Before the
Federal Trade Commission
Washington, DC

In re	
Mobile Security Project	Project No. P145408

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

In response to the Federal Trade Commission's ("FTC" or "the Commission") call for comments on April 17, 2014[1] requesting further comment on the June 4, 2013 forum on mobile security ("the 2013 forum"),[2] the Computer & Communications Industry Association ("CCIA") submits the following comments.

CCIA is an international nonprofit association representing a broad cross section of computer, communications, and Internet industry firms. CCIA remains dedicated, as it has for over 40 years, to promoting innovation and preserving full, fair, and open competition throughout our industry. Our members employ more than 600,000 workers and generate annual revenues in excess of $465 billion.[3]

I. An analysis of the risks of mobile devices and apps must also take into account the immense benefits for consumers.

CCIA commends the FTC for this timely inquiry into potential threats that may cause concrete harms to consumers, but urges that the Commission also keep in mind the myriad benefits of mobile devices and apps for consumers.

Mobile platforms enable innovative methods of communication, research, and entertainment that enrich and enhance the lives of citizens. Just this week, Kleiner Perkins Caufield & Byers partner Mary Meeker's annual report on Internet trends emphasized the growth of mobile, with mobile now accounting for 25 percent of web usage globally, up from 14 percent

[1] *See* http://www.ftc.gov/news-events/press-releases/2014/04/ftc-invites-further-public-comment-mobile-security.
[2] FTC, *Mobile Security: Potential Threats and Solutions* (2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions.
[3] A list of CCIA's members is available online at http://www.ccianet.org/members.

last year.[4] Mobile products and services have also revolutionized the way individuals and small businesses engage in commerce, creating new jobs and disrupting industries in tech and non-tech sectors. Mobile payments are projected to reach $1.3 trillion annually by 2017,[5] and in the food truck industry alone, which generally relies on mobile payment systems to accept credit cards, many diverse jobs have been created.[6]

Mobile apps help companies customize the consumer experience, and better tailor their products and services. Specifically regarding mobile payment systems, consumers benefit from features on these services that help them monitor finances and control spending, and that also provide increased context—and often increased security—to a transaction.[7] As CCIA explained in our mobile device tracking comments to the FTC several months ago, innovation in mobile retail technologies "can allow brick-and-mortar stores to more effectively compete with online retailers by, for example, bringing some of the benefits of online marketplaces to the physical space. Location data can help enable seamless checkout, personalized and efficient staffing, and less congested retail stores many of the hallmarks of online shopping giving offline retailers a new way to battle for shoppers' time and money."[8] Additionally, these technologies demonstrably help stop theft.[9]

II. Only a very small percentage of malware has been detected on mobile devices.

While the mobile malware threat is real and growing, it is not as substantial as many reports have made it seem by leaving out context. One of the participants at the 2013 forum, Patrick Traynor from Georgia Tech, conducted research with data from a major cellular ISP and

---

[4] Vindu Goel, *State of the Internet: Still Growing but More Mobile Than Ever*, N.Y. TIMES, May 28, 2014, *available at* http://bits.blogs.nytimes.com/2014/05/28/state-of-the-internet-still-growing-but-more-mobile-than-ever/.

[5] *See* Juniper Research, *Press Release: Mobile Payments to Reach $1.3tn Annually by 2017, as NFC and Physical Goods Sales Accelerate*, Hampshire, UK, Aug. 15, 2012, *available at* http://www.juniperresearch.com/viewpressrelease.php?pr=332.

[6] *See* Ben Worthen, *Businesses Catch a Ride on the Boom in Food Trucks*, WALL. ST. J., Jan. 16, 2013, *available at* http://online.wsj.com/news/articles/SB10001424127887324734904578241741879961644 (detailing the many jobs created by food trucks, which generally rely on mobile payment systems to accept credit cards).

[7] *See generally* Fumiko Hayashi, *Mobile Payments: What's in It for Consumers?*, Federal Reserve Bank of Kansas City, ECON. REV., First Q. 2012, 35, *available at* http://www.kansascityfed.org/publicat/econrev/pdf/12q1Hayashi.pdf.

[8] CCIA, In the Matter of *Mobile Device Tracking Request for Comments*, FTC, Mar. 19, 2014, *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/03/00020-89127.pdf.

[9] Jennifer Goforth Gregory, *5 Ways Tech Is Stopping Theft*, Entrepreneur, Nov. 7, 2013, *available at* http://www.entrepreneur.com/article/229674.

found 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."[10] He explained that despite reports to the contrary, "from the network perspective, we don't see infection happening all that often."[11]

Another panelist from the 2013 forum, Lookout's Derek Halliday, put his data in context, explaining that he saw that only 1.25 percent of U.S. Android users have encountered a bad app in 2012, which is "actually a pretty small chance of encountering malware in the U.S.," adding that when considering raw totals that might sound large, it's important to remember that "smartphone penetration is pretty impressive in the U.S."[12]

The mobile security threat was put in context in another way at the 2013 forum by panelist Gareth Maclachlan of AdaptiveMobile, who explained that there are a limited amounts of threats, and that the number of viruses reported is often artificially multiplied beyond the actual threat:

> 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.*[13]

A recent Blue Coat Systems report also found that mobile malware remains a limited threat, remarking that "[g]iven the proliferation of the devices and the roughly 1.5 billion new ways to steal data, passwords or money, it is, perhaps, surprising that the mobile malware problem isn't more widespread."[14] The report also explained that "[t]he malware threats targeting mobile devices are still pretty basic – largely confined to potentially unwanted

---

[10] Transcript of FTC, *Mobile Security: Potential Threats and Solutions* (2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/mobile-security-potential-threats-solutions/30604mob_0.pdf (hereinafter "2013 Forum Transcript"), at 55.

