn't quite fit the normal definition of malware.

I really liked the gentleman from Fatskunk encouraging us to really be clear what we're talking about when we refer to malware. But that is something that is not traditionally referred to as malware, but something that we at Facebook would refer to as malware and that we spend a lot of resources fighting and combating.

And I think the sheer number of things that could potentially be classified as malware is what really leads to a lot of the confusion in these talks when we're discussing malware and some people say, well, there's no malware anywhere, because there are very few, like, real root kits in traditional malware even though they already existed there, they do exist, but there are several million users who want pink Facebook and have installed pink Facebook. And those start to add up to very real numbers. And I'll leave it at that.

MR. OHM: Yeah, and I'm guessing your trademark lawyers have an opinion on that as well. I mean, a couple of the things you said, and I'm going to stick with you for a second, Alex Rice. A couple of things you said kind of talk about your relationship with the platform and you even talked about working with particular platforms.

So, one question, and I want to kind of hear other points of view on this as well, is in this complex ecosystem where we have all of these moving parts, and as Jon Oberheide said, you know, mind the arrows, pay attention to the connections between them. How does a medium/big company like Facebook decide which platforms to interact with, what the terms of those relationships should be.

Nithan helped us in the last panel by kind of -- nothing like having a visual array from open to close, is that the kind of critical factor? Or does a company like Facebook just say we're going to be everywhere all the time and do the best by security that we can depending on the platform?

MR. RICE: We go to wherever our customers are and at varying levels. We tend to get much more hands-on when it approaches the point where a very large percentage of our customers are there. So, we write our own IOS and Android applications, whereas on the slightly smaller platforms we work very closely with those platforms directly to build their own Facebook experiences into those.

There's very tight integrations with Facebook and the Windows mobile platform, but the majority of that code is written by Microsoft rather than Facebook. And, so there's a very shared relationship in the security there.

MR. OHM: Open versus closed, is that a piece of your decision-making about how you're going to implement something, whether you're going to go app versus web?

MR. RICE: The security team might have preferences on which ones are easier to -- or have fewer

headaches to deal with.

MR. OHM: Right.

MR. RICE: The company as a whole goes where the customers are.

MR. OHM: So, same question to the other members of different parts of the ecosystem, which is you want to create a new deal with Apple or with Blackberry or with one of the many Android handset providers. How do you decide, you know, which to use and which to choose, and specifically, where does security factor into that? Like is security a dominant part of that pro and con list, or is it, you know, more economics and consumers and eyeballs at the end of the day?

So, for Qualcomm with handsets, for carriers, you know, deciding which handsets to carry, depending on operating system, where does security come to that decision-making, if at all? So, it's a jump ball, whoever wants to take that.

MR. MARINHO: I'll start. And, again, on behalf of the association, which is not just the carriers, just to clarify, but, indeed, it's, as I mentioned earlier, there are standards and practices that are associated with security, just the way that there are standards and practices associated with the technology. You heard some of the speakers earlier talk about that.

Security is always part of the discussion, particularly given now that there was an Executive Order in February of this year by the President and, in fact, that's been a rallying point across 16 different sectors in working with the government on the Executive Order and in delivering the National Cybersecurity Framework in record time. Because the first draft is supposed to be done by October, I was in Pittsburgh last week, by the way, and there were 400 people that showed up for that second workshop with NIST.

So, indeed, the industry is focused, and I would cite that as examples of how important cybersecurity is across the board. And if everything goes according to plan, the Cybersecurity Framework will be done by February of next year, as required by the Executive Order and, indeed, all of the players are at the table, including the mobile industry. So, from that perspective I think, again, that's a clear focus and a clear priority, you know, on behalf of the nation relative to how this is important to the entire ecosystem and across 16 different sectors, because the threats are real. We don't dismiss at all any of the -- any of the threats and the vectors that we're seeing and the statistics that are often talked about in the press.

The reality is it's complex. The reality is

that there is no, you know, easy fix because, again, we live in a very dynamic and open marketplace, and we have to respect that, but also then keep in the context of how do we deliver security, and that is a top priority.

MR. OBERHEIDE: If I could take off my attacker hat for a little bit and put back on my application developer, you know, as a two-factor authentication company that offers authentication services on pretty much every mobile platform out there, I do have to agree with Alex that most businesses are going to follow where their users are. They're going to follow that demand.

Yes, security, especially in a two-factor service, is absolutely paramount, but we allow the customers to make decisions about, you know, what platforms they want to support. If, say, you know, you have a corporate policy that says you can only use this application on the latest version of Android that's fully patched against all known vulnerabilities, then you can define that. So, you know, giving users some control or giving enterprises some control while still covering all of your bases, especially for consumer services that, you know, if you decide not to support a platform, those users simply aren't going to use your service.

I think that's going to be common across most application providers. They probably don't see security

as their top concern. They're looking at, you know, adoption rates or just usability instead.

MR. MARINHO: If I could?

MR. OHM: Yeah, go ahead.

MR. MARINHO: Just to follow on that, at the risk of agreeing with Jon Oberheide, but, indeed, you know, you do have to follow the customer, but, indeed, you do that by making sure that you've got a variety of solutions that addresses their needs and their requirements. And to your point about the enterprise, you're absolutely right, and that's why enterprises are now employing things like mobile device management platforms that help manage policy associated with security for those devices that are used inside the enterprise, particularly in an environment where increasingly you have bring your own device into the enterprise environment for access to proprietary information, be it email or other applications.

So, again, we do have to, as an industry, keep it easy and simple for the app developers, because we want it to continue to flourish in terms of the app economy. And that's really the challenge because when you build a house you have to build security into every element in the house, from the foundation to the locks on the doors, the locks on the windows, all the way up

through, you know, everything that you're doing to do to that house to ensure that it provides a safe and secure environment, and perhaps not a perfect analogy, but it is a good analogy when you look at cybersecurity across what is a very, very complex environment.

But, again, at the end of the day, you know, we're keeping in mind all those requirements because we have to follow the customer.

MR. OHM: So, let me -- you know, the one thing we don't have on this panel, Jon Oberheide is closest to being this, and John Marinho probably has members who fit this, is we don't have the tiny app developer, right? We don't have the proverbial two people in the garage who are barely, barely focusing on their feature set, and the last thing they need to be told is security is their business, privacy is their business, legal compliance is their business.

And we often hear that this is tied to the kind of health of the innovation economy as well, right? It's a good thing, then, maybe they can forestall some of that attention. And, so, since Jon Oberheide, I'm not including your company because obviously you're a company that probably thinks a lot about security since you're trying to sell a security-related product.

So, what should we tell those small, two-people

developers in their first two months, you know, they're getting ready to drop out of Harvard because they saw the movie and this is the way to make a lot of money. Well, what do we tell them? Is security their business? Is it true that literally every member of the building of the house, is that the metaphor you just used, has to think about security? Or do some of them get a pass and then other people just have to help them like be secure enough?

MR. OBERHEIDE: I think that's the danger with -- I mean, broader than mobile, mobile adoption and cloud computing, it makes it really easy to scale service and to build an application where you can be two guys in a garage and you can develop an application, you can scale out via elastic cloud services to tens of millions, hundreds of millions of users with basically no oversight.

So, if you you know, rewind it back 10 years ago, if you had an application that was reaching 100 million users and you were protecting all their data, you would have fixed infrastructure, you would have data centers, you'd have ops teams, you'd have security teams, you'd have a very mature environment, where nowadays the fact that you can reach these populations, it's kind of a blessing and a curse. You have the ability to scale a

simple application, say, you know, Instagram, to a large number of users without the typical evolution of security practices that we used to have in place. So, suddenly you're in charge of all this very important data and privacy controls and issues, and yet you've kind of skipped a lot of sort of lessons in security along that path.

MR. RICE: Right. So, I think I can help channel a lot of the small app developers that we work with, since we do find ourselves in a position of providing advice and guidance to a larger number of these applications. And it's kind of a mixed bag, and like Jon just really hit on the core. Part of it there is that these apps do spin up to a very large scale very quickly, and you don't have the normal process of maturing your security program.

At the same time, there is a large number of shared components between these -- between these app developers. Like they're able to reach this scale that quickly because they are depending on so many platforms. And by platforms I don't mean the platforms we were talking about earlier; I'm talking about Facebook for their social platform, Amazon for their infrastructure platform, Google for their Android platform. And all of those platforms invest very heavily in providing app

developers with sound advice and guidance on how to use their platform safely.

So, the main advice that we give to developers to build securely is to follow our advice and the advice of the other platforms out there, because they really can't be expected to have secure or mature security teams that handle all of these things in parallel. But fortunately they're building on top of platforms that do have mature security teams and do provide a lot of advice and guidance to our developers.

MR. OHM: So, but you believe that you can have a lot of security in a box, basically? Like if you guys build a secure platform, you have some probably easy-to-digest documentation, user education, about how to build this secure app. You think that's going to get most of the way or a large part of the way?

Imagine a person who's never had a formal course in security, hasn't really done much reading in it, are they still --

MR. RICE: Yes. Narrowing the scope a great deal there to just talk about to our realm, if you are following the Facebook STK implementation guidelines for a normal app developer, you will end up in a very secure place with regards to the known vulnerabilities that you have to worry about.

MR. OBERHEIDE: How many hours would that take, to read it all carefully? I'm just curious. All of the security-related stuff.

MR. RICE: Well, the security-related stuff is quite straightforward in the best practices.

MR. OBERHEIDE: Okay.

MR. RICE: Especially for -- sorry, I don't mean to dodge the question there, but there's a wide range of documentation for like our photos at SDK or our logins at SDK and the amount of thought you have to put into security is very different depending on which one you're integrating.

Log-in is the one where our security documentation is the most mature, because it's the most sensitive one that we have. And it's not an insurmountable time, and it's tied right into the normal implementation guidelines. It's not like this separate thing you have to remember to go look up and run in parallel. We try to make sure the on-boarding process for a new developer is very streamlined and that people can get good advice in line with their other documentation.

If you search through our Facebook developer documentation, we don't have a large number of sections that are clearly titled "security" and "security best

practices." It is littered throughout our documentation, in line with the other documentation, which is common across most platforms. Even if you take something like Android, their documentation for building the right way is their documentation, and the right way tries to be the secure way.

And I don't mean to over -- or understate the issue, but that tends to be the practice across most large platform developers, not true across all of them, but they all are striving for that. And I think most of the platforms that have been represented and discussed on the panel here today do go out of their way to make -- to help developers build securely by default. There's been a number of examples of that today.

MR. OHM: So, this might be the same question. If so, just tell me, let's move on to something different. Steve Bellovin in his talk brought up the problem of the third-party SDKs. Problem may be the wrong word to describe it, but, you know, giving a ton of functionality to someone in a very easy-to-use format. I know that Qualcomm actually does some of this as well.

And, so, the question is how much of a part of the security problem is that, right? And we're talking, I'm sure, about different models. We have loosely organized open-source models that probably exist for a

couple months, and then the people go away to other things. And then you have company-backed ones that are really secure. So, Alex Gantman, you know, in the case of the SDKs you're pushing out, is like what Alex Rice was just saying about Facebook, that, you know, use it correctly, follow our documentation, and you'll be able to do this securely.

MR. GANTMAN: I think our case is perhaps more complex because we -- it's not that we release SDKs, right? We're really like a business-to-business business. So, what we release in a lot of cases is the actual source code, right, that the OEMs that integrate with and modify. And the reason for that is to, you know, facilitate greater innovation, customization and enable the OEMs to provide better products.

Now, with that comes a challenge in terms of addressing issues, right, addressing vulnerabilities. So, when we find a vulnerability, you know, we have to work with the OEMs to get those addressed, because we can't sort of just unilaterally fix it on our side a lot of the times. So, it's -- I wouldn't call it a problem, but it certainly sort of fits a dual-edged sword, right? It could help drive a lot of the innovation, but it prevents security challenges as well.

