



**May 30<sup>th</sup> 2014**

**RE: Mobile Security Project, Project No. P145408**

**To: The Federal Trade Commission**

CTIA respectfully submits the attached comments regarding the FTC's request for further public comment on Mobile Security; Project No. P145408 dated April 17<sup>th</sup> 2014. The comments represent the efforts of the CTIA's Cybersecurity Working Group (CSWG) which is comprised of industry experts in the field of mobile security.

Should there be any questions regarding the comments provided or clarification needed, please do not hesitate to let us know.

Yours truly,

/Michael Altschul/

Michael Altschul  
Senior Vice President, General  
Counsel

/John A. Marinho/

John A. Marinho  
Vice President, Technology and  
Cybersecurity

Copy to:  
Nithan Sannappa

**CTIA-The Wireless Association  
Cybersecurity Working Group (CSWG)**

---

**Comments to  
The Federal Trade Commission  
Mobile Security Project, Project No. P145408**

---

**Submitted May 30, 2014**

## TABLE OF CONTENTS

I.	INTRODUCTION AND EXECUTIVE SUMMARY.....	1
II.	SECURITY IS CRITICAL TO THE MOBILE INDUSTRY, WHICH HAS BEEN SUCCESSFULLY USING A MULTILAYERED APPROACH.....	2
	A.    The global mobile ecosystem is constantly innovating to provide consumers security tools as they interact with varied participants. ....	2
	B.    Mobility has driven economic growth and major changes to economy. ....	4
	C.    Industry and international standards groups are innovating on security, with important benefits for consumers.....	5
III.	FEDERAL AGENCIES SHOULD SUPPORT CONSUMER AWARENESS AND EMPOWERMENT TO PROMOTE INNOVATION. ....	7
	A.    CTIA encourages the FTC to focus on consumer protection and education, and emphasize the power of consumer choice to drive innovation. ....	7
	B.    Ongoing industry and government efforts on mobile cybersecurity continue to flourish. ....	8
IV.	THE FTC’S INQUIRIES SPAN MUCH OF THE MOBILE ECOSYSTEM.....	9
	A.    Each layer of the mobile ecosystem is working to ensure mobile security. ....	9
	B.    FTC Interest: Secure Platform Design.....	10
	C.    FTC Interest: Secure Distribution Channels.....	13
	D.    FTC Interest: Secure Development Practices.....	19
	E.    FTC Interest: Device Security and Updates.....	21
V.	CONCLUSION.....	24

## I. INTRODUCTION AND EXECUTIVE SUMMARY

CTIA—The Wireless Association® (“CTIA”) submits these comments in response to the Federal Trade Commission’s (“FTC” or “Commission”) request for public comment on mobile security.<sup>1</sup> CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Its membership spans the industry and includes carriers, manufacturers, operating systems (“OS”) and mobile application (“app”) developers.<sup>2</sup> The mobile marketplace is competitive, complex, and constantly innovating. Mobility has revolutionized our economy and our way of life.

Following up on its 2013 public mobile security workshop,<sup>3</sup> the FTC is exploring mobile security, particularly the areas of secure platform design, distribution channels, development practices, and so-called “security lifecycles” and updates.<sup>4</sup> CTIA’s comments explain the various components of the mobile security landscape. Section II describes the complex, global wireless ecosystem, its importance to the U.S. economy, and how industry is effectively addressing mobile security through voluntary, multi-stakeholder efforts. Section III encourages the FTC to focus mobile security efforts on consumer education and empowerment, rather than on device or network design or operation, and to allow industry and government efforts already underway to continue. Finally, Section IV addresses particular areas of the FTC’s inquiry into platform development, distribution, application development, and the interaction between security and product lifecycle.

In these comments, CTIA offers some key insights:

- **Mobile security involves every part of the ecosystem; no one layer is more critical or responsible than another.** Mobile security requires vigilance, innovation and cooperation. Network operators, device manufacturers, software companies, application/content developers, and end users are engaged in a virtuous cycle with support from government, private security specialists, and academia. Security is not achieved by finding an ideal hardware configuration or relying on one type of communications network to catch all threats. In a dynamic market, operating systems, applications, devices, and networks impact security in changing ways. No one layer can be expected to “fix” mobile security and no one part can shoulder principal responsibility.
- **Consumers are key partners in mobile security.** Reflecting consumers’ changing desires, the mobile marketplace is incredibly diverse. Consumers use and access mobile services and content in various ways. They choose among hundreds of devices

---

<sup>1</sup> See Press Release, FTC Invites Further Public Comment on Mobile Security (Apr. 17, 2014), *available at* <http://www.ftc.gov/news-events/press-releases/2014/04/ftc-invites-further-public-comment-mobile-security>.

<sup>2</sup> More information about CTIA is available on the Association’s website at [www.ctia.org/aboutCTIA](http://www.ctia.org/aboutCTIA).

<sup>3</sup> See FTC Conference, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), *available at* <http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions/> (“2013 Workshop”).

<sup>4</sup> *Id.*

and varied operating systems, they regularly switch between carriers, they access unsecured Wi-Fi networks, and they select from millions of applications across varied channels. They can modify devices and select their own apps. All of this empowerment has consequences for security, because the cybercriminals are also constantly innovating. Consumer choices—even an innocent click on a bad link—can expose devices and information to different threats, so consumers are vital to mobile security.

- **The FTC can promote consumer empowerment and work to ferret out bad actors.** Overall, mobile security is a success story. As explained below, the United States’ mobile malware infection rates are low—far below those in other countries. The market is responding to evolving consumer preferences to develop solutions, provide information, and help consumers determine the security measures that are right for them. The government can help industry build on this success. Regulation or standards would stifle security innovation and counterproductively provide a roadmap for bad actors. The FTC can help consumers and the ecosystem by investigating the purveyors of malware and unscrupulous application developers who intentionally deceive and defraud consumers.

CTIA looks forward to helping the FTC and other agencies gain insight about how the mobile ecosystem works together to address security and constantly developing industry activities in the area of mobile security.

## **II. SECURITY IS CRITICAL TO THE MOBILE INDUSTRY, WHICH HAS BEEN SUCCESSFULLY USING A MULTILAYERED APPROACH.**

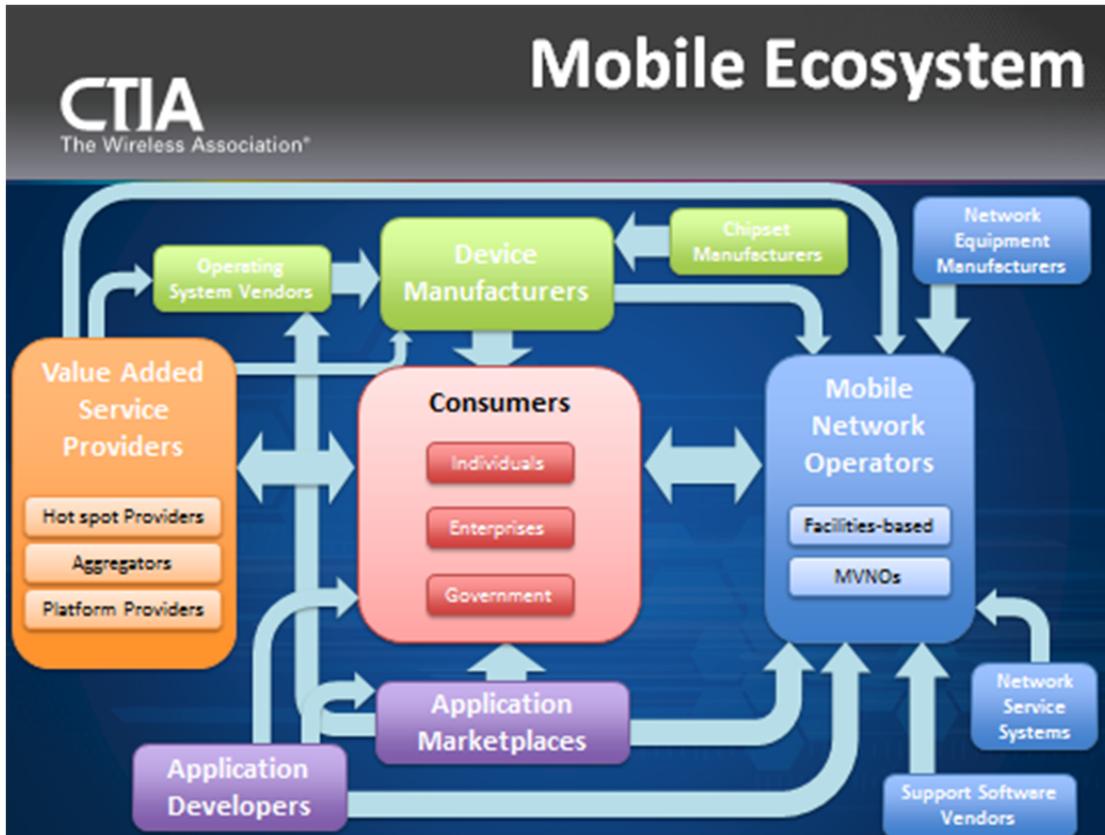
### **A. The global mobile ecosystem is constantly innovating to provide consumers security tools as they interact with varied participants.**

