Opening Remarks of Chairwoman Edith Ramirez
Federal Trade Commission Mobile Security Forum
Washington, DC
June 4, 2013

Good morning and welcome to the FTC's Mobile Security Forum. It is no exaggeration to say that we are in the midst of a mobile revolution. Today, consumers buy twice as many mobile devices as PCs.[1] Nearly a third of American consumers who use their phones to get to the Internet say it is their primary way of reaching the Web, and we are starting to see the rise of the mobile-only Internet user.[2] In the first quarter of this year, tablets and smartphones accounted for over a fifth of all e-commerce traffic in the United States, compared to only two percent just two years ago.[3] And smartphone users reach for their phones an astonishing 150 times a day on average to do things such as send a text, check email, place a call, surf the Web, or use an app.[4]

Today, though, we will turn away from our addictive smartphones and tablets – or so I hope – to consider the current state of mobile security, potential emerging threats, and the measures industry, government, and consumers can take to protect against risks to the security of our ubiquitous mobile devices.

---

[1] *See* Henry Blodget & Alex Cocotas, *The Future of Mobile*, BUSINESS INSIDER, Mar. 27, 2013, *available at* http://www.businessinsider.com/the-future-of-mobile-slide-deck-2013-3?op=1.

[2] Karen McGrane, *The Rise of the Mobile-Only User*, HARVARD BUSINESS REVIEW, May 28, 2013, *available at* http://blogs.hbr.org/cs/2013/05/the_rise_of_the_mobile-only_us.html; Aaron Smith, *Report of Pew Internet Center: Cell Internet Usage 2012*, June 26, 2012, *available at* http://www.pewinternet.org/Reports/2012/Cell-Internet-Use-2012/Key-Findings.aspx.

[3] *See* Alex Cocotas, *The Unstoppable Rise of Mobile Commerce*, BUSINESS INSIDER, May 22, 2013 (citing Monetate study), *available at* http://www.businessinsider.com/tablets-and-smartphones-ecommerce-share-2013-5.

[4] Liz Gannes, *The Best of Mary Meeker's 2013 Internet Trends Slides*, ALLTHINGSD, May 29, 2013, *available at* http://allthingsd.com/20130529/the-best-of-mary-meekers-2013-internet-trends-slides/.

The FTC's interest in mobile security is an outgrowth of our broad mandate to protect consumers, including 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 have brought a dozen enforcement actions against purveyors of spyware – from rogue ISPs that distributed malware, to companies that installed keystroke loggers that captured sensitive information, to businesses that transmitted nuisance adware that delivered pop-up ads.[5] 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 United States and across the globe.[6] As consumers migrate to smartphones and tablets in record numbers, the FTC is also turning its attention to the security of the mobile environment.

We have three main tools at our disposal – law enforcement, consumer and business education, and policy work, which includes promoting industry dialogue and advocating best practices.

On the enforcement front, the FTC has already begun to address mobile security with its first case in this arena. This February, the Commission alleged that HTC America, the mobile device maker, introduced an array of security vulnerabilities in the course of customizing its

---

[5] *See FTC v. Pricewert, LLC*, No. 09-CV-2407 (N.D. Cal. June 3, 2009); *FTC v. CyberSpy Software, LLC*, No. 08-CV-01872 (M.D. Fla. Nov. 17, 2008); *FTC v. Digital Enters, Inc.*, No. CV-06-4923 (C.D. Cal. Sept. 5, 2007); *In re DirectRevenue LLC*, No. C-4194 (June 26, 2007); *In re Zango, Inc.*, No. C-4186 (Mar. 7, 2007); *FTC v. ERG Ventures, LLC*, No. 3:06-CV-00578-LRH-VPC (D. Nev. Nov. 13, 2006); *FTC v. Enternet Media, Inc.*,CV 05-7777 CAS (C.D. Cal. Aug. 22, 2006); *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. Oct. 5, 2005); *FTC v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wash. Dec. 6, 2005); *In re Advertising.com, Inc.*, No. C-4147 (Sept. 12, 2005); *FTC v. Trustsoft, Inc.*, No. H-05-1905 (S.D. Tex. June 23, 2005); *FTC v. Seismic Enter'mt, Inc.*, No. 04-377-JD (D.N.H. Oct. 12, 2004).

[6] *See* Press Release, *FTC Halts Massive Tech Support Scams* (Oct. 3, 2012) (announcing six cases), *available at* http://www.ftc.gov/opa/2012/10/pecon.shtm; *see also FTC v. Innovative Marketing, Inc.*, No. 08-CV-3233-RDB (D. Md. Sept. 24, 2012) (imposing $163 million judgment).

mobile devices, thereby putting at risk the sensitive information of millions of consumers.[7] We charged HTC with violating the FTC Act's prohibitions on both deceptive and unfair commercial practices.

To resolve the FTC's charges, HTC agreed to establish a comprehensive security program and undergo independent security audits every other year for the next 20 years. Our settlement also includes a provision that is the first of its kind in an FTC order or, to my knowledge, the order of any other U.S. or foreign agency: a requirement that HTC develop and release software patches to fix the vulnerabilities on millions of its devices.

Cases like HTC demand sophisticated technological expertise and tools. To make these cases possible, we have created a forensic mobile lab to allow FTC staff to conduct research and investigations. We have brought in distinguished technologists like Steve Bellovin of Columbia University, and his predecessor, Ed Felten, of Princeton University. And we have created a Mobile Unit to ensure that the FTC is alert to mobile issues in *all* its consumer protection work.

As to the FTC's second tool – consumer and business education – the good news is that a number of you here with us today already offer a variety of innovative technologies, some of which are free, to help users secure their mobile devices and the data on them. But there is still work 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 to do that.[8] For consumers, the FTC offers extensive materials to help them stay safe and secure

---

[7] See Press Release, *HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers* (Feb. 22, 2013), *available at* http://ftc.gov/opa/2013/02/htc.shtm.

[8] See FTC Business Center, *Mobile App Developers: Start with Security* (Feb. 2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

whether on their home computer or 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.

With today's forum, the FTC is continuing its policy work in the mobile sphere. In the past year, the FTC has hosted roundtables exploring mobile cramming, mobile payments, and mobile privacy and advertising disclosures. This series of policy dialogues devoted to mobile reflects the high priority we place on ensuring that the FTC itself, industry, consumers groups, and other stakeholders are 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 discussion. Mobile devices depend on many different players – including device manufacturers, chipset makers, app stores, app developers – and each serves a unique but critical function in the user experience. So I am especially pleased to have such excellent representation from businesses across the complex mobile ecosystem. I appreciate your willingness to share your expertise on this important topic and 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 is no room for complacency about the need to keep the mobile environment safe and secure. My hope is that our discussion today will inspire action, encourage innovation, and engage each of us in that common cause.

We will begin the dialogue with an overview of the mobile ecosystem from Steve Bellovin, the FTC's Chief Technologist. Steve is a renowned expert on network security. The

FTC is very fortunate to have him with us this year, and also here this morning to lay the groundwork for today's program.

But before I hand the program over to Steve, I want to thank you all again for attending. I also want to extend special thanks to the FTC team who put on today's event, including Emily Burton, Colleen Robbins, Dan Salsburg, Nithan Sannappa, and Paul Ohm.

And now, please join me in welcoming Steve Bellovin.