MR. OHM: Okay, so before we move off that kind

of development, one more question. This wasn't in my set of questions, but I've been thinking about this all day. So, I think one could have watched everything up until now and you'll conclude two things, which is jailbreaking is always bad and there's no such thing as a reliable, trustworthy third-party app store.

And I just want to like throw those two propositions out there, because I personally don't believe those, but I want to see if that's what people should walk away from. And, again a jump ball. Does anyone want to like rush to the defense of these two things?

MR. OBERHEIDE: What does jailbreaking as bad mean?

MR. OHM: That there's no --

MR. OBERHEIDE: Like when attackers do it, or?

MR. OHM: There's no reason anyone should be doing it. Let's do the strongest version: These are not the official views of the Federal Trade Commission, its staff, or Commissioners, right? I mean, is that the -- is that a message we should take from this, that if there is someone out there who's trying to help people jailbreak phones, they're probably doing a bad thing and -- or is this too big --

MR. RICE: To put a very consumer --

MR. OHM: No, I've installed my own operating systems on most of my phones, and so I'm -- this is a very personal question for me. But I'm also just wondering. Go ahead.

MR. RICE: I will put a very consumer hat on for a moment and say that the consumers who jailbreak their devices so they don't pay a $60 tethering fee are not bad or evil people. They -- that is very -- consumers, but it's hard to condemn those people and just accept that they're going to be screwed and insecure because they were trying to operate outside the constraints of their device. It's definitely something that we can lean heavily against and not recommend, but I think we would be remiss to damn all those people.

MR. OHM: Well, what about third-party app stores? And it may -- correct me if I'm wrong, I think Facebook has sometimes offered some of your apps in a kind of side-loaded sort of --

MR. RICE: We do. And, so, third-party app store is a very generic term. To give you an example of a good third-party app store, the Amazon app store is a -- that is -- I don't want to speak for Google here, but I think that's what they're going for when they give consumers open choice. I think the Amazon app store is a very good thing, and it absolutely is a third-party app

store.

That said, there are probably more bad third-party app stores than there are Amazon examples, and I won't expand on it much further than that, but that is something to keep in mind when you're -- when we're talking about this, like open is absolutely good because it enables companies like Amazon to offer their own stores, in addition to the bad that happens along with it.

MR. OHM: John Marinho?

MR. MARINHO: Yeah, just one comment that I would make on the question of third-party app stores, and the reality is is that the Internet has no geographical boundary, and the issue is oftentimes you don't know whether, you know, the app store that you're accessing, whether it's pink Facebook and that's somewhere in Russia, or whether it's Facebook within the confines of the United States. So, it's that complexity and openness of the Internet that represents a challenge, particularly when it comes to third-party app stores.

But one of the things that the mobile industry has started to do, and you see that through the efforts of some of the carriers, is is that they will actually provide, not dictate, but actually provide recommendations to consumers in terms of, you know,

applications and/or app stores that they would recommend in the sense of, you know, putting their brand behind it because, you know, again, we've got to promote the growth of the industry, and a lot of that is through app stores.

So, at the end of the day, it's a juggling act, but we have to recognize the reality of the Internet that, you know, there are no boundaries. And, again, there are app stores in other countries besides the United States.

MR. OHM: Any other thoughts on either of those?

MR. OBERHEIDE: On the jailbreaking side, I would say that from a perspective of getting vulnerabilities patched or fixed, I guess I would say in general jailbreaking your phone is not good for security, but there are certain cases where third-party ROMs are actually getting security fixes out faster than the official platform providers.

So, you take an example of public jailbreak exploit that is dropped on the Internet, and you think about the long process it takes for the platform providers and the OEMs and the carriers to get that out to users, some of the third-party ROMs, you know, they don't have to go through FCC certification, and all of these other regulations in testing. And they can push

out these -- these security patches much more aggressively. Obviously this is at the expense of potentially reliability and stability of the device, but there can be cases where using a third-party ROM does make your device more secure.

MR. OHM: So, let's -- at the very end I'll give you each like one last moment to kind of reflect, but let me ask a question about patching before we get to that moment. And I won't call on anyone, but this will be a jump ball, and I'll give you my law professor evil eye if no one's answering.

But the way I want to kind of frame it is maybe put a slightly more positive spin on it, which is assume that -- hypothetical -- assume that you want to increase the kind of frequency, reliability, speed of -- with which patches are pushed out onto telephones. The story that I've been told is that part of the problem is there's a huge coordination problem among different people on that chart. Is there one quick fix we could do to kind of lessen coordination costs, to raise incentives, to change technological barriers?

Like, what is the nature of the problem, assuming it's a problem, and if what you want to say is it's not a problem, then please feel free to say that as well. All right, how do we -- how do we make patching

happen more quickly, if that's what we want to do?

MR. GANTMAN: So, that was a lot of questions in one.

MR. OHM: Yeah, thank you. You noticed that, right? But that means you can say anything and you'll still be answering my question.

MR. GANTMAN: I can talk about anything and claim that question was buried somewhere in the middle.

Yeah, so, I think your assumption is valid, right? So, I think we do want to make it simpler to patch, all right. But I think our motivations are not necessarily sort of in line with what Jon is saying, right? There is not necessarily an urgent threat that we're trying to protect against, right? But, in general, in terms of preparing for what the future may bring, right, we want to be -- we want to have agile response capabilities, and we want -- so, we want to focus on containment and being able to respond.

It is a challenging problem, though, and sorry, there was another part of the question, which is?

MR. OHM: Well, so, help me figure out how we begin to simplify things.

MR. GANTMAN: Oh, so, yeah, so basically yes. We're not sitting sort of on the secret easy solution and just like not using it, if that -- I think that was

another part of the question. There is no easy solution that I know of that we're just sort of keeping for future use. It's a real challenge, you know, with many stakeholders, with diverging interests.

I mean, that's one of the challenges in mobile, right. Like with a PC, right, like Jon, you own that PC, right, you are the stakeholder, right, it's yours. Well, and if it's -- well, in the case of your company, it's still yours, but, you know, for those of us who work for a large enterprise, if it's a company PC, it belongs to the enterprise. There's no question as to sort of who is the ultimate owner of that PC.

With the phone being a much more intimate device, even if you have a company-issued phone, right, you have now a lot of stakeholders, right? You have the enterprise, who wants to control it; you have the user that wants to control it; you have the carrier, and if it's subsidized, they legitimately feel that there's, you know, they still have a stake in it; and then even past the contract, right, it's on their proprietary network. You have the content providers, you have the app developers, the platform vendors, and we have this -- it's a real challenge of -- you know, we call it a problem of multiple masters or mutually assured distrust in a way and figuring out how to enable the system where

you have -- you don’t have a single root of trust that we’re used to having in security, right, where it’s like, well, that one entity is responsible and everybody trusts them and they can sort of make decisions and sign updates and deploy them. We have this really interconnected system with mutually distrusting roots that, I guess, we have a big problem and we don’t necessarily have an easy solution.

MR. OHM: So, Jon Oberheide, I realize we didn’t have you talk about the slides you prepared. Do you have like -- I know you’ve studied part of the kind of patching and the empirics of it, do you have like a top-line statistic you want to share?

MR. OBERHEIDE: Yeah, one of the things that John mentioned earlier is that -- and we’ve kind of been discussing throughout the session and the event is, you know, what is the right motivation? Where are the numbers? If it is 2 percent, if it is, you know, .0001 percent, and I think that, you know, if we look at, you know, the patching problem in itself, so we did a little research funded by DARPA that kind of looked broadly at the Android ecosystem. And Android is not unique in the way its patches are distributed through these, you know, chains of different responsibilities or chains of mutual distrust, as you said. But if you can contrast that

with, you know, a model like Apple where all the updates are essentially delivered, there's only a handful of unique hardware handsets that they have to test and configure and deploy to, you can see that Android is a very difficult ecosystem to secure and deliver timely patches.

So, part of this research was to release this application called X-Ray, which will actually perform vulnerability assessment on your device, so that it will actually look for the presence of vulnerabilities, not based on the version number or any sort of magic identifiers, but by actually analyzing the software, the machine code, on your device, to see if it's patched or not. And we released this about, you know, eight months ago, and we found that about 60 percent of Android devices out there have unpatched privilege escalation vulnerabilities, which would allow an attacker to either, you know, install a malicious app or via a drive-by attack, then escalate privileges to take full control of your device.

So, whether it's, you know, .0001 percent or it's 2 percent, I know, you know, several people in the audience today could release a exploit tomorrow that leveraged one of these payloads and would compromise your mobile device if you just visited a website, a link that

they sent you. So, whether or not the problem is happening today or attackers have that expertise, I think that the delta between where we are now and where either a motivated sophisticated attacker or an unsophisticated attacker who is good at sharing code, which is definitely a quality we learned from the desktop world, I think that is a pretty short delta, and I think we have a lot of work to do until we can get to the point where, you know, we are releasing rapid updates and patching the vulnerabilities quickly.

MR. OHM: So, this is all self-selected downloads, right? So, it's not -- you're not making scientific claims about --

MR. OBERHEIDE: So, this is -- I could put the slides up later, but this is based off 60,000 runs and downloads of our X-Ray application, which, of course, has some self-selections and selection bias because it's not your grandma who's downloading this application to run it, it's the very tech-savvy folks who are likely to have, you know, later device versions and might be running, you know, custom ROMs that are patched further and then extrapolate it out using Google's public data to the entire Android population.

So, you know, if we saw that 98 percent of users running 2.3.3 are vulnerable and we know that 2.3.3

represents, you know, 50 percent of the Android population, then we can, you know, extrapolate out to that number. So, I mean, I'm not a stats major, and I wouldn't hold this up to a stats professor, but even if you just look at the pie charts of distribution that Google puts out and the numbers -- diversion numbers that are associated with those pie charts and cross reference that with what public vulnerabilities have been disclosed and exploited in the wild that affect those versions, you can see that's a significant percentage.

MR. OHM: So, Alex Rice or John Marinho, you want to jump in on this topic?

MR. RICE: Yeah, to expand on that a little bit. Going back to Alex's comment earlier of -- and I think we were talking about a slightly different scale. You were talking about all the way from the chip level up to the top.

MR. GANTMAN: Yeah, I always talk about these in first person, yeah, so I'm talking about the problems that I have.

(Laughter.)

MR. RICE: So, let's narrow it down just to like the sandbox type vulnerabilities that are traditional, like an Android vulnerability, let's say. And I don't think we're quite in a place where we should

just throw our hands up and say that patching is too hard and we shouldn't do it, because there are many examples of patching getting right. Apple is probably the clean example there, but they're also the easy example, because they have a completely integrated platform.

If you take just Android and look at the other integrated devices that are on Android, Google's own nexus devices, those are all immediately patched and back reported and have a very generous end-of-life policy. Going back to the Amazon example, also, Kindle devices also receive updates very, very quickly.

So, when we're talking about how long it takes to get a patch from vulnerability discovered to vulnerability patched, it's really not any particular device problem, it really comes down to how many chains that it has to go through, as Jon was talking about earlier. And, so, you start running into these problems where the patch approval needs to come from Google to an OEM to a carrier down to the customer.

And in most cases it's not even a time delay; it's that those lines of communication are simply broken after the device is launched. The devices that were launched six months in the U.S. are essentially end-of-life and will no longer receive security patches because those chains just simply don't exist anymore. And

maintaining those chains and keeping them in place is definitely costly and complicated, but it's also something that should be happening.

And I think it's a little -- I'm going to be a little controversial and aggressive here. I reject the premise that we should wait until there's data showing that a sufficient number of people have been exploited and harmed before we release patches for it. I think waiting until there is evidence of harm before we go and try to correct the problem is really a disservice to all of our customers and the ecosystem in general.