The number and diversity of players in the wireless ecosystem have grown dramatically.<sup>5</sup> The ecosystem is composed of such varied parties as chip and handset manufacturers, operating system vendors, application marketplaces, application developers, mobile network operators, value-added service providers, and consumers. Assorted mobile network operators, both facilities-based and virtual operators, render mobile services to consumers. Network operators are supported by network service systems, network equipment manufacturers, and support software vendors. Carriers each support hundreds of different devices manufactured by dozens of manufacturers. Those manufacturers, or “OEMs,” deploy multiple operating systems (*e.g.*, Android, BlackBerry, iOS, Symbian, Windows, etc.) created by operating system vendors. Supporting OEMs are chipset manufacturers, who develop and manufacture mobile device integrated circuits. Myriad application and content developers build and publish diverse applications. Applications are available in numerous applications marketplaces or through

---

<sup>5</sup> See CTIA, *Today’s Mobile Cybersecurity: Protected, Secured and Unified 7*, available at <http://www.ctia.org/docs/default-source/default-document-library/today-s-mobile-cybersecurity-protected-secured-and-unified.pdf?sfvrsn=0> (“First CTIA White Paper”).

mobile network operators, often in an over-the-top (“OTT”) scenario.<sup>6</sup> There are different methods of connecting, as well, with Wi-Fi being an alternative to the mobile carrier network. Value added service providers include service aggregators, Wi-Fi-hotspot providers, and other platform providers that can render services to consumers directly or through the mobile network operator. This diagram illustrates the complexity of the mobile ecosystem:



The mobile marketplace is vibrant, giving consumers a great deal of choice in network providers, devices, OSs, and applications. As a result, consumers have varied relationships with different layers of the ecosystem, and those relationships shift over time. Consumers can purchase new or refurbished devices from OEMs, carriers, or third parties. They can choose between operating systems. They may obtain voice or data service through a carrier on a post-paid or prepaid basis, and may move their device between carriers. In the course of owning and using devices, consumers may access wireless service from Wi-Fi networks, and purchase and download apps—from games to financial programs to security solutions—from curated app stores<sup>7</sup> or from third parties. End users sometimes decide to “root” or “jailbreak” their device or sideload applications. Many consumers store data in cloud environments and use their devices in Bring-Your-Own-Device (“BYOD”) enterprise environments where system operators can help

<sup>6</sup> Over-the-top (“OTT”) refers to delivery of video, audio, and other media over the Internet without a multi-system operator (“MSO”) being involved in the control or distribution of content. Well-known examples of OTT services include Netflix and Hulu.

<sup>7</sup> Throughout, CTIA uses the term “curated app store” to refer to security curation/monitoring for either first-party or third-party app stores, and includes both automated and manual curation.

manage security. Consumers' experiences and relationships are far from static. In such a layered and fluid ecosystem, consumers do not have one single point of contact or vendor relationship.

## **B. Mobility has driven economic growth and major changes to economy.**

The mobile ecosystem has grown at a rapid pace. Global mobile traffic grew 81 percent in 2013 reaching 1.5 exabytes per month—up from 820 petabytes per month in 2012.<sup>8</sup> The U.S. wireless industry is valued at \$195.5 billion. There are currently more active mobile devices in the U.S. than there are people, with wireless penetration at more than 102 percent.<sup>9</sup> As mobile service has become ubiquitous, its uses have expanded beyond mere voice to data and countless services and functions. More than 89 percent of U.S. inhabitants have mobile broadband subscriptions.<sup>10</sup>

Not surprisingly, growth in applications also has been extraordinary. Analysts estimate that between 56 and 82 billion apps were downloaded in 2013, and there could be as many as 200 billion apps downloaded in 2017.<sup>11</sup> The U.S. app economy employs 725,000 developers and related jobs, and has grown by around 40 percent since 2012.<sup>12</sup> Analysts estimate that app revenues were \$20-25 billion globally in 2013—a statistic that could triple by 2017.<sup>13</sup>

The rise of mobile phone and smartphone technology has radically changed how Americans connect, communicate, and manage data. With the increasing growth of the Internet of Things and a shift towards BYOD, mobility will continue to present opportunities and challenges.

---

<sup>8</sup> Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018, *available at* [http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white\\_paper\\_c11-520862.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html).

<sup>9</sup> See CTIA, *Wireless Quick Facts*, *available at* <http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts> (last accessed May 27, 2014) (reporting wireless penetration of 102.2% as of year-end 2012).

<sup>10</sup> See *id.*

<sup>11</sup> See *Global Mobile Statistics 2013 Section E: Mobile Apps, App Stores, Pricing and Failure Rates*, mobiThinking.com (May 2013), *available at* <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/e>.

<sup>12</sup> See Progressive Policy Institute, *752,000 App Economy Jobs on the 5th Anniversary of the App Store* (July 8, 2013), *available at* <http://www.progressivepolicy.org/2013/07/752000-app-economy-jobs-on-the-5th-anniversary-of-the-app-store/>.

<sup>13</sup> See *Global Mobile Statistics 2013 Section E: Mobile Apps, App Stores, Pricing and Failure Rates*, mobiThinking.com (May 2013), *available at* <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/e>. Industry does not and cannot rest in the face of security threats. Threats to new and existing technology are constantly evolving. To be effective in today's mobile economy, policy must support nimble, real-time solutions that evolve as threats continue to rapidly change. In addition, security solutions are complex and highly technical. Policy makers must recognize and encourage this innovation and flexibility, and allow technical experts to solve security-related problems.

**C. Industry and international standards groups are innovating on security, with important benefits for consumers.**

The entire wireless industry is engaged on mobile cybersecurity and collaborates on improvements to stay a step ahead of bad actors. For example, CTIA members have formed the CTIA Cybersecurity Working Group (“CSWG”) which works toward the shared goal of delivering advanced cybersecurity to all users. It has over thirty-five members and includes key players and innovators across the wireless ecosystem. In addition, CTIA works directly with government and industry bodies to promote innovation and coordinated solutions.<sup>14</sup>

The CSWG has published several white papers on mobile security best practices. “Today’s Mobile Cybersecurity: Protected, Secured and Unified” provides a brief overview of the cybersecurity landscape of the mobile communications industry, the extent of its interdependence in responding to an environment of rapidly changing threats, a summary of the many cybersecurity features and solutions at work today, and a sampling of the many advanced protections available for device users.<sup>15</sup> “Today’s Mobile Cybersecurity: Blueprint for the Future” provides an overview of trends in mobile usage and threats, and shows how this analysis is reflected in the industry’s blueprint for ongoing cybersecurity investigation and technical improvements under study.<sup>16</sup> “Today’s Mobile Cybersecurity: Industry Megatrends & Consumers” provides an overview of how innovations in information technology are impacting mobile cybersecurity.<sup>17</sup> And, “Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication” addresses how stakeholders secure the Internet of Things and encourage continued innovation in this field while protecting consumers’ data.<sup>18</sup>

Industry supports international activities that aim to promote security. A host of international standards bodies actively produce and update a wide variety of mobile security standards upon which industry relies. Various industry standards-setting organizations, such as 3GPP, the Internet Engineering Task Force, the Alliance for Telecommunications Industry Solutions, and the IEEE, demonstrate the ongoing commitment to advance the state of the art for

---

<sup>14</sup> For example, CTIA’s Vice President of Cybersecurity and Technology, John Marinho, facilitates the CSWG and participated in the FTC’s panel on “Extending Security Through the Mobile Ecosystem” at the FTC’s June 4, 2013 Workshop. CTIA regularly meets with the FCC, FTC, NIST and others interested in mobile and cybersecurity.

<sup>15</sup> See First CTIA White Paper.

<sup>16</sup> See CTIA, *Today’s Mobile Cybersecurity: Blueprint for the Future*, available at [http://files.ctia.org/pdf/Cybersecurity\\_White\\_Paper\\_2.pdf](http://files.ctia.org/pdf/Cybersecurity_White_Paper_2.pdf) (“Second CTIA White Paper”).

<sup>17</sup> See CTIA, *Today’s Mobile Cybersecurity: Industry Megatrends & Consumers*, available at <http://www.ctia.org/docs/default-source/default-document-library/today-s-mobile-cybersecurity-industry-megatrends-amp-consumers.pdf?sfvrsn=0> (“Third CTIA White Paper”).

<sup>18</sup> See CTIA, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication*, available at <http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf> (“Fourth CTIA White Paper”).

mobile cybersecurity.<sup>19</sup> GSMA is working with 3GPP to develop a certification scheme for devices and products that meet 3GPP's security standards.

These industry efforts promote innovation and experimentation, so that security solutions evolve in response to the threat environment. As a result, many security solutions are available in the market. In addition to network operators providing security for communications transmission, network operators and platforms promote to consumers a wealth of optional tools that they can use to improve security and data protection for information that resides on the smartphone or tablet.<sup>20</sup> Such tools include device management capabilities, anti-theft, anti-malware, browsing protection, app reputation checking, call/SMS blocking and scanning, and firewalls. Similar to how security needs are addressed in the physical environment and the desktop, network service operators, platforms, and device manufacturers provide consumers with a choice of security tools that empower them to protect their devices and their information. The industry's competitive environment works in favor of advancing cybersecurity because each player understands the advantages of marketing products and services that deploy security solutions consistent with consumer demand; this provides choice and diversity.

