



May 30, 2014

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex X)
600 Pennsylvania Avenue NW
Washington, DC 20580

RE: Mobile Security Projects, Project P145408

Thank you for providing the Online Trust Alliance (OTA) the opportunity to submit comments in response to the Federal Trade Commission's request for public comment on mobile security. As a 501c3 non-profit, OTA's mission is to enhance online trust and empower users while promoting innovation and the vitality of the Internet.

OTA applauds the Commission's leadership in facilitating this and related discussions regarding data collection, privacy controls and security. As consumers and businesses worldwide increasingly rely on mobile devices and applications, the incidents impacting their data security and privacy continue to rise. As the "Internet of Things" becomes part of our lives, devices are now tethered to users with persistent identifiers and increasingly collect data on our lives.¹ The growth of mobile devices and applications are outpacing traditional PCs. It is estimated that mobile commerce will reach \$467.3 Billion in 2019.²

Combined these trends underscore the need for security and privacy enhancing best practices to be embraced by all stakeholders, including device and platform providers, carriers, distribution channels and hardware providers.

Fraudulent and malicious apps unknowingly are being hosted on platforms which have been found to exploit both device APIs as well as "attack" other legitimate applications. In the absence of standardized disclosure notices, applications are accessing users' location, photos, data and contacts often inconsistent with a user's expectation when downloading the application. While such terms may be disclosed within a privacy policy, the consumer has naively installed the application without understanding the implications.

Consumers generally assume apps are all trustworthy since they are being hosted by reputable brands, companies and carriers. They often nonchalantly downloading apps unaware of the security or privacy risks. The lack of controls and circuit breakers to prevent malicious

¹ http://en.wikipedia.org/wiki/Internet_of_Things

² <http://www.virtual-strategy.com/2014/05/30/mobile-commerce-m-commerce-market-expected-reach-4673-billion-2019-new-report-marketsandm>

applications from being hosted, has the industry and consumers chasing their shadows attempting to detect and remediate the threats after they have occurred.

The following comments are provided in response to some of the key questions identified by FTC staff;

I. Secure Platform Design

Trusted platforms and ecosystems are the foundation of the internet. While there is no perfect or absolute security, the entire ecosystem including the OS, device manufacturers, carriers, app stores and app developers must anticipate a range of exploits and commit to a security by design methodology and culture.³ It has been a decade since the first report of mobile malware, three years before the first iPhone.⁴ As criminals are moving to mobile, we are witnessing unparalleled level of malicious attacks against user's devices. Mobile malware and malvertising are forecasted to be the largest threats as hackers are developing more sophisticated mobile exploits.^{5 6}

Combined with malicious apps unknowingly being distributed, other apps have been poorly designed, underscoring how the OS must be hardened including limiting access to APIs and data stores. Additional best practices include automatic and default "out of the box" device updating, and the ability to remotely disable or revoke applications known to be malicious or violate the platform's terms of use.

Additionally developers should not be capable of circumventing security settings. As exposed with Credit Karma and Fandango, they entities disabled OS security settings putting consumer data at risk.⁷ In spite of documentation published by the OS community warning against disabling the default settings, these instructions were apparently disregarded.

It is important to note such threats are not limited to the OS or applications, but also to the device architecture and integrated apps and browsers. Cybercriminals are increasing exploiting the WI-FI and Bluetooth functions, and disabling browsing security settings. Progress has been made to secure these vectors, yet consumers are remain at risk of social engineered exploits.

Carriers and OS providers have made positive inroads providing remote wiping capabilities for lost or misplaced phones, data and communication encryption options along with new features Apple's find my iPhone feature help protect lost data.^{8 9}

Earlier this year smart phone manufactures committed to offer free anti-theft features on all phones made after July 2015 with a "kill switch". Combined these are positive examples of the industry adopting consumer protection and security best practices.¹⁰

³ https://otalliance.org/system/files/files/best-practices/documents/ota_securitybydesign.pdf

⁴ http://www.sophos.com/en-us/threat-center/mobile-security-threat-report.aspx?utm_source=Non-campaign&utm_medium=Cross-link&utm_campaign=CL-CorpBlog