And that's not to say that it's an easy problem. It is absolutely a hard problem, but there are places that have got it right, and I think we should encourage more of that across the ecosystem.

MR. OHM: Anyone else?

MR. MARINHO: Sure.

MR. OHM: John Marinho?

MR. MARINHO: Yeah, I'll take a stab. So, a couple of points have been made that I will run the risk of having to disagree with. One is the suggestion that the ecosystem is waiting. It's not. Patching is a priority. Now, the question is can patching always happen faster? Sure. It can always happen faster. It can always be improved upon.

Is it a priority for the industry? Yes, it is. You'll see that not only in what we've published, you'll see that in the work that we're doing within the cybersecurity working group, and we're bringing that forward into also the work that we're doing on the National Cybersecurity Framework that was directed by the Executive Order. So, my point there is is that to suggest that it's not a priority and that it's not something that the industry is focused on I don't think is a fair representation of what the industry is doing.

And, in particular, I would say that the lines of communication are open. I know this for a fact because I work with these folks almost on a daily basis. And it's not a fair characterization because, again, I know for a fact that security, in particular, is a priority for the carriers, and they put it through an expedited process.

I'm not in a position to disclose the process, because that's proprietary to each individual carrier, but I do know for a fact that they do this every day and they do it 24/7. And that's why they have things that are called network operations centers for security, and that's why they have CISOs, and a variety of other security mechanisms in their overall structure. So, again, I have to take issue with it not being a priority

because it is.

Now, can it be improved upon? Sure, it can. But it's got to be looked at in the context of the different ecosystems that have to be supported. On panel two you saw how many ecosystems across the table? There weren't just two. Because Blackberry, Microsoft, and Apple are all different companies, they do things differently, but yet all of that has to be accommodated in order to support a competitive and diverse marketplace.

So, again, the industry is doing everything that it can, including down to the chip level in terms of the actual foundation of the house in terms of the hardware to make sure that we're not doing anything to compromise reliability or the expectation that consumers have of the service, because at the end of the day, that's what we're focused on.

MR. OHM: So, I just -- I don't want to dwell on this too much longer, but I want to make sure, I think I heard you guys talk in the past to one another, I thought Alex Rice, and either one of you, correct, was talking about technical lines of communication, like the ability to send the signal to the phone. And you were talking more informally about kind of human lines of communication. Am I right about that?

MR. RICE: Take an anecdotal example there. My fiancé bought a device nine months ago. There was an Android privilege exploit vulnerability released not shortly afterward, like three to four weeks afterwards. Google patched it in a very short period of time. She's still waiting on a security update nine months later. That's just one of many security holes, and she's in -- absolutely in that 60 percent bucket that Jon was talking about.

And in the current state of the world, she will most likely buy a new phone before she receives a security patch. And you're absolutely right in that there is no known malware in the wild that is exploiting that vulnerability, but as a --

MR. OHM: I can make it happen.

(Laughter.)

MR. MARINHO: I would advise you not to. I'm not your lawyer.

MR. OHM: Hang on, hang on. So, what I want to do, because I really do want to end this on time, we have about three minutes, is since Alex and John Marinho both want to really jump in on that, I'm going to let you speak last on this next question. It's an open-ended question and, frankly, I don't care if you just ignore me and answer what other question you want to do.

But the question is if we got the band back together in five years and we did this panel again, what would we be talking about? Would things be better, worse, different? Would we have solved all of the problems? And, again, if you don't want to answer that question, then talk about something else. But, Alex Rice, you get the --

MR. RICE: The top of my wish list in the mobile security system, I think we need better mechanisms for passing data between sandbox applications. That's coming from a platform on a platform perspective. We're actively working on that, and I think the state of the world now is much better than it was two years ago.

The second item on my wish list is I think we need to get much better about delivering prompt security updates to the entire ecosystem, which is a hard problem.

MR. OHM: Jon Oberheide?

MR. OBERHEIDE: I kind of touched on this earlier, but I think that, you know, I do think that patching is the number one problem in mobile security now, or at least has the most impact or potential impact, whichever way you want to look at it. And I think the solution is to, you know, open up the platform a little more and, you know, provide the ability for third parties to step in and provide security services and allow

carriers to kind of like brush that responsibility off their shoulders. I don't think they want it. I don't know if they're currently equipped to do it. And I think that, you know, opening it up to the market will be the most productive and efficient way forward.

MR. OHM: John Marinho?

MR. MARINHO: Well, again, at the risk of taking issue, the marketplace is open. There are lots and lots of security companies that are in the business of providing security to mobile devices. A lot of them sit on the groups that we have within the industry. So, from that perspective, again, I struggle with the issue of openness because at one point we were saying that the ecosystem is too open, but now we're advocating for openness.

But, again, putting that aside, I think if we get the band back together in five years, I think we will be surprised at how the rest of the globe has really followed the example of the United States, because it's not gone unnoticed that, again, the infection rates in the United States are where they are compared to other markets because I see that from carriers, I see that from OEMs, and, indeed, even the whole issue of curated app stores.

So, I think what we'll see in five years is,

again, how the industry has evolved to really address best practices and standards across the board, across every element of the ecosystem, including the application developers. And it will be easy to follow. We'll, I think for the most part, be surprised at how expansively the marketplace has become, again, being driven by applications and everything that we do on smartphones.

And I also predict that in five years everybody will wonder what a PC is. And, so, with that, thank you.

MR. OHM: Sure, Alex Gantman?

MR. GANTMAN: Yeah, so, all right, so I'm going to take you up on the offer and basically talk about something else.

MR. OHM: Yeah, sure.

MR. GANTMAN: But I'm -- I'm not -- in part because I don't want to be trying to predict the future, because I still remember how far like off I was five years ago in terms of predicting what would be happening now. But I also want to, you know, disagree with Jon and Alex on some of the, you know, patching everything and mitigating every vulnerability. I mean, in a way it's an approach that we -- that our community ridicules when it comes to national security, right, in the airport security theater, and it's not the approach that we take in our daily lives, right?

So, I'm guessing that our houses are full of vulnerabilities, right, we don't have bars on our windows, we don't have stone walls, we don't have moats with drawbridges. Those are undeniable vulnerabilities that are really improbable -- you know, are really unlikely to be exploited, so we don't bother patching them, right? And, you know, when I look at the mobile ecosystem now, yes, there are vulnerabilities that, you know, that have been discovered and fixed in your products, and at the same time if we look at what's the potential impact on the users if all of them were patched sort of by the end of panel today, the percentage of users that would actually experience, you know, a degradation and unwelcome behavior is going to be negligible, right, so it's not really going to impact most of the users.

So, as an industry, we're trying to look at the data and focus on things where we can sort of make the most impact. And that's not to say that patching is not an important problem to solve for. We have to have visibility to react in part because we can't predict what's going to happen five years from now. So, it is something that we're working to address, but it is especially sort of down at the lower layers. It's a very challenging problem.

Now, if I have time --

MR. OHM: Really briefly.

MR. MARINHO: So, a really brief anecdote. So, a couple of years ago, my son was asking me about my job. And, you know, I was trying to make it interesting to a 10-year-old, so I described, you know, software and malware and its vulnerabilities and exploits and trojans and viruses and all the terms that luckily we picked that sound cool for a 10-year-old.

And he had a really unexpected reaction, right? He asked me, so, with so many things that can go wrong on the Internet, should I be even using a computer, should I even go on the Internet? And it's not at all the reaction that I was hoping for. And so I was a little bit shocked, and I thought about it, and I told him, look, you know, every time you leave your house bad things can happen, right? There are actual bad people out there who will try to hurt you, you know, you can get into accidents. And I tried to explain it to a 10-year-old, right? So, there are diseases; lots of things can go wrong. But we don't stay, you know, locked up in our houses, right, because the reality is, I mean, we get much more value out of communicating with other people.

And these devices are similar. Today we get much more value out of using them than the risk -- I

mean, security is not absolute, right? It's a benefit-to-risk ratio, and these days, you know, the pace of innovation is so high that we're adding value at a much higher, you know, rate than sort -- we can't even measure the risk in some cases.

MR. OHM: So, ending on a note that is simultaneously very dark and also kind of hopeful, it's a good way to end.

MR. MARINHO: It's hopeful. It's hopeful.

MR. OHM: Please join me in thanking the panel.

(Applause.)

MR. OHM: Why don't we give you five minutes back? We're running a little behind. So, 3:20, does that sound okay? At 3:20 we'll reconvene for the last panel. Thanks.

PANEL 4: SOLUTIONS FOR CONSUMERS TO PROTECT THEMSELVES FROM MOBILE THREATS

MS. ROBBINS: All right. Well, thank you for being here for Panel 4. I know, the last panel of the day. And this panel is going to focus on passwords and authentication and also antivirus and antitheft solutions for consumers. And we have some really terrific speakers today to talk about these issues.

To my left, we have Jeff Fox, who's technology editor for Consumer Reports. And then next to him, we have Markus Jakobsson, who you have already heard from, who's the CTO of Fatskunk. And then to his left, we have Kayvan Alikhani, who's the CEO of a company called Passban.

And then to his left, we have Terry Shofner, who's the VP of sales at Yubico. And then we have Derek Halliday, who's the director of product management at Lookout. And then, finally, we have Mikko Hypponen, who is the chief research officer at F-Secure.

So, we have a really terrific panel here today. And our first speaker, Jeff Fox, is going to sort of set the stage for us and give us some statistics from Consumer Reports' State of the Net Survey.

It's really tight.

MR. FOX: Because we have got more panelists

this time.

Good afternoon -- it always helps to have the mic, yes. Good afternoon. Actually, I am kind of glad we're the last panel, because I got to hear everything that came before, and there was an awful lot of talk about malware, but I am going to say now something completely different or almost different.

As a consumer representative, we're looking at this from the consumer point of view, from the household, not studying networks and peering inside, you know, all the intercommunications. We're going at it strictly from the consumer point of view.

How do I move to the next -- just page-down? There we go. Okay.

So, we're going to look at some other threats besides malware but also malware, and we were going to pitch our number along with -- it's not zero and it's not like a gazillion people -- as to how many people have actually experienced malicious apps.

Just by way of background, some of you might be familiar with our State of the Net Survey, which we have been doing now for almost a decade. Those are some of the samples up there. A couple of years ago, this was the survey that found, for example, like millions and millions of kids on Facebook, underage kids on Facebook.

But we've been tracking malware on computers for almost ten years, since we started actually with the FTC working on this.

Our survey is nationally representative, so we project numbers in millions nationwide, very sophisticated. The same people that do our annual questionnaire do this survey.

Whoops. How did that happen? No. I hit the end button. Can you just get me back to it? Sorry. I hit the end button instead of page-down. I'll be careful which button I touch.

Okay. So, let's get into some of our findings, nationally representative findings. These are some of the areas that we looked into, malicious software, stolen and lost funds, location tracking risks -- okay, location tracking risks, I know people think of it as a privacy issue; we actually found some data where it's a security issue -- the use of insecure hotspots and how consumers are or are not securing their phones.

So, here are our numbers, and this is based on actually asking people how many times a malicious app has been installed on their phone in the past year. We gave them examples, symptoms, unauthorized calls or texts, excessive advertising, other kinds of behavior that security experts told us were the appropriate

symptoms. So, as you can see, together, this is 5.6 million consumers. I think that might be a little higher than the 2 percent, but it's in the same ballpark, but way higher than the 1/11000th of a percent.