Despite the number of industry players providing security solutions in the mobile ecosystem, consumers are in control of much of their mobile experience. As consumers have become more dependent on mobile devices, they have become more confident and empowered to adapt technology to suit their needs. Consumers have become critical gatekeepers when it comes to mobile security. Whether by choosing not to use passwords, downloading apps from insecure sites, or using their device on an unsecured Wi-Fi network, consumers—often unwittingly—can dramatically affect even the most “secure” device or network and make it easier for attackers to succeed.

Consumer awareness and choice are therefore essential. Consumers have access to a vast array of mobile security information from many different sources, including news reports, blogs, public and private consumer education, and others. In addition, industry educates consumers by providing tips, tools, and guides for best practices. Advice covers security at every stage, from

---

<sup>19</sup> See, e.g., 3GPP SA WG3 Home, available at <http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security/home> (stating that 3GPP's SA WG3 is “responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architecture and protocols”); The IETF Security Area Homepage, available at <http://trac.tools.ietf.org/area/sec/trac/wiki> (stating that the Security Area relates to Internet Security and is also concerned with “the appropriate application of security mechanisms in protocols developed by working groups in other Areas of the IETF”); ATIS Standards & Solutions, Committees & Forums, available at <http://www.atis.org/committees/index.asp> (describing several ATIS committees focused on cybersecurity issues); 35th IEEE Symposium on Security and Privacy, available at <http://www.ieee-security.org/TC/SP2014/> (the annual IEEE Symposium on Security and Privacy is an important forum for presenting developments in computer security and electronic privacy, and for bringing together research and practitioners in the field); IEEE Roundup, *A Look Inside IEEE Xplore: Cybersecurity* (Aug. 7, 2013), available at <http://theinstitute.ieee.org/ieee-roundup/opinions/ieee-roundup/a-look-inside-ieee-xplore-cybersecurity-> (highlighting IEEE resources on cybersecurity); see also CTIA, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication 19*, available at <http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf> (highlighting the many additional industry, international, and public-private partnerships that are working to advance cybersecurity best practices).

<sup>20</sup> See, e.g., Android Official Blog, *Expanding Google's Security Services for Android* (Apr. 10, 2014), available at <http://officialandroid.blogspot.com/2014/04/expanding-googles-security-services-for.html>.

how to configure devices to be more secure to how to check permissions and understand the security (or lack thereof) found on different types of apps and networks. Industry, including platform providers and application developers, continually works to make the loading of applications and software permissions more intuitive and easier to understand. For example, by following the CTIA Cybersafety Tips, consumers can actively help protect themselves and their data.<sup>21</sup> Consumers are empowered and have many choices. They should continue to drive security through market choices.

Industry efforts, from technology to awareness, have borne fruit. The mobile malware infection rate in United States is very low—estimated at between 0.5 and 2%; far better than overseas where malware infection rates are orders of magnitude higher and application stores can be severely compromised.<sup>22</sup> As made clear at the FTC’s 2013 Workshop, different actors in the ecosystem are producing diverse security solutions. We see constant innovation in security applications, app stores, and device manufacturing and support, both by existing players and new entrants focused on security. This innovation will continue to meet consumer demand in different ways.

### **III. FEDERAL AGENCIES SHOULD SUPPORT CONSUMER AWARENESS AND EMPOWERMENT TO PROMOTE INNOVATION.**

#### **A. CTIA encourages the FTC to focus on consumer protection and education, and emphasize the power of consumer choice to drive innovation.**

As the nation’s consumer protection agency, the FTC is positioned to support consumer awareness of the choices available to them to protect their data and devices. By emphasizing consumer choice, the FTC will further drive market innovations for mobile security. Working with international law enforcement and mobile industry partners, the FTC can continue to address malware, fraud, and consumer deception, taking action against bad actors.

The Federal Communications Commission’s (“FCC”) light regulatory touch has allowed the mobile ecosystem to thrive while still ensuring that consumers have choices. Heeding Congress’s direction that wireless be left to develop largely free from regulation, the FCC has helped promote a dynamic and innovative marketplace, with robust, market-driven security solutions.<sup>23</sup> The FCC has “worked to foster a climate for innovation and investment” and “promoted competition to drive wireless innovation.”<sup>24</sup> FCC policies “support regulatory

---

<sup>21</sup> CTIA, *Cybersafety Tips*, available at <http://www.ctia.org/your-wireless-life/consumer-tips/tips/cybersafety-tips> (“CTIA Cybersafety Tips”).

<sup>22</sup> See *infra* at 18-19, 25.

<sup>23</sup> See, e.g., *Implementation of Sections 3(n) and 332 of the Communications Act*, FCC Docket No. 94-212, Third Report and Order, 9 FCC Rcd. 7988, 8004 (¶ 29) (Rel. Sept. 23, 1994) (explaining that the “overarching congressional goal” was to “promot[e] opportunities for economic forces – not regulation – to shape the development” in the wireless market).

<sup>24</sup> *Prepared Remarks of FCC Chairman Julius Genachowski to University of Pennsylvania – Wharton* (Oct. 4, 2012), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-316661A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-316661A1.pdf) (“Genachowski UPenn Remarks”).

frameworks that are pro-competitive, transparent and technology-neutral”<sup>25</sup> with the flexibility for wireless providers “to deploy the network technologies and services they choose.”<sup>26</sup> The FTC likewise can promote market-driven security innovations.

Government efforts to influence mobile security solutions through regulation or standards could be counterproductive. The market is responding to evolving threats and consumer needs with innovation. The private sector develops cutting-edge solutions based on industry-wide best practices, collaborative efforts, codes of conduct, as well as their organizations’ needs and capabilities. Standardization of security solutions—through regulation or government preferences—could stunt responses to evolving threats, and provide a roadmap for bad actors.<sup>27</sup> The FCC’s Technical Advisory Council has noted that “standardization” of mobile device operating systems benefitted bad actors by helping them focus attacks.<sup>28</sup> Industry functions well because it is free to address mobile security as the market demands and technology allows. It would be a challenge for federal agencies to keep pace with the rapid evolutions that occur in mobility and cybersecurity in particular. Well-intentioned efforts to identify and promote particular approaches might inadvertently stifle innovation and better security solutions.

The FTC should support consumer choice and promote continued innovation in technology, platforms, and distribution methods, all of which work together to address security. CTIA knows from experience that the many players in the ecosystem develop their own models, and work together to secure the various layers of the mobile segment. Each layer is critical. Whether it is OS developers, manufacturers, carriers, or application developers, each segment complements each other and contributes to a layered approach to security. Consumers are provided with myriad choices as they interact with each layer of the wireless marketplace, and those choices drive further innovation, both in terms of technological solutions and available information. Together, the ecosystem is continually improving security.

## **B. Ongoing industry and government efforts on mobile cybersecurity continue to flourish.**

Ongoing, collaborative, and voluntary activity on cybersecurity will further strengthen the security of wireless networks, devices, and systems. This model, if properly supported, promises to yield timelier, flexible solutions than any top-down regulatory approach. The President’s Executive Order (“EO”) and Presidential Policy Directive (“PPD”) on cybersecurity make clear that cybersecurity efforts must be voluntary.<sup>29</sup> Industry has the expertise and

---

<sup>25</sup> See Federal Communications Commission, *Connecting America: The National Broadband Plan*, at 60 (2010) (“*National Broadband Plan*”).

<sup>26</sup> See *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993*, WT Docket No. 10-133, Fifteenth Report, 26 FCC Rcd. 9664, 9734 (¶ 106) (Rel. June 27, 2011) (“Fifteenth Report”).

<sup>27</sup> See Second CTIA White Paper.

<sup>28</sup> FCC Technological Advisory Council (“TAC”) Security & Privacy Working Group, *Longer Term Anti-Malware Recommendations 2* (Dec. 10, 2012), available at <http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting121012/TAC-WS&P-anti-malware-recommendations.pdf>.

<sup>29</sup> See Executive Order, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), available at <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>; Presidential Policy Directive-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013),

incentive to adopt reasonable and appropriate security measures. As directed by the EO and PPD, the National Institute of Standards and Technology's ("NIST") Framework was released on February 12, 2014.<sup>30</sup> CTIA and representatives of the mobile ecosystem actively participated in the Framework process.<sup>31</sup>

In the wake of the NIST Framework, the wireless and communications industries are focused on aligning industry with the Framework through voluntary activity, including through the FCC's Communications Security, Reliability, and Interoperability Counsel's ("CSRIC") Working Group 4.<sup>32</sup> Those efforts are substantial and ongoing, and represent an effort to improve cybersecurity across all platforms and segments of the mobile ecosystem. CTIA has been actively engaged in the FCC's process, offering comment on developing cybersecurity certification regimes and other topics.<sup>33</sup>

#### **IV. THE FTC'S INQUIRIES SPAN MUCH OF THE MOBILE ECOSYSTEM.**

##### **A. Each layer of the mobile ecosystem is working to ensure mobile security.**

The FTC expresses interest in platform design, distribution channels, application development, and the so-called "security lifecycle" of mobile devices. Each relates to a layer of the global mobile ecosystem and is influenced by entities large and small around the world. Particularly in a BYOD environment, hardware and software best practices contribute to, but do not alone determine, mobile security. For mobile devices, ultimate security decisions often rest with end users. Informed users exercising caution have a key role to play in managing cybersecurity risks.