[11] 2013 Forum Transcript at 56-57.

[12] 2013 Forum Transcript at 269.

[13] 2013 Forum Transcript at 34-35 (*emphasis added*).

[14] Blue Coat Systems, *2014 Mobile Malware Report: A New Look at Old Threats* (2014), *available at* http://images.machspeed.bluecoat.com/Web/BlueCoat/%7B1bf5b2de-4d3c-4be0-94c6-48eded2b6752%7D_report-mobilemalware-fn.pdf, at 3.

applications and premium SMS scams."[15] Similarly, Verizon's recent data breach investigations report found that less than 1% of crimeware occurs on mobile.[16]

III. Consumer education is an important tool for reducing the spread of mobile malware.

Omar Khan of NQ Mobile explained at the 2013 forum that social recommendation aspects and self-regulating environments of major app marketplaces have been found to be extremely effective; consumers can look at how apps are rated, and how many times they were downloaded, and avoid potentially malicious applications.[17] There seemed to be a general consensus among the panelists that larger sources of apps like Apple's App Store and Google Play are relatively secure; third-party app ecosystems and app delivery via websites or SMS are a greater source of problems.

Panelists at the 2013 forum emphasized that there are things that consumers can do and not do to avoid mobile malware, with Maclachlan explaining "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."[18] Halliday said that the number one thing that can be done now is consumer education and empowerment, raising awareness of what they can do to protect themselves, even things as seemingly basic as passwords.[19] He also put it in context, explaining that "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."[20]

IV. The Commission should conduct a broader inquiry than just mobile, considering that most of the data security issues this year were not mobile.

Mobile malware is substantially less common than PC malware. A recent SophosLabs report explained that the amount of malware they have seen is "a tiny fraction of the number of

---

[15] *Id*. at 7.

[16] Verizon, *2014 Data Breach Investigations Report* (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf, at 33.

[17] 2013 Forum Transcript at 27-28.

[18] 2013 Forum Transcript at 34-35.

[19] 2013 Forum Transcript at 272.

[20] 2013 Forum Transcript at 287.

pieces of malware out there for the traditional PC."[21] A recent F-Secure report agreed, finding that "[c]ompared to PC-based threats, the number of mobile malware is miniscule."[22]

F-Secure's Mikko Hypponen, a panelist at the 2013 forum, supported these findings, saying that "there's much less mobile phone malware than PC malware,"[23] and that while "we also do have a problem with mobile malware, but it's nowhere near [the PC malware problem]. Nowhere near. In fact, you could say that mobile security is a success story."[24] He added that "[t]he problem is very limited. It's unlikely still to run into mobile malware. It's much more likely to run into PC malware."[25]

To the extent that the FTC wants to focus on malware harming consumers, it should consider broadening the scope of this investigation beyond mobile.

V. The Commission should ensure that attempts to police the mobile ecosystem don't stifle innovation and competition.

The Commission can protect and promote privacy in the mobile space without slowing innovation by focusing on demonstrated harms and balancing its concerns about the mobile ecosystem against mobile's many benefits to consumers. Evidence-based policy must be favored over government intervention in any nascent industry based on merely speculative harms.

The greater the ex-ante compliance costs a security regime imposes, the higher the barriers to entry for new players. Considering one of the great strengths of the mobile app ecosystem is the diverse number of players and sources of innovation, a thorough cost-benefit analysis of new regulation is essential. There are 275,000 registered iOS developers in the United States,[26] and more than 450,000 registered Android developers,[27] and many of them operate as individuals or small businesses, which are especially susceptible to ex-ante costs.

---

[21] SophosLabs, *Sophos Mobile Security Threat Report* (2014), *available at* http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf, at 1.

[22] F-Secure, *Mobile Threat Report for Q1 2014* (2014), *available at* http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014_print.pdf, at 3.

[23] 2013 Forum Transcript at 276.

[24] 2013 Forum Transcript at 278.

[25] 2013 Forum Transcript at 279.

[26] Apple, Job Creation, *available at* http://www.apple.com/about/job-creation.

[27] Lauren Darcey & Shane Conder, *Android Wireless Application Development Volume I: Android Essentials* (2012), *available at* http://books.google.com/books?id=5qHBnd58ybAC&pg=PA22#v=onepage, at 22.

It is inadvisable to make the growing mobile industry operate under legal uncertainty, which threatens to reduce investment in the mobile ecosystem. Any regulation, enforcement, and advocacy in this space should be mindful of not deterring mobile innovation.

May 30, 2014

Respectfully submitted,

Ali Sternburg
Public Policy & Regulatory Counsel
Dan O'Connor
Senior Director,
Public Policy & Government Affairs
Computer & Communications
Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070