We also looked -- we also looked -- we asked those people how the malicious software affected them. So, you can see what -- you know, what happened to them. Now, this was a very small sample size because of the low incidence. So, these percentages are percentage of the people who had malicious software, and the most common -- I think it's better to just look at which are the bigger lines and which are the smaller numbers than to get caught up in the numbers. But resetting the phone to its settings or having some sort of problems were the most common things, but there were, you know, bills, toll fraud, losing stuff on your phone. There were some examples of people being harassed or ID theft, and a small percentage of people had to deactivate their wireless account.

We also asked about what we call imposter apps, which are, I guess, repackaged apps, which are apps that are made to look like brand name apps. We asked people how many brand name apps they downloaded that then turned out to be a -- actually a malicious imposter.

And we project that 1.6 million users installed those last year, and I know some people that I've talked to are skeptical about this, but if you take a look at the app stores -- and I don't know how many -- if you can read some of the fine print on here, we visited some of the major -- these are the major app stores. These were found in major app stores, not the little ones we've been talking about all day.

This Dropbox look-alike has a little disclaimer that I encircled there. It says the application is not affiliated with Dropbox, but that little disclaimer doesn't show up unless you click "Show Details." You see, it says "Hide details" under there. But in each box, the first logo is of the original app, and then the other logos are for things that are kind of looking a lot like them. I'm not saying these are malicious, but you can see how consumers might not be able to tell the real thing from something else.

Looking at phone theft and loss -- and we just announced this yesterday -- that we projected 1.6 million smartphones were stolen last year and another 1.2 million were lost and not recovered, which is a security problem, perhaps not quite as much as a stolen phone, but if you lose your phone, you know, somebody could still get at your information.

These were some of the things that people experienced as a result of a phone theft: unauthorized access to their bank account or to their email account and permanent loss of photos, and as you see the note there, again, there was such a small number of people that we can't give numbers for these.

Then we asked the people, you know, what they were doing to protect their phone, and of all the measures that we asked about, the winner is over there on the right, which is none of the above, at 40 percent of people, and that was kind of our big news when we first ran this story. Probably the most common process, people are backing up. About one-third are backing up. And four-digit pass codes and longer pass codes together are about 36 percent, 23 and 13 on there. So, it's still the majority of people are not using pass codes. Lots of people I've spoken to since we did this story didn't even know you could use a pass code longer than four digits. When they saw the story, they said, "Oh, you can do that?" So, there's a lot of lack of consumer education here that I think there's a lot of work to cut out.

I think there's a lot of room for growth for the antivirus makers that are here. Only 15 percent right now are using antivirus, maybe because they think they

don't need it. Our survey of PC users over the last ten years show that something like in excess of 80 to 90 percent of PC users use antivirus. So, this is clearly, you know, way lower than we find on desktop computers.

A couple of other things we found. One is that the four-digit pass code is not all it's cracked up to be. A properly equipped thief can crack it in 20 minutes. Consumers -- the lack of transparency in app stores, consumers can't tell when they -- when they look at apps in the store or even when they're running them, often, whether they secure the transmissions. If you go to Starbucks or the airport or the hotel -- and tens of millions of people do use apps there -- you can't always tell if it's encrypting your wireless transmissions.

Also, the last point here is that app developers vary a lot. We talked to people who told us that there were developers who do very little to protect the data they store on your phone in the event that it's stolen or lost, whereas, you know, guys like Facebook, I'm sure, you know, are doing everything that Apple or Google provide them with. But there's no way that you, as a consumer, can tell the difference between a developer that's doing that and the developers that really aren't protecting the data, and we think there's a need for more transparency about that kind of stuff.

It's really worth reading -- I have a little pitch here for The Magazine Store read. The whole thing is on the Web for free. We have tutorials for people on how to secure their phones. There's a lot more detail there, including how many Apple users have actually gone outside of the Apple App Store, but I'll let you go read the story to find out some of that stuff.

MS. ROBBINS: Great. Thank you, Jeff. So, I actually added up some of the numbers on your slides, and it looks like 64 percent of consumers don't have passwords on their phone at all, and I can say from experience that my nine-year-old had to tell me, when I first got my smartphone, that I could do more than a four-digit pass code.

So, now, Markus Jakobsson has put a lot of thought into the vulnerabilities of passwords, and so, Markus, can you please tell us your thoughts and what you envision alternatives could be?

MR. JAKOBSSON: Thank you.

So, let me just start by commenting on one of the numbers that Jeff gave. I think the survey is great, but it's one risk that you're facing when you're asking people what they're doing, that maybe they don't know what they're doing. When corporations measure how much -- to what extent malware -- antimalware products

are deployed, they don't see 80 percent. They see much smaller numbers.

So, it might be because people think that they have antivirus protection, because they once did and now it expired, or they think that they did but it was really something else. Many people install what they believe is free antivirus and it's really malware. So, I mean, this is not to call into question the numbers. It's just to highlight the risk of asking the end user.

Now, in my presentation here, I will speak about the end user but from a different perspective. So, I'll talk about passwords and why I think it's a great problem on handsets. One of the foremost issues is that it's very hard to enter a password, a good password on a handset, and also, the number of applications and opportunities to authenticate that people interact with on handsets are greater than in the desktop market, and, therefore, the likelihood that people will reuse passwords is greater and also the probability that they will use something really simple is greater. So, there are lots of risks here.

The question I want to start by asking is why is it that people have such a hard time with passwords on phones when they can kind of manage it on desktops, when, in contrast, they're managing SMS'ing text and

emailing friends from the phones very well? And one of the big differences is that there's autocorrection on SMS and emails. If you type the wrong word, the right word appears. And that is not the case, of course, for passwords, because we don't enable autocorrection for passwords.

And the second question to ask is, why are good passwords hard to recall? And this is not in the context only of mobile, of course, but in general. And that's because we want -- we, as a community, want passwords to be weird. We want them to be unpredictable. We want them to have a special character and a couple of numerals, and this is not how humans relate to things. I mean, we are designing passwords as credentials that should be memorized by humans, not machines. So, it's kind of absurd to ask people for all these special things that probably aren't going to be that random after all.

If you look at the distribution of things and if you ask people to put some digits after the word that they put, something like 1-9-7-6 -- 1976, which is a year that you might have been born or somebody you know has been born -- is much more common than a number such as 1742, a year you obviously were not born. And so there is a very uneven distribution, and the people who

manage the corporations' log-in centers, they don't know, because they don't see the passwords. They don't actually touch passwords. They store them in a safe way. But the attackers do. The attackers see all the passwords, and they know what we don't know unless we take unusual measures.

So, now, let me show you a stab at a solution to address both of these things at the same time. Imagine that you're allowed to use a word as your password. Of course, that is not a good practice, because -- well, first of all, there aren't that many words, but it has one nice aspect. Say that your password now is "frog," and you fast finger the keyboard and write "frof," all right? Not a word. But the application, the password entry would know that, well, "G" and "F" are kind of close to each other on the keyboard, and "frof" is not a word, but "frog" is, and so it would autocorrect. So, that takes care of one big problem here, which is that it's a constrained input.

Now, the problem, of course, is that there are about 64,000 words, and not all words are equally common. You would find "love" much more common than "homomorphic." So, this is another problem with it, of course. Now, if you take three words after each other, you actually get a very good security, and it still

allows for autocorrect. And so that is something that, in my view, is better to deal with than passwords, and it's simpler on a handset.

So, let me show you some graphs for speed. This is -- the green line here is the time it takes -- this is a cumulative distribution, how long it takes to enter a simple password, and the red one is a strong password, and the blue line here is what I've shown you, which I just called a fast word. And the portion of users on the X axis, what it really means, if you look at, for example, the 50 percent, it's halfway along the X axis, you'd see that almost all of the simple and strong passwords, close to 100 percent, fall in that -- they take 100 seconds, or about, to enter, whereas 50 percent of the fast words take only about 5 to 10 seconds to enter. So, this is a huge difference in terms of the time it takes, because autocorrection and autocompletion works in our favor.

Now, if you look at the security, this might not make sense unless you understand second logarithms, but this is a guessing probability in log 2. This is the average fast word security, whereas here, off the scale is the average password, about 19 bits of security, whereas you have got more than 40 bits of security, and this is based on actual distributions. So, this is what

users said.

And one other thing in favor of this is that you get dramatically higher recall rates, because three words that mean something, you can relate to a story, as opposed to some number and some strange character that you have to include, and that's a benefit. Now, if people do forget, for example, if they are forced to use different credentials at different places, they can't remember what credential did they use in one place, you could actually give them a hint. You can give them the first word and say you've got to remember the other two. Of course, you're degrading the bit security by one-third, but still it's more secure than a password. The benefit is that nobody forgets now.

So, say that you -- your story is a weird story about when you went jogging in the forest and you stepped on a squirrel, all right? Jogging, forest, squirrel. If it happened to you, it's hard to forget, but maybe you don't remember that this is the one you used for log-in at your financial institution. The minute you're told jogging, you know what it's about.

Now, let me talk about something completely different, which is how do you authenticate on a platform that doesn't even have a keyboard, not just a small keyboard, but no keyboard at all? And I am going

to use Google Glass as an example. Apart from a camera and a microphone and also voice feedback, it's got a touch sensor that allows you to say back, forward, and up. Those are the three things that, by rubbing your glasses, you can communicate. And that's going to be how many menus are traversed if you are a Google Glass user.

I am going to show you how you could input a credential using only that, and here, the context is very limited output, you know, you have a teeny tiny screen that can say just a little bit, and you have got an adversary that, in essence, knows everything you know -- you show to the public. If you speak out your credential or if you make gestures, like a 2 in the air in order for the camera to capture it or show a number or fingers, the adversary potentially knows about it. So, that is an unusual setting.

You could think of a handset as being an input opportunity, where there's nobody eavesdropping on you. You could input on your phone without somebody seeing it, but on Google Glass, you cannot. So, here are the instructions that will be given. Change the PIN to yours, all right? So, that's all the instruction you're given. Now, assume that you are a typical user. That means your PIN is 1234, sorry to say, and it starts at a

random point. This is not your PIN.

Now, you could see there's a cursor, and you could scroll that up and down, which on Google Glass actually corresponds to forward and backward. So, if you don't like having a 1 as a first character, then you change. This is forward, this backwards. Now, if you like 1, which in this case you do, you're tapping, saying next. So, tap. You like 1. Now you want a 2 here. You go back, back, back, back, back. You got a 2. You like this, so you tap. Three is fine. Five is not. You've got to change it. So, now you change it to a 4. And then you submit.

Now, the question is, what did the adversary learn? Nothing. You start at a random point. The adversary, who knows everything you're doing from observing you, microphones and camera, sees you rubbing your glasses. Not a big clue. But you're logged in. So, this is to say that when you have new input/output opportunities, there are different attacks, but there are also different opportunities and we should take advantage of them.

So, there are lots of things that I would like to speak about, which I don't have the time to speak about, but which I encourage you, if you are interested in, to take a look at. If you are interested in how to

avoid spoofing, there's a link to an effort that I've been involved in; how to create PINs if your users don't have any but they have a password; and what I talked about first, but more details. Thank you.

MS. ROBBINS: So, before we get into the other two presentations about authentication technologies, I want to just play this one clip for you. Oh, thank you. Perfect.

(Video Clip.)

(Music.)

"It has been reported that in the future simply typing in your pass code may be obsolete. Here at the School of Information, researchers are studying the use of brain wave authentication as an alternative to logging into computers.

"These laptops, they can scan your fingertips to log into. There is now secure systems that would scan, for example, your retina. And we wanted to build a system where we would scan someone's brain waves, and then we would -- using their brain wave sample, we would be able to identify them and authenticate them into the system.

"Undergraduate Hamilton Nguyen has been working with Professor John Chuang and his team in researching the use of passed thoughts. Here, users think of

certain thoughts or images in order to gain access to their computer devices. The team has been using the company NeuroSky's MindSet device, a bluetooth headset with a sensor that measures the dominant brain waves. The sensor is placed on the left frontal lobe, where emotions and mental concentrations are most dominant.