The FTC's 2013 Workshop illustrated varied approaches being used in this diverse, global, and fast-paced industry. As CTIA has consistently stated, existing security approaches are flexible and holistic, customized to the particular device or platform to secure the system and shape user behavior. Comprehensive solutions implicate almost every aspect of the mobile "system of systems," including: device provisioning and reprovisioning, Mobile Device Management ("MDM") software, enterprise systems, Help Desk solutions, device

---

available at <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

<sup>30</sup> National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 1 (Feb. 12, 2014), available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf> ("NIST Cybersecurity Framework").

<sup>31</sup> See e.g., Comments of CTIA – The Wireless Association, the National Cable & Telecommunications Association and the U.S. Telecom Association on the Preliminary Cybersecurity Framework Released by the National Institute of Standards and Technology, Docket No. 130909789-3789-01 (Dec. 13, 2013), available at <http://www.ctia.org/docs/default-source/Legislative-Activity/12-13-13-nist-comments-final-clean.pdf?sfvrsn=0>.

<sup>32</sup> The CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. The CSRIC's Working Group 4 focuses on cybersecurity best practices.

<sup>33</sup> See e.g., generally Comment of CTIA-the Wireless Association, *Cyber Security Certification Program*, PS Docket No. 10-93 (July 12, 2010), available at <http://www.ctia.org/docs/default-source/fcc-filings/ctia-files-comments-to-fcc-s-cyber-security-certification-program-noi.pdf?Status=Master&sfvrsn=0>.

manufacturing, OS platforms, application developers, and security platforms.<sup>34</sup> Critically, industry empowers consumers to improve their own mobile security through responsible and proactive behavior. There is no single way to enhance mobile device security. Security is best achieved when each player does its part to drive innovation in response to the circumstances and the market.

## **B. FTC Interest: Secure Platform Design**

The FTC is interested in understanding platform design and how it can be more secure.<sup>35</sup> Platforms, as described, have not standardized, but are innovating and evolving. A variety of development tools and security standards are available to platform developers. The FCC has identified and promoted best practices,<sup>36</sup> and industry standards groups including Messaging Anti-Abuse Working Group (“MAAWG”),<sup>37</sup> 3GPP, and GSMA have been refining industry technical approaches and are developing a certification scheme. 3GPP and GSMA have teamed up to create a process for implementing and certifying security best practices. 3GPP is developing methodology to promote network architecture security, and GSMA is developing a program to certify that vendors and others are applying the 3GPP methodology.<sup>38</sup> In addition, ISO offers guidance in 27001 and SANS offers its Top 20 Critical Security Controls.<sup>39</sup>

The role of ecosystem stakeholders in platform design varies. There are different approaches to platform design and the degree to which they are open. Platforms are open ecosystems, and wireless carriers’ ability to control or affect security on platforms is limited. For example, carriers do not have the ability to “lock-down” a mobile device if it is infected with malware. And, carriers have no role in security if a device is not using a carrier’s network, but is connected to the Internet via WiFi or some other means. When a device is not connected to a carrier’s data network, consumers can download suspicious apps or otherwise compromise the device or data with no visibility by the network.

---

<sup>34</sup> See CTIA Comments, Guidelines on Hardware Rooted Security in Mobile Devices (Draft), Department of Commerce Special Publication: 800-164 (Draft), 5-6 (filed Dec. 14, 2012).

<sup>35</sup> The FTC states in its request for comment that “Commenters may interpret the term ‘platform’ broadly to include mobile operating system providers, device manufacturers, app stores, or others that maintain two-sided markets for third-party developers and consumers. In some cases, a platform may serve several of these roles (e.g., providing a mobile operating system and an app store).”

<sup>36</sup> See *Ten Cybersecurity Tips for Small Businesses*, FCC.gov, available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-306595A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf).

<sup>37</sup> In October 2012, the MAAWG issued its Best Practices to Address Online Mobile Threats, which issued recommendations on how to address new and increasingly sophisticated online and mobile hazards. MAAWG, *Best Practices to Address Online and Mobile Threats* (Oct. 15, 2012), available at [http://www.maawg.org/sites/maawg/files/news/M3AAWG\\_LAP\\_Best\\_Practices\\_to\\_Address\\_Online\\_and\\_Mobile\\_Threats\\_0.pdf](http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf) (“MAAWG Best Practices”).

<sup>38</sup> See 3GPP, *Security Assurance Methodology (SECAM) for 3GPP Nodes*, available at [http://www.3gpp.org/news-events/3gpp-news/1569-secam\\_for\\_3gpp\\_nodes](http://www.3gpp.org/news-events/3gpp-news/1569-secam_for_3gpp_nodes).

<sup>39</sup> See ISO/IEC 27001 – Information Security Management, available at <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>; see also SANS Top 20 Critical Security Controls, available at <http://www.sans.org/critical-security-controls/controls>.

Industry makes great efforts to educate customers on security best practices and to offer approaches that can help customers protect themselves and their data. By way of example, on April 15, 2014 CTIA and participating wireless companies announced a “Smartphone Anti-Theft Voluntary Commitment,” under which each participant agreed that new models of smartphones first manufactured after July 2015 for retail sale in the United States will offer, at no cost to consumers, a baseline anti-theft tool that is preloaded or downloadable on wireless smartphones, and committed to permit the availability and full usability of a baseline anti-theft tool to be preloaded or downloadable on smartphones.<sup>40</sup>

But even the most secure platform can be altered by consumers who inadvertently or intentionally subvert security policies. In some cases, device owners are able to modify firmware content, such as with customized boot loaders and recovery images. Through modification of the operating system, kernel, or other means, a sophisticated user could also affect interaction with the hardware context in unintended ways, such as directing read/write to memory for the device’s web browser or other applications. “Rooting”<sup>41</sup> and “jailbreaking”<sup>42</sup> present security challenges. When a user removes the software controls that restrict access to “apps” and “app stores” other than those supported by the device’s operating system, consumers may inadvertently expose their data, causing sensitive information to become unprotected. Thus, rooting and jailbreaking increase a device’s vulnerability to cyberthreats such as malware, spyware, and viruses, and CTIA discourages consumers from taking these types of actions.<sup>43</sup> Finally, consumers may decide to permit others to physically access their device or provide others with authentication information necessary to access the device. Changing a mobile device’s security features, downloading new apps, or giving others access to a device can expose users to security risk, but many who choose to do so have balanced the risk against the benefits of using mobility as they see fit.

Any action by the FTC related to platform design should reflect the diversity in platform design that provides consumers with choices in the marketplace. Just as the FTC should not choose winners and losers in the marketplace by dictating what technology is appropriate to implement cybersecurity measures, it also must be careful not to encourage particular platforms

---

<sup>40</sup> See CTIA Press Release, *CTIA and Participating Wireless Companies Announce the “Smartphone Anti-Theft Voluntary Commitment*, available at <http://www.ctia.org/resource-library/press-releases/archive/ctia-announce-smartphone-anti-theft-voluntary-commitment>. Network operators, device manufacturers and operating system companies are participating in the voluntary commitment. They include Apple Inc.; Asurion; AT&T; Google Inc.; HTC America, Inc.; Huawei Device USA; LG Electronics MobileComm USA, Inc.; Motorola Mobility LLC; Microsoft Corporation; Nokia, Inc.; Samsung Telecommunications America, L.P.; Sprint Corporation; T-Mobile USA; U.S. Cellular; and Verizon Wireless.

<sup>41</sup> According to CTIA, “[r]ooting allows a device owner to obtain full privileged control within the operating system to overcome any software parameters or other limits on the device. With this access, a hacker may alter or overwrite system protections and permissions and run special administrative applications that a regular device would not normally do. Once rooted, the device is jailbroken.” See <http://www.ctia.org/resource-library/glossary/archive/rooting>.

<sup>42</sup> According to CTIA, “jailbreaking” “[i]nvolves removing software controls imposed by the operating system by manipulating the hardware and/or software coded into the device.” See <http://www.ctia.org/resource-library/glossary/archive/jailbreaking>.

<sup>43</sup> As a policy matter, manufacturers and others in the mobile ecosystem should not be responsible for consumers who choose to take risks, or be required to block consumers from modifying their devices.

to dictate industry security standards. Instead, the FTC should promote flexibility for platform developers and others to adopt reasonable substitute approaches to security. Such an approach will foster better security across all platforms and encourage technological advances that can be shared across platforms.

**1. The FTC asks how platforms can create robust development environments while limiting the potential for abuse by privacy-infringing or malicious third-party applications.**

Platform design encourages app developers to experiment and innovate on both new services and security. Many app stores and third-party app developers and distributors take steps to guard against bad apps and abuse. Examples of some helpful, voluntary practices include app store owner oversight of applications, timely removal of malicious applications, relationships with app developers, and best practice tools provided for app developers to help them think about and incorporate security best practices throughout the app development process. Some apps and app stores include notice to customers about what information the app will be able to access, whether at the initial installation stage, or by asking for specific permissions when the app operates. Facilitated by some platforms, stakeholders also coordinate disclosure practices, which allows for reporting of vulnerabilities to the app owner with confidence that an identified risk will be remediated in a timely and appropriate manner.