"Their study experimented with participants who performed a multiple mental task, including thinking of a repetitive motion and singing their favorite song. In doing so, the headset recorded and measured each individual's brain waves. Brain waves are similar to fingerprints and are measured through electroencephalogical, or EEG, signals.

"Everyone has brain waves. Everyone has brain waves that are unique to them. So, this should -- though this could possibly be a more universal form of biometric authentication.

"However, there are some concerns. The team has yet to figure out how to stop hackers.

"If an attacker knew the user's pass thought, could they think the same thing and be able to dupe the system that way? That's not something that we've -- you know, that's not really something that we've had time to look into, but that would be a -- you know, a possible security concern."

MS. ROBBINS: Okay. So, that's just food for thought for a moment.

Now we're going to get into -- we have two companies here who have developed authentication technologies. One is Passban, and the other is Yubico. And so, Kayvan, do you want to tell us --

MR. ALIKHANI: Sure.

MS. ROBBINS: -- about your authentication technology?

MR. ALIKHANI: Thank you. Thank you so much. Great panel and great sessions today. Learned a lot.

I'm here to talk about the death of the password, whoever's going to be unhappy about this one, but the sessions I've seen so far and also the conversation surrounding security, the selection of a strong password, something that's complex, and changing it, I don't think people look forward to putting upper case, underscore, question mark on their smartphones to log into their applications, not in public environments or in transit or at work. That's the bad news.

And the good news is that over the past, I would say, four or five years, the smartphones and tablets that we've grown accustomed to using have now become extremely more powerful in that the devices are capable of detecting who we are by our facial recognition, what

we say by voice detection, how we move a device through a gesture, our location, what we wear, as a wearable device, and carry it with a smartphone or tablet. Ultimately, more advanced methods, such as pass phrase that was just mentioned, sentences, or the use of pass colors, a color palette shows up and you select colors as a means of detecting or identifying yourself.

So, ultimately the idea being that the device is incredibly capable of actually performing everything I just said without the need of any additional effort on the user's behalf. You are who you say you are because of your face, your voice, or because of your location or something that you're wearing. As a result, the need for remembering the complicated password that can be so easily compromised -- as I'm sure a lot of you read the same articles and publications, we just read an article about three hackers competing on how fast they could decrypt 20,000 passwords stolen from a set, hashed up, completely encrypted. Within less than a day, one of them was able to, using a very average, modest machine, decrypt all those passwords.

So, the concept is this is a foregone conclusion in our opinion, and obviously the compromises we're seeing left and right show that the passwords are just something that served their purpose for a long period of

time, but now, with the capabilities of the devices, we're of the opinion that there's more modern, more seamless and, frankly, more convenient ways to identify a user rather than asking them to put in a 16-digit password so it takes a year decrypt it, and obviously it takes a year to input that data as well. So, that's really the idea, is to provide mobile security and inherent solutions on the smartphones and tablets, considering the capabilities that these devices have.

I'm not going to repeat the statistics. Obviously our stats are more around the group of -- the set of surveys that we did, around 2000 people, not nearly as elaborate as the report we heard from Consumer Reports. But basically because of frustration or I don't want to enter this data, what then ends up happening with all of this is people push that "remember me" button, right? So, you end up not entering the password, using -- I don't know, of the audience here, how many actually enter the password to get into your email or to get into your calendar or to your -- any application. You're typically looking for that "remember me" or "keep me logged in" button.

That's not because of the application developer's lack of interest in security but more because they wanted to provide that user convenience,

the ability for you not to have to enter that complicated data on the system, on the device.

So, the challenges that we see with some of the solutions that -- and some of the mole security challenges that people face is now you end up saying, okay, well, I've installed 15 applications or 20 applications on my smartphone, and if I'm wanting to do real, true mobile security the right way, I have to have different passwords for each of these applications. So, you end up now having to manage a group of passwords. You add a question mark to the end of one, add an underscore to the end of the other, and it becomes inconvenient and leaky and easy to guess. If you end up using the same password across multiple applications, now just one system needs to be compromised for all of your data to be available to whoever's trying to get access to it.

The other challenge that we've seen is a lot of emphasis has been put on actual phone security. So, lock the phone and unlock the phone and now everything's available to the end user. This may be a great solution for actual first responder or first line of defense, but if you think of a shared environment or where actual compromises are happening, where data, identity theft, and basically compromises occur, a lot of it is by

people you know, is actually at home or at work, within the environment that you're actually working or live. And so a lot of these devices are actually in a shared environment.

At home, for example, we have an iPad that's shared amongst five -- four people, and the password is 0000 because my four-year-old has to be able to use it, and I have to be able to use it, and she can't enter any other data as a password yet. So, in a shared environment like that, if the locking factor supposedly was my face or any other wearable device, in the absence of me being there, now none of the other family members would be able to use that device. So, maybe the solution is to say, you know, unlock the device, and using a very simple or complicated password -- take your pick -- but secure the applications and certain transactions or events that happen through the application.

Maybe Angry Birds doesn't require protection or encryption or password-based access -- maybe it does you want to protect your score -- but maybe your financial or banking app or the healthcare app that provides critical or sensitive information about you is worth securing. Maybe Dropbox, as an application, doesn't need to be concerned, but maybe if you secure a specific

folder or two or three documents within that and provide authentication or verification, that would solve the problem.

And then we really think that it's time for a lot of these products to come together. You know, you're having -- in today's panels, you see a security solution from Apple and uses identity through Apple ID, and then Google obviously has the Google Authenticator solution and Microsoft has a similar solution, and then compound that, multiply that by a thousand, each company has their own siloed way of identifying users. And if you now start introducing multifactor or methods of face or voice, and imagine you have to enroll now into each of those applications separately, we are actually going to create a bigger mess than we already have.

So, we think the time has come for single identity or a means of identifying users using one form of identification across multiple applications, and there's a lot of initiatives, such as FIDO, that have started to address that, to provide a means of bringing authentication solutions together.

Application usage is exploding, and that 13.4 billion downloads during just one quarter is amazing in that if you think of Android and the phones that are commercially using them and how long has it been taking

us to get here, we're talking about a four- or five-year time span, and now we're talking about this number of applications being downloaded. So, it's a healthy and growing usage by users; however, we think that as a result of so many applications being downloaded on devices that are so capable of multifactor verification capabilities, it's time to introduce them into these applications.

There's some surveys also we did. What apps would you secure and what transactions would you secure? And it was interesting to me that, you know, myself, I don't secure my email application on my smartphone, just access gmail, but it was number two. If people had a convenient way of securing email by simply using a face or a gesture or maybe an item or phrase or using a wearable tapping on a wristband, for example, to unlock the application, they would use it.

And also, shocking personally to me was the need for requests by people ages 29 and under, 40 percent of whom were asking I would protect my Twitter or Facebook or what's an app-type application in that they don't want other people to see the messages or stream of events that are happening on their specific Facebook page. So, ultimately, what we're seeing is looking for solutions that are adaptive.

One thing, also, that I want to mention is solutions that end up asking the user to be in a perfect environment for it to work. The face only works if it's well lit and if you're in front of a good camera and it's got the right frame per seconds. Well, you know, users are not always in those environments. So, there has to be a method of adapting to the user's environment.

Flexible devices. I had an iPhone and now I'm on an Android device. I had an iPhone, now I'm using an iPad. These types of identity solutions have to work across these devices. You don't want to put the user through the process of re-enrolling and re-introducing multiple passwords, and that's now a possibility with the ecosystem that we have.

And play well with others, systems that are providing, okay, I can do password and I can do face, but this device is capable of doing voice verification, for example. Bring that into the solution, play well with others. This is also now very much a possibility to use the capabilities of the device but introduce new methods of verification.

And ultimately, portability, in that if you're using a device, you lose it or it gets stolen, that you should be able to use that same identity on a new device

that you acquire. These are the kind of, I would say, four or five items that we've identified as the key metrics for this.

Thank you so much. Do I go through this to the next?

MS. ROBBINS: Great. Before we get into questions about your technology, Terry, would you like to talk about Yubico's new authentication technology?

MR. SHOFNER: I sure would. Thank you very much. It's a pleasure to be here. My name's Terry Shofner. The company is Yubico.

I'm going to -- listening to some of the conversations today sort of took me back. I'm not a scientist. I'm not a technologist. I am an engineer that went to school, and when I got out of -- got graduated, I said, man, I got a job. I fooled a lot of people and was able to keep going with this thing.

What I am going to try to do is bring you to a level, and when this was probably a corn field, and think about the guys down the hill that had -- their major asset was their home. I'm going to take that and just carry that with me or stay with me a little bit. I know it's getting late in the day.

But you had a home, and you probably didn't lock it; you probably didn't have keys. But eventually

people started using keys to lock the doors on their home. And then about 100 years ago, somebody came up with an automobile. That was a cool device, too, and it was also a major asset. And this major asset in those days, that didn't have keys. The trick there was just, you know, do you know how to drive it? And a few people did, and so that was the -- how you were protected. But eventually, keys came into play. And today, you have keys that are quite sophisticated. You get -- walk up, you get close, it opens up. There is some technology that makes that fun and makes it easy to use.

And then now, today, we live in a world where our assets are tied up in bank accounts or we're working on the Internet, and think how -- and I know everyone knows how important it is to have access to the Internet. You can lose your phone, you can be without a phone or be without a home phone, but take away Internet access for a day and you've got problems, or at least I do, because I can't do my job. There's so many things that I can't do.

And the cell phones today become smartphones, and it keeps getting better and better, but there's still one common thing to that. You have a key. That's where I'm going with this, what I am going to be sharing with you a little bit.

I assume that I just hit an arrow and we go forward?

If you go back 20 years ago, a technology came up -- we started thinking and talking about two-factor authentication, what you have and what you know. And this has been around for a long time basically in very competitive modes but very similar. This product works the same way. And where I'm going back is a little bit on legacy user names and passwords are broken. Some of the statistics that we borrowed from you are a trillion in one year. That's a lot of hacking.

Now, going into malware and the bad things that are happening, I'm just talking about things that can happen and get into your phone or your data. It used to be your house, used to be your car; now it's getting into the cloud and the services that you're using on a daily basis. And if you look at smartphones -- and it goes to one of my associates about how difficult it is to take a smartphone, and if you are going to use a user name or a PIN and then plug in a -- not a four, but maybe a six, maybe a 12-character, that's pretty tough stuff to do, especially when you're clumsy, as I am. It's very difficult to do. So, doing that, the complexity or just the awkwardness of using a product that's been sort of legacy-driven, well, there's some

things that are out there that are -- that are coming along that are better.

The company Yubico has been around for about seven years, and in the earlier days, it was a vision that someone had of taking a token, a USB token, and you insert into a PC -- we're agnostic as to the operating system, whether it's a Mac or a PC -- and you can just touch this button, touch that button, you would generate a 44-character, one-time, AES-encrypted password. Wow, that's pretty cool.

And when you did it, you didn't have to repeat it. You didn't make a mistake, because in this case, it's event-driven. If you screwed up or something, you lost your connection, you go back and touch the button again. So, the product that we're talking about is this little thing right here, waterproof to 50 meters, no battery, no LCD, nothing. You just insert it and touch the button and go.

So, this is where we got our footing, and we have been growing and we continue to grow. Today, we're just speaking in terms of millions -- and if I knew how to do this -- hang on with me, I've got the button wrong. I know what I'm doing. Prove me. But we were limited to the USB device, and that's still good, because we have a lot of people that have been sitting

on these panels today that are using this product in their environment. It's just simply a USB device.

And the idea -- the name Yubico comes from our founder, who said the idea is for this to be ubiquitous, meaning affordable and everyone has it. If you're using this single token -- there is a message here that I'm going to -- but having this single token, that's readily available, that you can use as a consumer, and make connections securely where you need to work or where you need to go is a pretty good and pretty powerful thing.

So, what has happened, the technology, people in our company, you know, when smartphones -- consumers, pretty much all of us will have one of these phones. This one just happens to be an Android. And I am going to think about what you do today to authenticate, and if you don't use passwords, that's probably not a good thing, but if you do, it's good.

So, I've just turned on this phone. I've put in my pass phrase. Now, what did I do with it? Okay, here's my YubiKey. I don't know whether you can see this or not, but I'm just simply touching this to the back of the phone. What just happened, I've opened the browser, entered the URL, sent a 44-character, one-time pass code, and let me get in. Now, I didn't have to remember anything. It wasn't my face. It wasn't my

breath. It wasn't my DNA. It was simply touching something that I have, that's secure -- a secure element, I might add, that it connected up to my server for me to do my work.

The only difference is I did this for wow purposes and I didn't put any PIN number in. I used the swipe code. But this is where we think the world is going. Affordable, fast. Fast. Think about no support. Think about your support issues pretty much going away.

Okay. So, this thing gets even better, because can you imagine a token like this that has a PIV applet on it or it could be -- you know, there could be money stored on it, so when you go to your Starbucks, you touch it to the token and walk away, because it's CCIT-ready. Anyway.

And then going on to some of the conversations on the standards. It's been sort of a wild west for a while, and there seems to be now an emerging group of people putting their heads together, saying, okay, what's the best protocol? And we're part of that group, and we've partnered with Google and another manufacturer called NXB that is in the technology world, the chip manufacturing. It's one of the concepts that we think is a good way to approach the market.

At sort of the end of the day, you have got this standard universal-2 Factor, U2F it's sometimes called. So, you're a user, you have your YubiKey or you have -- you're using your phone or your PC or your tablet, anything in this case -- I didn't qualify that it has to be NFC-ready, which is pretty much everybody out there except for one manufacturer, and that's Apple, but these devices are ready. You could be going to your retail store, you connect, and then you can do your banking or you connect to the services that are out there.

So, you just envision what -- this is ready today. This is a product. This is not the future. This is what we're offering out for you today. But you have this ability to do single sign-on, SAML, all these things. Password managers, there's a company out there called Last Pass, that if you have a YubiKey, it just integrates with them automatically out of the box. We're hoping you'll see the banking take a hold and recognize this as a good way to go. That's it. Thank you very much.

MS. ROBBINS: Thank you, Terry. I think Markus would like to comment.

MR. JAKOBSSON: So, I just wanted to briefly mention that on the topic of password managers, that, of course, this is where it ties into the whole malware

discussion, because that's the one-stop-shopping opportunity for the malware authors, to steal all the credentials at the same time. So, this is a good touch point between the two portions of the panel, to recognize this is where it matters.

MS. ROBBINS: So, before we get into that, I want to just talk about one thing that Kayvan had said about keeping your device unlocked, and the purpose of, I guess, using biometrics and your authentication technology is that you would only have to authenticate -- you would lock individual apps. So, it wouldn't actually lock your phone; it would lock your apps.

MR. ALIKHANI: Or both. The idea was to be able to use that same device in a shared environment, and if there's one password and now five people have to know the same password, it kind of defeats the purpose. So, the idea was lower the bar maybe for unlocking the device but increase the bar for selective applications that need to be secured.

MS. ROBBINS: Okay. And I'd like to ask -- so, both of -- both, Kayvan and Terry, your authentication technologies, how will those help consumers who have actually had their phones stolen? I mean, so we're talking about authenticating -- getting on -- you know,

getting onto apps or getting into websites, but if someone's phone is lost or stolen, how would that -- because it seems that your phone wouldn't necessarily be locked itself, right? The device itself wouldn't necessarily be locked. It would be your apps or your -- you know, authenticating yourself on a website.

MR. ALIKHANI: Right. And do you want to --

MR. SHOFNER: No, go ahead.

MR. ALIKHANI: Typically, when your phone is lost, you are probably less emotionally attached to the phone itself than the data that you lost on that phone, and that data is -- again, if you think of the statistics and what apps you're running on that phone, it's probably two or three or four of those apps may be pictures, messages, and some application that is storing mobile content locally that you are very, very interested in not providing unauthorized access to.

A lot of great applications provide remote wiping of that data. So, you know, now that you've found out that it's lost or stolen, as long as the device is not taken off the network, you can provide remote wipe capabilities. But the application that -- the solution that we're advocating would then say it's fine. The device is lost or stolen. It's useless in the wrong hands. But that person who stole the device

has to also be you from a biometrics perspective or has to wear your wearable device or the type of two-factor device that Terry was just explaining. So, it significantly increases the bar in terms of -- it raises the bar in terms of preventing unauthorized access to the application in the wrong hands.

MR. SHOFNER: So, let me build on that just a little bit more. It's the same thing, you have to support it. The difference, if you lose the phone, but in our case, you have to have the token, and you have to have the PIN number. So, it's what you have and what you know, you still have to have that to access those applications.

In our world, we're taking a standard YubiKey and being able to use it across the board with many applications. So, on the back end, the companies that subscribe -- that's not the right word -- that use the authentication mechanism that we provide, they're good to go. And those may be different. It's not the same, because it changes every time you touch that button. But you're generating that one-time password or, you know, it's the secure elements generating the way that it links so that it doesn't. You can't -- you can't get into those applications.

MS. ROBBINS: So, Markus, I think you were

starting to touch on, then, the security vulnerabilities, I guess, of these authentication technologies. Is that something that you could expand on?

MR. JAKOBSSON: Well, so once you speak about user authentication, of course, the most practical paradigm is to authenticate to your device and then let your device authenticate to the websites. That means that you have a storage of credentials. That is, for example, the principles behind what the FIDO alliance is implementing. They have keys that are stored on the device.

It might be that they are sandboxed, depending on the implementation. It might be that the code is hardened, but nevertheless, the credentials are on the device. This is where authentication meets malware, because that is the source of monetization for the malware authors, exactly that storage.

MS. ROBBINS: So, do you see this as not a benefit, then, for consumers?

MR. JAKOBSSON: This is why many large financial institutions do not support password managers, and that's all I'm saying. It's a cost-risk benefit. If anybody in this room wants to use a password manager, that's probably safe, but if the -- society, as such,

switches to password manager of any kind, it's going to cause a new type of fraud in which you won't see phishing, but you'll see more malware.

MR. ALIKHANI: By the way, let me just say, also, these passwords are already stored on these devices. So, you know, whenever you are pushing that "remember me" button, you are, by default, asking for that information to be cached or stored locally on the device.

And to Markus' point, talking to a variety of different people, we get different answers, all the way from I don't want my biometric data to be stored on your server, to I don't want any of my biometric data to be stored on this device. And each of them have their good reasons for it. Some of them, to your point about the device is most vulnerable in the wrong hands, they can hack into it and decrypt it and access it, but also, if you're storing information on the server, not providing that local cached data, you are asking for a transmission of data across the wire for authentication purposes.

MS. ROBBINS: Okay.

MR. SHOFNER: And I need to clarify, too, because we're not -- in our case, our passwords are not stored. That phone that I just used for demonstration,

I took an out-of-the-box YubiKey. All I did was turn on the NFC capability, and I touch it, and it goes to my server. There's no password. There's no application. This is working directly off of the firmware that's inside of the key.

So, I may have not used password managers or just something else that we work with among many, many, you know, thousands of things, but most people in the consumer world are using or trying to use things that they get away from so many passwords that have to change. It's a -- sort of an easy way out. I'm certainly not promoting that. I'm just saying this is something we work out of the box with.

MS. ROBBINS: Mikko, I know you wanted to say something.

MR. HYPPONEN: Yeah. One difference between saving your passwords, like ticking the box "remember me," and using password managers, like the popular Lost Pass or one-password systems, when you use those password managers, many users don't actually know their passwords anymore. They autogenerate random passwords, which they have never even seen themselves.

When you save your own passwords, you basically know a password. And this opens up a new angle of attack, which is ransom attacks, attacks against

password managers, not to steal the credentials, but to take away the credentials from the users and make the user pay to regain access to systems where he has no passwords anymore, because he never knew them and they have now been taken over.

And we have seen ransom malware, in general, raise in popularity by the attackers on computer platforms. We haven't really seen attacks like this before, but it's a pretty obvious angle for an attack.

MS. ROBBINS: Go ahead.

MR. HALLIDAY: Changing gears slightly on this, you know, I think someone mentioned that the majority of mobile users don't actually have passwords enabled on their devices. I forget if that was Jeff.

MS. ROBBINS: Right.

MR. FOX: Yes.

MR. HALLIDAY: And one thing that I was really struck by when Markus gave his presentation on sort of Google Glass and a way to input a password, I was just thinking like, wow, could you think of a worse way to, like, authenticate on a wearable device, scrolling through numbers, clicking yes, scrolling through numbers. I mean, we have to think about -- when we talk about the fundamental problem here, which is the fact that users don't -- the majority of users don't actually

use passwords, we need to think about ways to actually enable that in sort of a usable way.

And as we move forward from just, you know, mobile phones to tablets to wearable computing to whatnot, you have a lot more options than just, you know, a PIN code. And when we talk about multifactor authentication and the pairing of something that you know with something that you have, we can expand the world of things that we know significantly beyond just, you know, entering a PIN.

Glass, for instance, has gaze detection, so you could actually -- you know, you could actually wink and that could be viewed as an input. I was fortunately blessed by Google to have the chance to pay them $1,500 to use a Glass, and there's actually an open-source application already developed and out there that is very similar to what Markus mentioned, and it's called Bulletproof, that lets you enter a password, because basically Glass doesn't come with a PIN code for security purposes.

It's similar to what Markus mentioned, but instead of selecting digits, it actually interprets swipes as unique identifiers. So, your password to log in could be swipe forward twice, tap, tap, swipe forward, swipe backward twice.

So, when we talk about some of these new options towards authentication and multifactor, it's -- I think it's useful to remember that I think rumors of the demise of the password are greatly exaggerated. I think that there's always going to be room for one piece of authentication, which is something that you know. Now, we just have to not be myopic about what's meant by that.

MS. ROBBINS: So, I think, you know, is the message to consumers then that -- in light of the statistics of lost and stolen phones and consumers who, you know, don't use passwords at all, and so their data is much more at risk, I mean, what is the message to consumers? To continue to use passwords that are easily cracked, that are -- you know, they reuse them, they -- you know, they lose them, or is it to move forward in one of these new authentication type of technologies, biometrics? You know, what is the message to consumers who don't even want to use a password to begin with?

MR. FOX: Well, I'm not in the position to solve the problem. These guys are solving it, but I think whatever the solution is, it's got to be something that most ordinary people are willing to do, and, you know, we're all kind of geeky -- I know I am -- and may be willing to tap, tap, twiddle, twiddle, or blink, blink,

or whatever. Not many people in my family are.

I just don't see the people doing that. People that don't even want to punch four digits and slide their finger over to open a phone, I don't see them getting into some kind of little Morse Code with their eyes and their fingers. So, you also have to think about nontechnical people, what they're willing to actually do.

MR. JAKOBSSON: So, I wanted to say that I hope that passwords are going to largely go away and be replaced by biometrics, but I wouldn't want to instill hope that they're going to go away entirely, because after all, when you're getting a new device, you need to kind of introduce yourself to that device. That's one form of authentication, and the other one -- before it can learn your biometrics or download them, for example, and another kind is the recovery.

So, if somehow you cannot use biometrics or somehow your Yubico device was, you know, lost or you put it -- displaced or you don't know where it is, somebody took it from you, I don't know what would happen. You need a backup. And the interesting thing is, if you use a password every day, you probably remember it. If you use it twice a week, you probably do, too. But if you use it twice a year, you're not.