Consumers have extraordinary choice when choosing apps and navigating the Internet on their mobile devices. Multiple sectors of the ecosystem engage in consumer education about the risks of accessing third-party applications from untrustworthy sources, the dangers of clicking on links they receive via SMS text messages, and the importance of understanding permissions they are granting to apps they choose to install. Some consumers prefer the controlled environment of actively-managed app stores and choose trusted sources, while others seek out apps from varied sources. Some consumers are more concerned than others about apps' access to data, and may avoid apps that access more data than they are comfortable with or that provide inadequate disclosures. Others tolerate more risk in exchange for desired functionality or innovation. There is no one right way to manage applications, and consumers choose the platforms and apps that best suit their needs.

**2. The FTC asks whether particular design approaches have proven more or less effective in protecting consumer privacy and security.**

A layered and flexible approach to platform design works best because the mobile ecosystem has several segments. First, the input, or upstream, segment provides the backbone of wireless communications networks and includes towers, network equipment, backhaul facilities, and spectrum. Second, wireless carriers transmit voice, messaging, and data services over the network. Finally, in the edge, or downstream segment, sophisticated mobile devices containing operating systems, platforms, applications, content, and mobile commerce connect consumers to the network.<sup>44</sup>

---

<sup>44</sup> See generally, Fifteenth Report (¶¶ 264-357) (describing segments).

Security is relevant to each segment. For example, in the input segment, network-based security provides consumers the power to protect their information through device management capabilities, firewalls, secure storage, and virtual solutions. Network operators and others also use innovative encryption techniques to protect email and data. In the downstream segment, effective solutions include a focus on end-user education and device solutions such as strong authentication and secure connectivity. As discussed below, innovation also is occurring in app development and in methods of app distribution.

Diverse platform design approaches used in the U.S. have resulted in effective mobile security. Given the low incidence of malware infection in the United States, compared with the rest of the world, this layered approach works. Different design approaches that incorporate security best practices—for example, open platforms versus walled gardens—drive innovation and give consumers choice. Even if superior technical approaches emerged, regulation or standardization could be counterproductive because, as noted, it can prematurely concentrate solutions, stifle innovation for better approaches, and limit the flexibility needed to stay ahead of bad actors.

### **3. The FTC asks about trade-offs between different approaches to providing developers with access to consumers' personal information or device resources.**

Apps need access to different levels of information and device resources depending on the setting and function involved. Access to more data or device resources can drive innovation and better user experiences. As a general matter, an application should provide notice and obtain consent from a user to access personal information that it needs to provide or support its function. Responsible application developers strive to limit the access to the consumer's mobile device data. For example, a flashlight app should not need to access all of the contacts on the mobile device. But, access to the phone's contacts could be vital to a social networking app.

The market is experimenting with different approaches to personal data use, and CTIA supports the efforts to combat true consumer deception about data collection practices in the app marketplace. Appropriate enforcement efforts can effectively protect consumers while fostering the diversity of apps and distribution methods that have enabled consumers to reap the benefits of mobile innovation.

#### **C. FTC Interest: Secure Distribution Channels**

Distribution channels for apps are diverse and global. They can cultivate collaboration and improved security, and are one part of the overall picture in mobile device security. Different platforms have app stores, including Apple's iTunes, Microsoft's Windows Phone Marketplace, Nokia's Ovi Store, and Google Play. Independent app stores abound as well, from tablet and device app stores, to carrier app stores, to Amazon. Security can vary across this market, a natural byproduct of competition and innovation. Consumers can learn about app store security through blogs, websites, and services.

Distribution channels engage in self-regulatory practices by setting industry standards, but distribution channels are just one part of the multilayered mobile security approach. Their

efforts in combination with appropriate privacy and security practices by app developers serve to best protect consumers and provide them choice. Pinning similar responsibility on distribution channels will create a system where only companies with vast resources to police and test apps for security will have the ability to create or maintain distribution channels, which will lessen competition.

CTIA offers consumers helpful information about distribution channel security and privacy. CTIA provides a list of key steps consumers can take to improve their cybersecurity profiles, including guidance about downloading and using apps.<sup>45</sup> CTIA advises consumers to “check to make sure” that downloads are “legitimate and trustworthy BEFORE you visit or add them to your mobile device.” This is important because, “[u]nfortunately, there are some questionable companies that include spyware/malware/viruses in their software or applications.” CTIA also advises consumers to “[r]ead user agreements BEFORE installing software or applications to your mobile device. Some companies may use your personal information, including location, for advertising or other uses.” CTIA further advises consumers to use beneficial security apps, noting “many applications stores offer encryption software that can be used to encrypt information on wireless devices.” Similar information is available from industry participants and third parties.

### **1. The FTC asks about the role platforms should play in creating secure distribution channels, such as app stores, for mobile applications.**

Platforms have a role to play and are part of the ecosystem’s response to security. Curated app stores relied on by U.S. mobile customers are one of the key factors for our low mobile malware infection rate. App store curators engage in various security-related practices, including actively monitoring the applications for sale and guarding for malware, providing security privacy guidelines for app developers, and offering developers best practice tips to build security into applications from day one.<sup>46</sup> This has been accomplished through market forces and without the need for regulatory activity.

Each app store’s approach necessarily aligns with its mission and resources. Diversity in approaches to app stores and other distribution channels is good for consumers, has generated innovation, and, as a result, investment in application development has flourished.<sup>47</sup> This has been facilitated by the hands-off approach taken by the FTC, FCC, and other government agencies with a role in this arena. Endorsement of one app store or distribution model over another could stifle innovation and decrease consumer choice.

---

<sup>45</sup> CTIA Cybersafety Tips.

<sup>46</sup> See, e.g., J.D. Biersdorfer, *What it Means when Google ‘Verifies’ an App*, N.Y. TIMES (May 9, 2014), available at [http://www.nytimes.com/2014/05/09/technology/personaltech/what-it-means-when-google-verifies-an-app.html?\\_r=0](http://www.nytimes.com/2014/05/09/technology/personaltech/what-it-means-when-google-verifies-an-app.html?_r=0).

<sup>47</sup> See *A List of Alternative App Stores for Distributing Your App or Mobile Game*, mobyaffiliates.com (Jan. 28, 2014), available at <http://www.mobyaffiliates.com/blog/a-list-of-alternative-app-stores-for-distributing-your-app-or-mobile-game/> (describing why some app developers may want to distribute their apps outside of the Apple Store or Google Play); *Global Mobile Statistics 2013 Section E: Mobile Apps, App Stores, Pricing and Failure Rates*, mobiThinking.com (May 2013), available at <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/e> (app revenues may have been \$20-25 billion in 2013, a number that could triple by 2017).

The FTC's efforts to educate consumers support industry efforts to raise awareness about which app resources consumers can trust, and how to determine whether an application from an unknown or little known source could compromise data security. With information, consumers can make decisions about which applications to download based on their own risk tolerance. CTIA, with industry and third parties, provides and continues to improve upon these consumer education tools to wireless customers.

**2. The FTC asks whether application review and testing is scalable and what techniques have proven effective in detecting malicious or privacy-infringing applications.**

Due to the explosion in innovation in mobile device applications, there are over 6 million apps in the ecosystem. Various participants in the ecosystem are developing and using different kinds of effective approaches to application review and testing. Mobile application and security companies can review applications with technology grounded in big data and predictive analytics. Applying security analysis to continuous telemetry, platforms can identify emergent threats and indicators of compromise that signal novel and targeted attacks. These techniques often capture risky and anomalous behaviors of threats before the exhibit malicious behavior.

U.S. app stores engage in a variety of comprehensive security practices, which may include creating relationships with app developers, so that they know who is developing the apps in their stores; reviewing apps that are submitted; and responding quickly to customer complaints about any apps that do not behave the way they are advertised. As noted above, this vigilance has contributed to low U.S. malware infection rates.<sup>48</sup>

In contrast to the diverse and effective approaches in the United States, certain app stores based overseas tend to be less secure because they generally do not apply the same controls. Observers have noted that various types of malicious apps are common overseas, particularly in China and Russia, "most likely" because of a "lack of 'standard' app stores."<sup>49</sup> Third-party app stores are much more common in certain parts of the world and tend to focus on specific countries, languages and regions. Malware authors may find it easier to distribute malware in those app stores."<sup>50</sup> Overall, observers report, 2.13 percent of unique users attacked worldwide

---

<sup>48</sup> See Lookout, *Mobile Threats, Made to Measure* ("In 2013 mobile threats were clearly a global problem, but Asia, Russia and parts of Eastern Europe and Africa continue to stand out with higher levels of risk."), available at <https://www.lookout.com/resources/reports/mobile-threat-report>.