And so we are moving in a direction of where it's more convenient to the user because of biometrics, but when disaster happens, it's really bad, and you need to be able to enter a credential then and you should not have forgotten it. So, that's an interesting dilemma.

MR. HALLIDAY: I would also say that, you know, it's important that we don't encourage consumers to, you know, get a false sense of security with some of these new technologies that are emerging. I mean, there's still going to be dependence on things like passwords, especially in the short term, and enforcing just reasonable behavior in terms of, you know, reasonable complexity as well as just sort of being generally paranoid about who you show your password to, I think is generally a good thing to encourage amongst mobile users.

I mean, even right now, it sort of all depends on, I guess, your threat model, but I think almost everyone in this room right now knows Terry's password on his phone from his presentation, and I could -- I could unlock his phone right now, you know, if I had a lead pipe. So, it's sort of -- so, it sort of depends on your threat model.

MS. ROBBINS: So, I'd like to move into the next area now where we're going to talk about antitheft and

antivirus technologies that are solutions for consumers, and this is, I think, particularly relevant because -- well, first of all, Jeff has said that in the Consumer Reports study, that two of the main risks to consumers are lost or stolen phones and malware, and we learned this morning that there is a big malware problem and there isn't a big malware problem for U.S. consumers. So, we won't go into those statistics right now, but we know that -- I just want to throw out some statistics about stolen phones.

So, Consumer Reports found 1.6 million smartphones were stolen last year, and there was a recent Lookout survey that found one in ten people in the U.S. had their phones stolen. And in New York City, 11,000 Apple devices were reported stolen in a nine-month period, and in D.C., 40 percent of the robberies in 2012 involved cell phones. So, given that backdrop, I'd like Derek and Mikko both to give their presentations about their antitheft and antivirus technologies, and then we can get into some discussion.

MR. HALLIDAY: Let me see if I can get this working. Okay.

So, first, I'll try to keep this quick so we're on time. But at Lookout, we basically build tools to help people use their mobile devices, you know, with

confidence, and since around 2007, we've provided a set of features oriented around security that include things like data backup, antimalware protection, protection for lost and stolen devices, ability to remotely lock and wipe devices. Since that time, it's actually become a feature set that's somewhat recognizable, essentially the sort of de facto standard for security on sort of the mobile platform.

And we've heard a lot about -- you know, during today's discussions about threats that people face on their mobile devices and sort of relative degrees of risk that people are faced with. We've been in a unique position to have been tracking a number of these threats for a number of years, and I wanted to provide a little bit of -- a little bit of context across a few things that have been mentioned today.

We've seen that, you know, in 2012, an estimated 1.4 million U.S. Android users encountered a bad app over the course of 2012. So, that's -- you know, that's a million people. That's a lot of people. But when you talk about percentages, that equates to a pretty small chance of actually encountering malware in the U.S., just over 1 percent or 1.25 percent. So, while the raw total might be large on the surface, you know, smartphone penetration is pretty impressive in the U.S.

And if you look closer, you know, that rate varies tremendously geographically. So, I know that, you know, we're focused on really the -- so, the U.S. problems in this context, but that same likelihood metric of encountering malware jumps -- I think someone might have mentioned this in one of the previous panels -- jumps to around 40 percent in Russia and around 20 percent in China, where really broad-based, economically driven attacks have a lot more freedom to operate for I think a number of reasons that have been discussed at length.

So, compare that to the fact that around four in ten people clicked on an unsafe link from their mobile device in 2012. So, what do I mean by "unsafe link"? Well, I mean a phishing link, a compromised website, for instance, something that might trigger a drive-by download without their knowledge.

So, statistically speaking, you know, a much more prevalent problem and an equally troubling one, particularly because of the restrictions, you know, we've talked about in terms of, you know, what mobile presents from a form factor perspective, the ability to really scroll past and not see what URL you're clicking on, but also generally the lack of perception amongst users that, well, mobile devices and the mobile browser

are really subjected to the same types of risks that they might see on their PC browser.

And so lastly, you know, compare this to the fact that, you know, Colleen just mentioned that nearly 10 percent of people in the U.S. have had a phone stolen, and we found that actually through a survey earlier this year. So, when you factor in the economics here, this one becomes much bigger than the others, really a driving factor. We estimate that it cost consumers around $30 billion in 2012, which is no laughing matter.

And I'll be happy to dive into some more detail on the first and second items in this list, but I wanted to sort of dive into the third one, which is not quite as commonly discussed within these contexts. So, to put that -- to put that in perspective, in 2012, we found a phone every three seconds. So, that -- that's a pretty big problem. And while each of those loss events actually equates to, you know, a loss of a few hundred dollars in your pocket, like the panelists have mentioned, that's only one component of it.

What we've found is the theft is much more than -- represents much more than physical loss, and when asked -- when we asked consumers out there what they were concerned about, sure, the monetary downside

was one thing, but the loss of data was really sort of a compounding factor, if you will.

And so thinking about how we're actually solving this problem, so not talking about necessarily malware for the time being, how do we solve this problem? You know, I'm reminded by a quote from one of our investors that I think I may be butchering here, but there is really no silver bullets for this one, only lead ones. And so you can stack a bunch of different solutions together potentially to help solve this, but really, it's similar to, you know, the discussion on the previous panel around patching. You can't just snap your fingers and all of a sudden it's solved.

So, what are some of the things we can think about? Well, number one, you know, education, empowerment is big. People often talk about the education piece of it. So, you know, raise awareness and, you know, basically tell people they can put passwords on their phones. That's great, but it's not very usable and it's not very effective if the tools you give to them aren't really driving them to use them. So, if only -- you know, if the majority of users out there aren't putting passwords on their phones, they've probably had someone scold them about that, whether it's their, you know, teenage son or daughter or something or

whether they have a coworker who's noticed it, but there's obviously something wrong with the process if people are still sort of not adopting what should be a sort of basic, fundamental tenet.

So, some of the things we actually try to do at Lookout are to improve some of these basic features and make them more engaging and more usable. One really simple example was a tool -- a feature called Signal Flare, which helps you find a lost or stolen phone that may be running low on battery and sends you an email with the device's location on a map as the phone is running out of battery. So, you can actually find it if it's -- you know, if it has run out of battery.

The second one is called LockCam, which helps you identify anyone that's tried to log into your phone -- presuming you have a password, of course -- three times incorrectly. So, you can actually see that maybe on this phone, you know, our panel moderator has been a little busy while I have been away from my phone.

And so beyond education and empowerment, the second one is really marrying technology with law enforcement. So, we've been really busy with the District Attorney's Office in San Francisco and the AG in New York around, you know, enabling law enforcement to work effectively with technology companies when it

comes to solving this lost and stolen device problem.

And the third is -- is reduce incentives. Easy, right? Not so much. It's actually a really, really tough one to solve here, and when we think about what's driving this problem, at least when it comes to stolen devices, not necessarily lost ones, it's the fact that they can be resold or repurposed at an economic gain. And so there's a much broader cooperation that's needed to solve this problem between, you know, operators, platform providers, OEMs, et cetera, et cetera.

So, the FC -- the recently -- well, not even recent anymore. The FCC-mandated stolen device database is a nice step in the right direction, but way, way overdue, to be honest. By contrast, European operators established the EIR, which is the Equipment Identity Register, to hold a list of handset IMEIs back in 2003, and at the same time, there's been recent calls to enable sort of a kill switch, as it were, on mobile platforms and operators that has various pros and cons, but I'll leave that for discussion by the panel.

So, hopefully this provides a little more context to the real securities that consumers face, and, you know, we look forward to solving them with the broader community.

MS. ROBBINS: Thank you.

Mikko?

MR. HYPPONEN: Thank you.

So, when I look at the platform split and I look at the operating systems we are running, while it's been the case for the last 20 years that it's mostly the Microsoft platforms, they are all hit by malware. Windows has always been where malware is, and especially these Linux users have always been very happy about the problems Microsoft has been facing.

However, if we look at the situation right now in 2013 in a little bit more detail, we'll see that the three most common platforms you might be running on your computer are the same most common platforms you might be running on your smartphone, because your computer is either running Windows or OSX or some Linux distribution, and your phone is either running Windows or iOS or some Linux distribution. That's the top three for both. Of course, when we speak about Linux on phones, we mostly mean Android, because Android is Linux.

And as we know, on computer side, it's all Windows problems. Almost all of the malware we keep finding still today targets Windows systems. In fact, mostly the little bit older Windows systems, especially Windows XP, which is now 11 years old, which will be out

of support by Microsoft next year, yet it is the second-most common operating system. Windows 7, number one, Windows XP, number two, and then Windows 8 and Windows Vista.

So, yes, it would be easy to make the mistake of -- it would have been easy to guess a couple of years ago that it's going to look exactly the same on phones, but as we now know, it looks exactly the opposite. On phones, Windows phone has no malware, no malware at all, and Linux, in this case Android, has pretty much all the mobile phone malware. Of course, there's much less mobile phone malware than PC malware, but that's pretty much how it worked out. And Apple, on both sides, has a little bit.

This is quite surprising, actually. In fact, Android became the first Linux distribution that finally brought the malware problem into the Linux world. Out of all possible Linux distributions, it was Android that really brought the problem there.

There has been several mentions throughout the day about different statistics and the growth rate and how many tens of thousands of malicious mobile malware we keep finding. I'm not going to go through any details on the statistics we have. I'll just make a note that we, at F-Secure, we put out a mobile threat

report four times a year with detailed statistics and full-blown numbers about the growth rate of the problem.

Now, when we speak about mobile malware and Android malware, the problem can pretty much be distilled into this. This here is Angry Birds from Rovio, downloaded from Google Play. This here is Angry Birds, from Rovio, downloaded from Google Play. One of them is trojanized. One of them is the original. One of them is trojanized. One of them is a game. One of them is a game and does something bad, like dials out to toll numbers. How do you tell the difference? Well, you can't.

Here is a screen shot from Google Play. That's the official Google Play, not a third-party app store or not downloaded from the Web. It has Minecraft, Hay Day, Simms, Grand Theft Auto. Hay Day is actually made by a company called Supercell. Here, it's not made by Supercell. It's made by somebody called gilbert8332. Minecraft is done by a company called Majango. Here, it's not done by Majango. It's also done by Gilbert. Grand Theft Auto and Simms are made by EA, Electronic Arts. How do you tell the difference? How do you know, when you go and download something, whether you are getting the real thing or not? And, yes, Google does a very good job in limiting stuff like this getting into

Google, but yet they sometimes get to Google Play.

In fact, I just checked, there's very similar examples like this on Google Play right now. If I would have live Internet connection, I would show you. And, yes, Google does kick them out very quickly. So, we have to be fast to make a screen shot like this before they disappear, but they do exist.

Yet when we try to illustrate the difference in the problem size on your computer and on your phone, the best equivalent I can give you is the difference between size of sun and earth, all right? We have a massive problem with PC malware, mostly with Windows computers, and, yes, we also do have a problem with mobile malware, but it's nowhere near. Nowhere near.

In fact, you could say that mobile security is a success story. That's a bit an overstatement, but we're close to it, because ten years ago -- actually, nine years ago, when we found the very first mobile phone virus, we found the first mobile phone virus called Cabir in summer 2004. And if I would have estimated what would the situation look like ten years into the future, I would have estimated a much more grimmer situation.

I would have estimated we would have massive wormlike SMS-spreading malware in all major mobile

platforms. I would estimate mobile Botnets to be rampant and millions of infections. And that's not where we are.

We seem to be able to learn from past mistakes. None of the players in mobile space want to repeat the mistakes that were done with the PC platform, and the situation clearly is much better.