<sup>49</sup> Trend Micro, *TrendLabs 3Q 2013 Security Roundup 6*, available at <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trendlabs-3q-2013-security-roundup.pdf>; see also Trend Micro, *Fake Apps, Russia, and the Mobile Web: Making the SMS Fraud Connection*, available at <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fake-apps-russia-and-the-mobile-web.pdf>; see also Lookout, *Mobile Threats, Made to Measure*, available at <https://www.lookout.com/resources/reports/mobile-threat-report>; see also PC Mag SecurityWatch, *Nearly 7,000 Malicious Android Apps Infest China's Appstores* (Aug. 27, 2013), available at <http://securitywatch.pcmag.com/mobile-security/315218-nearly-7-000-malicious-android-apps-infest-china-s-appstores> (examining 20 major Chinese third-party app stores).

<sup>50</sup> See Alcatel Lucent, *Kindsight Security Labs Malware Report - Q4 2013 9* (rel. Jan. 29, 2014), available at <http://resources.alcatel-lucent.com/?cid=172490>; see also Lookout, *Mobile Threats, Made to Measure*, available at <https://www.lookout.com/resources/reports/mobile-threat-report> ("When it comes to malware, people who use trusted, mainstream app stores (as the bulk of users in the US and Western Europe do) are less likely to encounter

were located in the United States in 2013, in contrast to the 40.3 percent of worldwide victims of malware located in Russia.<sup>51</sup>

Continued consumer education, like that pursued by CTIA and its members, about the risks of rooting or jailbreaking and downloading apps from unknown sources is the best way to combat the spread of malicious or privacy-infringing applications. The FTC may be able to help by welcoming collaboration with distribution channels, which could lead to a better understanding of bad actors that exploit the ecosystem. Given the innovation and overall success of private sector efforts responding to the market, government should remain wary of any action that seems to pick winners and losers in emerging technology, including techniques for detecting malicious apps.

**3. The FTC asks whether smaller players in the mobile ecosystem, such as third-party app stores, have the resources to deploy such techniques.**

Some third-party app stores have the resources to provide monitoring and curation similar to some platform-specific app stores. Others are also gaining this capability as it is demanded by their customers and as they collaborate with device and software developers. The market is working. Different parts of the mobile industry, third parties, consumer groups, and others provide recommendations and guidance to the public about software, applications, or app stores they recommend. For example, carriers provide lists of recommended apps for users across platforms.<sup>52</sup> As discussed in more detail below, they also provide security applications for their customers.<sup>53</sup>

Other technology companies have stepped in as well. Cybersecurity companies offer a variety of mobile security tools, including anti-theft and anti-malware services that categorize apps, flag and protect against threats in real time, offer browsing protection, and other features.<sup>54</sup> These services also include security awareness to determine if an app is trusted, malware, or unknown; information on potentially unwanted apps (“PUA”) to determine whether they are leaking contacts, photos, or other personal data; and details on apps’ effect on battery life and bandwidth consumption.<sup>55</sup> One cybersecurity company quickly delivered an application to

---

malware. By contrast, users in Eastern Europe, Russia and Asia face a risk of encountering malware that is as much as 20 times higher due to the widespread use of high-risk third-party stores.”).

<sup>51</sup> See SecureList, *Mobile Malware Evolution: 2013* (rel. Feb. 24, 2014), available at [http://www.securelist.com/en/analysis/204792326/Mobile\\_Malware\\_Evolution\\_2013](http://www.securelist.com/en/analysis/204792326/Mobile_Malware_Evolution_2013).

<sup>52</sup> See, e.g., AT&T, *Apps for Cell Phones, iPhone, Android, and More*, available at <http://www.att.com/shop/apps.html>; Sprint, *Applications for Every Phone*, available at <http://www.sprint.com/landings/applications/?ECID=vanity:apps>.

<sup>53</sup> See, e.g., Sprint, *Total Equipment Protection*, available at <http://protection.sprint.com/>.

<sup>54</sup> See, e.g., Product Description, Norton Mobile Security, available at <https://mobilesecurity.norton.com/>; Product Description, Lookout, available at <https://www.lookout.com/android>.

<sup>55</sup> See, e.g., Symantec Blog, *Symantec App Center 4.4 – now with Norton Mobile Security* (May 6, 2014), available at <http://www.symantec.com/connect/blogs/symantec-app-center-44-now-norton-mobile-security>.

detect the Heartbleed vulnerability for both platform and applications installed on a device.<sup>56</sup> These efforts provide consumers with information and tools they need to make better choices and stay safe and secure online, illustrate how the market responds to demand for help and guidance, and demonstrate how consumers' varied needs drive offerings. Some consumers want the diversity and accessibility of apps from varied independent sources, while others want to rely on trusted sources. Consumer choice is driving market innovation.

**4. The FTC asks whether limiting application distribution to a single channel provides substantial security benefits, and what trade-offs this approach would impose.**

Given that U.S. consumers have access to both “walled garden” application distribution and more open network application stores, it is clear that different distribution models have been successful in meeting consumer demand and largely preventing the spread of malware. As a practical matter, given consumers' control over their devices and their freedom to customize and download from different sources, it would be difficult, or even impossible, to strictly limit distribution to a single channel. But even if it were possible, it would not be desirable: varied distribution and access points benefit consumers.

Consumers make tradeoffs when it comes to rapid adoption of new apps, preferences between operating systems, and relative openness. Different consumers have different approaches to risk given their different mobile habits and preferences. This choice has effectively driven the U.S. app market to be one of the safest in the world. A single distribution channel may increase risk, as it could spread malware more efficiently and provide a single set of controls that attackers would need to subvert. Moreover, the availability of multiple distribution models gives consumers and app developers choices that lead to competition and innovation.

**5. The FTC asks about potential alternative approaches to detecting or impeding malicious or privacy-infringing applications on end-user devices.**

Companies are constantly offering new tools to detect and impede malicious apps. The wireless ecosystem offers a host of options. Carriers offer security apps to their customers, and other free and low-cost applications are available from third parties to monitor mobile device security. Examples of technologies from market leaders show how consumers can be protected across a variety of settings: device, network, and cloud.

For example, one cybersecurity company offers both free and premium services, which have been downloaded millions of times, showing that consumers look to the marketplace to protect their devices and information.<sup>57</sup> This company and others like it offer security solutions like anti-theft, anti-malware, call/SMS blocking, and browsing protection. They also offer app reputation checking, a cloud-based technology that scans applications to ensure that private

---

<sup>56</sup> Andrew Blaich, *Heartbleed Bug Impacts Mobile Device*, Bluebox (Apr. 8, 2014), available at <https://bluebox.com/blog/technical/heartbleed-bug-impacts-mobile-devices/>.

<sup>57</sup> See Product Description, Symantec Mobile Security, available at <http://www.symantec.com/mobile-security>.

information is not being leaked without a user's knowledge or to an extent to which they are not aware. Another company provides a cloud-based service that works at the DNS level to prevent browsing to sites that are known to host malware, spam originating sites, phishing sites and those on the Internet Watch Foundation's Child Abuse Image Content ("CAIC") list.<sup>58</sup> Carriers also offer security services to their customers, including the ability to locate a lost or stolen device on a map, remotely lock and wipe a device, sound a loud alarm, learn the location of a device right before it runs out of battery, and backup contacts and photos in the event a device is compromised by malicious software.<sup>59</sup> Varied companies also have shown interest in innovating around mobile app advertising; for example, one company is developing and offering guidelines on mobile app advertising to equip mobile app advertisers and developers with clear privacy and use experience guidelines as they explore new mobile advertising techniques.<sup>60</sup>

Enterprises are able to engage in MDM, both on enterprise devices and BYOD devices, which typically include over-the-air distribution of applications, data, and configuration settings for all types of mobile devices. By controlling and protecting the data and configuration settings for all mobile devices in an enterprise's network, MDM can improve security by sending needed patches, installing security applications, and monitoring for malware or other suspicious security-related activities.

Many carriers offer Hosted Mobility Management Services ("HMMS") to help businesses quickly and flexibly deliver enterprise technology services to BYOD or enterprise devices through a wide array of MDM solutions, network-based security, anti-virus and anti-malware device scanning, prohibited application alerts, BotNet identification, and end-to-end support.<sup>61</sup>

Finally, some platforms also take creative approaches to security. Some platforms offer "Bug Bounty" programs—rewards to independent parties who identify malware or other bad applications and alert the app store. Others are innovating in how to monitor for malware, from studying internet traffic patterns to the economics of malware and identifying what vulnerabilities would be the most profitable to exploit.

---

<sup>58</sup> See Product Description, Norton ConnectSafe, available at <https://dns.norton.com/>.

<sup>59</sup> See, e.g., T-Mobile Support, *About Lookout Mobile Security Premium*, available at <http://support.t-mobile.com/docs/DOC-10013>.

<sup>60</sup> See Lookout, *Mobile App Advertising Guidelines: A Framework for Encouraging Innovation While Protecting User Privacy* (June 2012), available at <https://www.lookout.com/resources/reports/mobile-ad-guidelines>. The aim of the guidelines is to support growth and innovation in mobile advertising while protecting user privacy and increasing the trustworthiness of ads. Lookout also uses these guidelines to define what qualifies as adware for its users. If it found that one of its users downloaded an app that contained adware, Lookout would highlight the presence of adware to the user and give him or her the option to remove the application. As a result, Lookout found that a majority of the users chose to uninstall apps that contained adware once they were given notice of their existence.