So, we manufacture -- just like Lookout, we manufacture mobile security solutions, and we have lots of operator customers, lots of consumer customers all over the world; however, the vast majority of those don't get our mobile security product to fight malware because they don't think malware's a problem. And in many ways, they are correct. The problem is very limited. It's unlikely still to run into mobile malware. It's much more likely to run into PC malware.

So, the main reason why they typically get mobile security solutions is for the other benefits of a mobile security solution, like the remote locate, remote lock, remote wipe, or web filter, or, for example, we have a filter for -- you can filter out texts or calls from certain numbers. So, if you have an irritating neighbor who keeps calling you, you can lock -- he can't call you anymore. Stuff like that.

Our remote local wipe system has been designed

to work with text messages. The idea is that you don't even need to have an Internet connection. You can just text your lost phone from anybody's phone, set a PIN, and mention that PIN in the text message, and you can, for example, send a text to your own phone saying "locate," and it will respond back with a text message which gives you a Google Maps link. It can tell you where your phone is.

And, of course, one thing which has been mentioned several times is phishing and other malicious website content and then web filter functionality. You give a tablet or a smartphone to a child, you want to make sure that she or he won't be able to access websites about violence or drugs or porn, where you want to be able to limit that functionality. And even for a normal user like yourself, who don't really need a web filter to filter out violence, you still want to filter out phishing content. As has been mentioned earlier in the panels or previous panels, phishing is a real problem still today, and it works better on phones than on PCs.

Thank you.

MS. ROBBINS: Thank you.

So, Derek, I just want to go back to something you had said about you and Lookout cooperating with law

enforcement. So, the DA in San Francisco has actually been very public about calling for a technological solution to lost -- to stolen phones and asking for a kill switch that would permanently disable the phone upon theft.

And so I want to ask you, what do you think of that idea of a kill switch? And how would that -- would that detrimentally affect consumers, do you think?

MR. HALLIDAY: It has a nice ring to it, doesn't it, you know, "Kill switch, turn that phone off." I think it depends on the degree to which it's implemented. So, sort of as it goes with a lot of these polarizing types of questions, it's -- I think the answer is somewhere in the middle. Like I sort of mentioned during my remarks, I think it's been way too long to have any sort of antitheft solution in place within the U.S. Even the solution that's being mandated by the FCC, to my knowledge, doesn't necessarily integrate directly with the EIR in Europe. So, it leaves open the potential to just ship handsets you might have stolen that are compatible with GSM networks in Europe and there you go.

So, I think it -- there's a number of different issues at hand. I think, you know, one potential other issue that arises is let's say you develop a kill

switch. That's great. Now, who sort of -- you know, who watches the watchers, as it will -- as it were. So, the kill switch is all of a sudden one new potential vulnerability that could be taken advantage of and presents its own set of security issues.

So, I think that movement in this direction is progress, because where we're at right now, there's not nearly enough protecting users, and that's, I think, obvious from just the massive number of lost and stolen devices that are occurring right now, but we have to be careful about, you know, walking before we run.

MS. ROBBINS: Mikko?

MR. HYPPONEN: This reminds me of the discussion regarding the great big Internet kill switch to be used by the President of the United States of America, and my comment back then was that if you build a kill switch, don't be surprised if someone else presses it.

MS. ROBBINS: So, one other question on antitheft and then we will just do one -- I think we only have time for maybe one or two questions on antivirus. But is there a way, do you think, for industry to solve this problem? I mean, I know this has been equated to the problem with car thefts, and so car thefts have gone down significantly since car -- automobile manufacturers have instituted antitheft

technology into cars. So, is there a similar technological solution, do you think, for phones to reduce the incentive for thieves to steal those phones?

MR. HALLIDAY: Yeah, I do think so. I think there's an option and room for improvement here. I mean, when we talk about the economic drivers here, it's about, you know, reselling the device or really shipping it off somewhere to be resold, you know, as a used or refurbished device. And when you put additional barriers in place that sort of drive up the economic cost from the bad actor's perspective, you're going to generally reduce incentive.

That said, there's -- I think there always will probably be ways to sort of fiddle with the device identifiers. So, if kill switches are sort of primarily acting on a number of device identifiers that are sort of hardware-based, there are always complex ways to get those to change if you are a determined attacker. But what we're really talking about here is trying to have an effect on the lowest -- essentially the low-hanging fruit here, and I think that's really sort of opportunists and reducing their ability to really sort of make a quick buck on this.

MS. ROBBINS: Now, Markus, your company, Fatskunk, offers an AV solution for consumers known as

software-based attestation. So, how does that differ from the products that F-Secure and Lookout offer to consumers?

MR. JAKOBSSON: So, let me start by correcting you. It isn't for consumers.

MS. ROBBINS: Okay.

MR. JAKOBSSON: It's actually to be built into the infrastructure.

MS. ROBBINS: So, how does it benefit consumers like that would?

MR. JAKOBSSON: So, it benefits consumers by having -- not only consumers. What it does, it aligns the abilities to detect with the liability. So, those who need to detect aren't always the consumers, but it's the financial service providers and so on. They can determine if you have malware, and if so, they can restrict your device so that you actually won't lose any money from that device.

And the way it does, it's -- theoretical computer scientists refer to it as an extreme version of the time-space trade-off. For the normal person, it means that you stop all processes, and then you run something very competitive-intensive for a few milliseconds, about two milliseconds, and that thing takes much longer if there is the presence of anything

on the phone. If anything is there on the phone and executing, which active malware, of course, will do, then it will take longer time for your process to execute, and, therefore, somebody who observes the time it takes to execute will know, and that somebody is aligned with whoever cares, so that your bank, for example, can tell if your phone is infected, and you can encrypt portions of your device by having somebody hold a key to that and only release it when a scan is passed.

But this is not something necessarily that consumers would purchase, but it's more what whoever deals with the consumers would want, enterprises and financial institutions. Now, that said, it is not on the market either. We do have it running on an Android device, but it's still in the concept stage.

MS. ROBBINS: So, it would be on the back end. So, consumers would never even know that it was there.

MR. JAKOBSSON: It -- devices will ship with it, and consumers or financial service providers or employers can enable it, after which it can be selectively enabled so that for certain resources, you have to perform this scan, which is not noticeable to the consumer, and it's not running when the scan is not initiated. So, it's a different kind of paradigm, and it doesn't block malware to get to your device, but it

does block malware from being able to monetize your device, because you can't get access. And so it's a good complement to code hardening and to the traditional antivirus approach. So, to answer your question, it's not an alternative, but a complement.

MS. ROBBINS: Okay. Okay. So, then, that leads me to my next -- my last question, I guess, because we're out of time, but given the statistics that we've heard today, that it seems like mobile malware isn't as huge of a risk for U.S. consumers right now, you know, what should the message be to consumers about putting antivirus on their phones and, you know, should this -- should consumers be doing this?

Is it really necessary or is it necessary because, as Mikko said, in conjunction with having the antitheft and that -- you know, that technology as well, that that's really beneficial to consumers?

MR. HALLIDAY: Yeah, sure. So, we talk a lot about, you know, one end of the spectrum here in terms of applications, which is, you know, the overtly malicious, you know, stuff that's going to steal your money and, you know, eat your babies and things like that. It's -- and at that end of things, I think that the risk, like we've all sort of come to agree, is fairly low.

I think that there's a broader opportunity here that's not necessarily being as openly discussed, and that has to do with the rest of the continuum of applications. There's a lot going on on your mobile device that the majority of consumers don't really have a full grasp on, and when you talk about moving beyond the set of applications that are clearly malicious to this sort of vast gray area in the middle, where some information about you might be collected or some information about your device might be collected, there's almost a sort of willful ignorance in place because of the complexity that that brings with it.

And so at least from the standpoint of Lookout, we look at -- you know, we look at malware and spyware and surveillanceware and all these things as just one piece of educating consumers about the risks of using their mobile devices, and what we want to be able to provide to them is really an opportunity to make, you know, an informed choice about what's actually going on on their devices. We think that at least right now, that the fundamental pieces in place from a platform perspective are okay but not great.

On Android, for instance, you breeze by the permission screen whenever you install an application because you really want to play that game, but you

really don't know what repercussions that has in terms of information that's being collected about you.

So, I think that the recommendation to consumers is broader, and it's -- if you are interested in understanding -- and, of course, some people maybe aren't -- but if you are interested in understanding, you know, what implications your mobile use has, there's an opportunity to sort of learn that and make more informed choices by using an app like F-Secure.

MS. ROBBINS: Well, I think we're out of time.

MR. FOX: I just want to say that our advice to consumers in Consumer Reports is it depends on your exposure. We've found that a lot of people only have 10 or 20 apps on their phone. If you don't download a lot of apps and you stick with places like Google Play and the iTunes, you know, App Store, you're relatively safe. If you're very active, you're doing a lot of apps and you've got a lot of sensitive information and your exposure is greater, then it would be a prudent thing to do to use antivirus.

MS. ROBBINS: Ten seconds or less?

MR. HYPPONEN: Ten seconds. We would love to see all the consumers install an antivirus before the first global, huge, massive outbreak happens, but realistically, they probably will install it only after

it.

MS. ROBBINS: Thank you. Thank you.

(Applause.)

CLOSING REMARKS

MR. HARWOOD: Can I just ask the last panelists to stay there? We will wrap up very quickly.

My name is Chuck Harwood. I am hijacking the Congress -- no.

I am the Acting Director for the Bureau of Consumer Protection for the Federal Trade Commission. I want to thank all the panelists we have had today. I want to thank the coordinators, moderators, the Division of Marketing Practice, the Division of Privacy and Identity Protection for the work they've done on this.

I just wanted to offer three quick observations regarding some of the things we've heard about and talk a little bit about going forward in the couple minutes we have.

First, here are three things I picked up. First -- and there are many others, but these are just three I want to mention. First, there is clearly, as Paul Ohm observed and others observed, a range of views about how serious the mobile malware problem is. Undoubtedly, some people think it's very serious; others think, eh, maybe not so much so.

Secondly, there seem to be lots of opportunities for better communication and cooperation. The discussion of patches that we had earlier today

illustrated that. We could do a lot more with regard to communications, with regard to cooperation than we're currently doing.

Third, it's pretty clear that the U.S. market is actually taking good steps to try to secure the mobile environment, but that doesn't mean we can't -- we can let up. We have to continue to remain vigilant with regard to this effort, because you know that the hackers, the scammers, the folks who are putting the malware out, they are going to keep trying. They are going to keep pushing at it. So, we have to remain just as vigilant.

This morning, the Chairwoman talked about three themes. She talked about law enforcement, she talked about education, and then thirdly, she talked about cooperation. And it seems to me that for purposes of addressing the three points I've just mentioned, as well as many others we heard, cooperation is the key.

The FTC is committed to trying to address these high-level points I've mentioned, as well as other points I've mentioned, but frankly, to do so in a sensible way; to do so not just today, but tomorrow and in the future, we need the kind of cooperation that we've seen here today from all of you, from industry, from consumer groups.

We need to keep hearing you. We need you to keep telling us what else we can do to try to make this environment a better and safer environment for consumers and for businesses. So, with that, I would just say thank you very much. Please, please keep in touch with us, keep in touch with our moderators, and let us know what else we should be doing to ensure that consumers can continue to use this wonderful new technology safely and in a way that will benefit the marketplace.

Thank you very much.

(Applause.)

(Whereupon, at 4:49 p.m., the conference was concluded.)

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

DOCKET/FILE NUMBER: P134400

CASE TITLE: MOBILE SECURITY: POTENTIAL THREATS AND SOLUTIONS

DATE: JUNE 4, 2013

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: 6/18/2018

LINDA D. METCALF, CER

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.

SARA J. VANCE, CMRS