<sup>61</sup> See, e.g., T-Mobile, *Mobile Device Management*, available at <http://how-to.t-mobile.com/hmms-mobile-device-management/>; AT&T, *Mobile Security Service*, available at <http://www.business.att.com/content/productbrochures/mobile-security-service.pdf>.

Because stakeholders face different risks, individual users and participants determine whether and how these sorts of tools can best be deployed. Myriad options are available and innovation continues as companies look to meet and drive demand.

#### **D. FTC Interest: Secure Development Practices**

Players in the mobile ecosystem are collaborating to improve app development security practices. Consumers have access to security information from a variety of sources, and CTIA and others also work to educate consumers about best practices.

##### **1. The FTC asks about secure application development resources available to third party developers, whether the developer community is taking advantage of these resources, and how industry supports secure development.**

The app developer community is diverse and thriving, so it is not surprising that approaches to security vary. Big players (carriers/app store curators) and app developers have been increasing collaboration on app security. As the developer community evolves and matures, security is improving. Market forces have resulted in third parties and others stepping in to provide development guidance and apps to improve security.

CTIA and industry players make available varied tools to optimize application development. Both the storefronts (such as Apple, Blackberry, Google, and Microsoft) and the major U.S. carriers have developer relations teams that can help developers with questions about their platforms. For example, carriers have taken steps like establishing monthly public meetings to share best practices for mobile application development with app developers and other members of the mobile security community. App stores likewise provide information for developers. For example, Apple's iOS Developer Library provides a Secure Coding Guide which teaches coders how to write programs, including mobile applications, so that they are resistant to attack by malicious or mischievous people or programs.<sup>62</sup> Android provides similar guidance to its app developers in the Android Developer Security Guidance.<sup>63</sup>

Organizations like the Application Developers Alliance, Association for Competitive Technologies, MoDev, Mobile Future, and Mobile Monday also help the developer community. CTIA describes and provides links to its own and other resources on its website.<sup>64</sup> The FTC also provides tips for app developers to build security into their offerings.<sup>65</sup> All of these efforts show collaboration between carriers, platforms, and other players in the ecosystem, highlighting how the mobile industry is making security a top priority.

---

<sup>62</sup> See iOS Developer Library, *Secure Coding Guide*, available at <https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html>.

<sup>63</sup> See Android Developer Security Guidance, *Security Tips for Android Developers*, available at <http://developer.android.com/training/articles/security-tips.html>.

<sup>64</sup> CTIA, *Know My App*, available at <http://www.knowmyapp.org/developers.aspx>.

<sup>65</sup> See Bureau of Consumer Protection Business Center, *Mobile App Developers: Start with Security* (Feb. 2013), available at <http://www.business.ftc.gov/documents/bus83-mobile-app-developers-start-security>.

**2. The FTC asks whether consumers have information they need to evaluate the security of an application, if they are aware of potential security risks (e.g., the insecure transmission of data), and whether there are ways to make application security transparent to end-users.**

Consumers have access to information about mobile security from myriad sources. Mobile security makes headlines around the world, technology bloggers actively monitor the security of apps and other parts of the mobile ecosystem, and security concerns are often raised in app reviews. Different applications provide notice and information to consumers in different ways. As participants in the FTC’s 2013 Workshop noted, there are different ways of engaging consumers with information about how applications operate and use data.<sup>66</sup> Those practices are evolving in response to market demand and increased interest and attention. To help consumers, industry provides information on application selection, evaluation and use. For example, CTIA has published consumer guidance to inform consumers of mobile security best practices.<sup>67</sup> Carriers also provide best practices and security applications.<sup>68</sup>

The FTC’s consumer education is invaluable to consumers. It advises consumers:

Before you download an app, consider what you know about who created it and what it does. The app stores may include information about the company that developed the app, if the developer provides it. If the developer doesn’t provide contact information – like a website or an email address – the app may be less than trustworthy. If you’re using an Android operating system, you will have an opportunity to read the “permissions” just before you install an app. Read them. It’s useful information that tells you what information the app will access on your device. Ask yourself whether the permissions make sense given the purpose of the app; for example, there’s no reason for an e-book or “wallpaper” app to read your text messages.<sup>69</sup>

As consumers’ expectations evolve and application developers continue to improve apps and create new security solutions, consumers will have varied options and approaches. Ongoing

---

<sup>66</sup> See FTC, *Mobile Security Forum Potential Threats and Solutions*, Transcript 82-83, 97, 100-17 (June 4, 2013) (discussion of how permissions vary across platforms), available at [http://www.ftc.gov/sites/default/files/documents/public\\_events/mobile-security-potential-threats-solutions/30604mob\\_0.pdf](http://www.ftc.gov/sites/default/files/documents/public_events/mobile-security-potential-threats-solutions/30604mob_0.pdf).

<sup>67</sup> See CTIA Cybersafety Tips (advising consumers to “avoid rooting [o]r jailbreaking” and to “[r]ead user agreements BEFORE installing software or applications”).

<sup>68</sup> See, e.g., AT&T Wireless Support, *Protect Yourself from Mobile Malware*, available at [http://www.att.com/esupport/article.jsp?sid=KB423850&cv=820&br=BR&ct=800007&pv=3#fbid=YUcO\\_-2V54Z](http://www.att.com/esupport/article.jsp?sid=KB423850&cv=820&br=BR&ct=800007&pv=3#fbid=YUcO_-2V54Z) (advising customers to “[i]ninstall anti-virus and anti-spyware security software on devices,” “create strong, secure passwords,” “click on links only sent via text or email from a known source,” and “disable the Wi-Fi auto connect feature”).

<sup>69</sup> See *Understanding Mobile Apps*, OnGuardOnline.gov, available at <http://www.onguardonline.gov/articles/0018-understanding-mobile-apps#malware>.

efforts to promote consumer understanding—of what is a trustworthy application source and how to evaluate and use applications—will be key for consumers to avoid malicious apps from untrustworthy sources while still promoting consumer choice.

### **E. FTC Interest: Device Security and Updates**

The FTC seeks information about the so-called “security lifecycle of a mobile device,” including whether “companies distinguish between a mobile device’s general product lifecycle and its security lifecycle,” and what factors “affect the length of a mobile device’s security lifecycle.” The FTC asks about what information is available to consumers concerning “the security lifecycle of their mobile devices” and whether consumers can “factor security into their device purchasing decision.”

The FTC’s framing of “security lifecycle of a mobile device” is not reflective of the industry’s approach to device development and the diverse mobile ecosystem, insofar as the FTC’s formulation might suggest that mobile security is device-driven or has a specific start and end date, like a device’s “product lifecycle.” Equipment manufacturers, software manufacturers, and network operators are continually monitoring for security issues, and provide consumers with a variety of tools to address security issues even after a product lifecycle has completed. FTC policies should continue to support a partnership between industry and consumers, and help educate consumers so they can make smart choices about security.

*First*, and fundamentally, security is not a product or end point; it is a risk-based *process*. Security is an important part of development, support, and use of software, devices, and networks by individuals and enterprises. The federal government recognizes this. Working with industry as it developed the Cybersecurity Framework, NIST embraced the concept that cybersecurity needs to be incorporated into business processes in a risk-based way. The NIST Cybersecurity Framework recognizes the need to “address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.”<sup>70</sup> The private sector and the government are working to evaluate and operationalize the Framework, recognizing that there is no one solution, no best model, and no end state to security.

*Second*, product “lifecycles” can include—but are conceptually distinct from—security. Software or device “lifecycle” generally refers to when the product is marketed and receives standard software updates. One company explains that “[t]he lifecycle begins when a product is released and ends when it’s no longer supported.”<sup>71</sup> Software and device lifecycles vary and are constantly changing. For example, according to a report from September 2013, the smartphone replacement cycle was 21.7 months, up slightly compared to the historical figure of around 18 to 20 months.<sup>72</sup> Operating systems and applications have their own lifecycles.

---

<sup>70</sup> NIST Cybersecurity Framework at 1.

<sup>71</sup> See Windows, *Windows Lifecycle Fact Sheet*, available at <http://windows.microsoft.com/en-us/windows/lifecycle>.

<sup>72</sup> See Mark Hoelzel and Marcelo Ballve, *Consumers Are Taking Longer To Upgrade Their Phones, Another Sign The Smartphone Revolution Is Maturing*, BI Intelligence, (Sept. 5, 2013), available at

Security concerns are not driven by or tied to a device's product lifecycle. Equipment manufacturers, software manufacturers, and network operators continually monitor for security issues, and provide consumers with a variety of tools to address security issues even after a product lifecycle has completed. Like computers, older mobile devices may not receive the latest versions of operating software updates, and indeed may not be able to support newer software. Security patches, however, are not necessarily tied to operating software updates, and may occur at any time.

*Third*, mobile security involves far more than devices and updates. As discussed above, in the complex, multilayered wireless ecosystem, security depends on software, applications, distribution channels, networks, devices, and end users, who are critical to security. Care should be taken not to elevate *device* security over other elements that are equally or more important.

Several factors affect the roll out of security updates to end users, including considerations about the severity and predicted impact of the identified vulnerability, the technical capabilities of the device (*e.g.*, enough memory or processing power to satisfactorily store or execute the update) as well as the many players involved in the development, testing, approval, and distribution of patches and updates to software and applications.

Notwithstanding this complexity, network operators, device makers, and platforms have had great success in improving mobile security in the U.S. As noted above, the malware infection rate in the United States is quite low.<sup>73</sup> Patrick Traynor, Associate Professor in the College of Computing at Georgia Tech recently conducted a study on mobile malware, which he discussed at the FTC's 2013 Workshop. He noted that that "we saw a few thousand devices, 5-6,000 devices, that were infected during our three-month study. . . . [W]hen you put it into context . . . over the course of our study it turns out that less than 1/1000th of 1 percent of devices in this provider's network were infected with what the community agrees is mobile malware, malicious applications."<sup>74</sup>

More fundamentally, though, patches and updates cannot prevent or fix many threats. Industry collaboration helps it address and stay ahead of rapidly changing threats. But, the

---

<http://www.bullfax.com/?q=node-consumers-are-taking-longer-upgrade-their-phones-anothe> (based on research by Roger Entner); *see also* Roger Entner, *Handset Replacement Cycles Haven't Changed in Two Years, But Why?*, FierceWireless (Mar. 18, 2013), *available at* <http://www.fiercewireless.com/story/entner-handset-replacement-cycles-havent-changed-two-years-why/2013-03-18>; Gartner, *Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013* (Feb. 13, 2014) *available at* <http://www.gartner.com/newsroom/id/2665715> (noting a slightly longer replacement cycle in February 2014).

<sup>73</sup> *See supra* at 18-19.

<sup>74</sup> FTC, Mobile Security Forum: Potential Threats and Solutions 55 (June 4, 2013), *available at* [http://www.ftc.gov/sites/default/files/documents/public\\_events/mobile-security-potential-threats-solutions/30604mob\\_0.pdf](http://www.ftc.gov/sites/default/files/documents/public_events/mobile-security-potential-threats-solutions/30604mob_0.pdf) (fraction was reflected in transcript as "1/111,000<sup>th</sup>"). The research paper referenced by Professor Traynor, *The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers*, is available here: <http://www.cc.gatech.edu/~traynor/papers/lever-ndss13.pdf>. It states in its Abstract that "The mobile malware found by the research community thus far appears in a minuscule number of devices in the network: 3,492 out of over 380 million (less than 0.0009%) observed during the course of our analysis. This result lends credence to the argument that, while not perfect, mobile application markets are currently providing adequate security for the majority of mobile device users."

nature of cyber threats often evolves more quickly than the techniques used to combat them. Even where a vulnerability is recognized and a fix is designed before an exploit happens, often the publication of the fix leads cyber attackers to develop and distribute an exploit before the public has time to respond. Even with a rapid patch, risk remains because attacks often rely only on simple tricks to lead users astray—malicious apps, phishing attempts, or persuading users to click on bad links. Trend Micro reported that in the third quarter of 2013 a variety of tricks were being used by bad actors, including malicious apps, fake emails including malicious links, and phishing sites designed to target mobile devices. It found “a 53% increase in the number of phishing sites” in 2013 compared to 2012, and that 42% of the malicious sites spoofed banks and other financial institutions.<sup>75</sup> Lookout reported in 2012 that four out of ten users in the U.S. would click an unsafe link on a mobile device, a 30% increase from the year before.<sup>76</sup> And, while not specific to mobile, Symantec noted an increase in spear-phishing attacks in 2013.<sup>77</sup> Thus, while patches and updates are important, the real area of risk is from external sources, bad actors, and the actions and understandable missteps of end users. This is why innovation, along with continued emphasis on basic internet and mobile cybersafety, will remain our best defense.

The FTC expresses interest in whether a consumer can factor information about the security lifecycle” of mobile devices into a “purchase decision.” As noted above, much more is involved in mobile security than the device. Consumers often consider many factors when making decisions about how to purchase and use mobile technology and services, including functionalities, price, quality and reach of the communications network, processing power, battery life, access to applications, software capabilities, and aesthetics, along with security. Consumers can take advantage of the explosion of information about all of these aspects of mobile service from tech reviewers and other third party sources. In addition, OS developers, OEMs, carriers, application developers, and mobile security companies provide consumers information on product features and security from their own unique perspectives. Like all the foregoing factors, when it comes to security, consumers exhibit different preferences. For example, as explained above, some consumers want the relative security and predictability of exclusively using curated app stores, while others choose to modify their devices and install applications from third parties. In partnership with industry, end users drive the market, as the highly competitive industry reacts to their needs and demands for technology, services, and information.

A few examples highlight the information and tools available: Android’s Open Source Project explains that there “are many Android-based products available to consumers, and most of them are created without the knowledge or participation of the Android Open Source Project.”<sup>78</sup> As such, “[t]he manufacturer of each device is responsible for distributing software

---

<sup>75</sup> Trend Micro, *Trend Labs 3Q 2013 Security Roundup 7*, available at <http://about-threats.trendmicro.com/us/security-roundup/2013/3Q/the-invisible-web-unmasked/>.

<sup>76</sup> See Lookout, *State of Mobile Security 2012*, available at <https://www.lookout.com/resources/reports/state-of-mobile-security-2012>; See Dean Takahashi, *The Chance that You’ll Hit an Unsafe Mobile Link in the Course of a Year: 30 Percent*, venturebeat.com (Aug. 2, 2011), available at <http://venturebeat.com/2011/08/02/the-chance-that-your-smartphone-has-encountered-malware-in-past-year-30-percent/>.

<sup>77</sup> Symantec, *Monthly Intelligence Report 11* (Sept. 2013), available at [http://www.symantec.com/content/en/us/enterprise/other\\_resources/b-intelligence\\_report\\_09-2013.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_09-2013.en-us.pdf).

<sup>78</sup> See Android Security FAQ, available at <http://developer.android.com/guide/faq/security.html#fixes>.

upgrades for it, including security fixes. Many devices will update themselves automatically with software downloaded ‘over the air,’ while some devices require the user to upgrade them manually.”<sup>79</sup> Apple encourages consumers to “[b]e sure that you are running the latest version of system software” and states that it “will release security updates from time to time, and having the latest available system software version should improve the security of your system.”<sup>80</sup> Apple also states that “we focus our response efforts to have the greatest impact across Apple’s product line” and that it “does not discuss or confirm security issues until a full investigation has occurred and any necessary patches or releases are available.”<sup>81</sup> Apple usually distributes information about security issues in its products through its website and identified mailing lists.<sup>82</sup> Industry members advise customers, among other things, to “say yes to updates” to help keep their devices secure.<sup>83</sup>

Likewise, CTIA advises consumers to “[t]rain yourself to keep your mobile device’s operating system (OS), software or apps updated to the latest version” because “[t]hese updates often fix problems and possible cyber vulnerabilities.”<sup>84</sup> The FTC also advises consumers about avoiding malware and other security concerns, saying “[i]t’s a good idea to update the apps you’ve installed on your device and the device’s operating system when new versions are available. Updates often have security patches that protect your information and your device from the latest malware.”<sup>85</sup> Third parties and public interest groups also provide advice. For example, Stop, Think, Connect provides “Safety Tips for Mobile Devices.”<sup>86</sup>

Consumers thus have available an abundance of information about security to help them make choices that meet their needs.

## V. CONCLUSION

Companies that provide mobile services and consumers who use them must work together on mobile security. Focusing too heavily on one element, be it the device, the network,

---

<sup>79</sup> *Id.*

<sup>80</sup> See Apple Product Security, available at <https://ssl.apple.com/support/security/>.

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

<sup>83</sup> See, e.g., Windows Phone, *How-to Basics, Tips to help keep my phone secure*, available at <http://www.windowsphone.com/en-US/how-to/wp7/basics/tips-to-help-keep-my-phone-secure>; AT&T Support, *Keep your Device Software Up-To-Date*, available at <http://www.att.com/esupport/softwareUpdates.jsp#fbid=AxdB1uAlSoC>; T-Mobile Phone Software Update Tips, available at <http://how-to.t-mobile.com/phone-software-updates/>.

<sup>84</sup> See CTIA Cybersafety Tips.

<sup>85</sup> See FTC, *Consumer Information: Understanding Mobile Apps*, available at <http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps>.

<sup>86</sup> See Stop, Think, Connect, *Cybersafety Tips for Mobile Devices*, available at <http://stopthinkconnect.org/tips-and-advice/safety-for-mobile-devices/> (“Mobile devices are computers with software that need to be kept up-to-date (just like your PC, laptop or tablet). Security protections are built in and updated on a regular basis. Take time to make sure all the mobile devices in your house have the latest protections.”) (providing practical tips and advice).

the operating system, or the application store, will not result in the best mobile security outcome. Likewise, no one kind of company, be it a service provider, OS developer, manufacturer, or application developer can take on singular responsibility. No one layer of the complex mobile ecosystem can unilaterally address security, dictate a uniform approach, or comprehensively manage an end user's experience. Security expertise within the wireless industry, competitive market forces, and consumer education and empowerment are key to continued improvements in mobile security.

CTIA and its members are pleased to offer information to the FTC and other government agencies working in this area to understand how the global wireless ecosystem operates and how it effectively addresses mobile and cybersecurity. CTIA encourages the FTC to support the flexibility and innovation that have fostered remarkable growth in the wireless sector and have produced exceptional security outcomes.