⁵ <https://otalliance.org/malvertising.html>

⁶ <http://www.reliaquest.com/mobile-malware-trends-greatest-security-threat-2014/>

⁷ <http://business.ftc.gov/blog/2014/03/default-lines-how-ftc-says-credit-karma-and-fandango-sslighted-security-settings>

⁸ <https://itunes.apple.com/us/app/find-my-iphone/id376101648?mt=8>

⁹ <http://www.itworld.com/mobile-wireless/420208/new-ios-app-secures-im-traffic-post-quantum-encryption-scheme>

¹⁰ http://www.huffingtonpost.com/2014/04/16/smartphone-kill-switch_n_5158926.html

It is important to note that developers and consumers alike can benefit from the collection of online data, yet all too often consumers innocently allow this tracking and data collection without realizing the implications. While the FTC has taken enforcement action against some developers including the “Brightest Flashlight”, platforms should work to help prevent such abuses.¹¹ While these practices can be discovered by scrolling through device options, ideally platforms should disable non-material data sharing and present users with a consolidated view of all apps via a recurring reminder.

II. Secure Distribution Channels (DC):

Distribution Channels offered by the device manufacturers, OS provider or carriers play a vital role in creating and maintaining a trustworthy distribution channel for apps. They need to establish and enforce guidelines to help insure compliance. In the absence of such practices, un-vetted platforms are highly susceptible to infringing and malicious applications. Repeated instances of unsecure apps will result in consumer’s trust in the platform and respective apps to diminish.

Consumers have a reasonable expectation that the apps hosted or promoted by a DC (whether they are managed by a platform provider (Apple, Microsoft, Google) or a carrier, are safe and secure. Not unlike going to a name brand store, consumers have expectation that the products sold and distributed are not harmful or counterfeit. Progress has been made to improve the apps integrity within DCs including Microsoft, but this has yet to be embraced 100% by any of the DCs.¹²

Platforms providers have a responsibility to help assure that the apps they host meet minimum standards in security, privacy and user notice. As dominate market players, DCs have a responsibility to minimize the risk by swiftly revoking apps which may be infringing on the brand of legitimate companies. Past delays of taking down infringing apps have taken up to six months not only harming legitimate developers but most importantly consumers.

Additionally, DCs should take steps to notify impacted users, when revoking an application may not be possible. Examples include but are not limited to contextual notices prior to the app opening, in app notices and SMS messages to the user.

Consumers and apps developers alike will benefit from robust security screening and testing. While testing and scanning is being provided by some, it is not consistent and often ad-hoc. OTA proposes best practices with a “code of conduct” using a common framework, leveraging existing app development and data security standards.

Such a code needs to consider a reputation review and verification in the onboarding process of the developer. Not unlike the threats from cybercriminals attempting to infiltrate cloud service providers and the advertising supply chain, measures need to be in place to verify and authenticate the publisher. OTA recommends the adoption of an onboarding framework to help identify bad actors, “while fast tracking” legitimate developers.¹³ In the absence of such reputational systems, criminals often “repackage” their app and re-submit them under another

¹¹ <http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived>

¹² <http://www.microsoft.com/en-us/download/details.aspx?id=36173>

¹³ https://otalliance.org/system/files/files/best-practices/documents/new_account_risk_evaluation_framework.pdf

name. The adoption of such best practices and code can enhance online trust without hampering innovation or competition.

Applications should not only be scanned, but should also be signed by a third party to help verify the developer to ensure the code is not misaligned or corrupted. As a best practice, device platforms should only allow signed apps to be in their DC. Today this is required for all apps in the Windows App store and is a best practice for all DCs to consider.^{14 15} In addition, platforms should conduct ongoing monitoring of applications, as well as create abuse reporting mechanisms for both the industry and users to report suspect behavior.

Testing of apps has not been embraced for several reasons including cost, impact to resources, delay in getting products to market and potential liabilities. Other have argued against testing in favor of optimizing a platform for openness to promote innovation and ability of developers to reach the market. The lack of security vetting can have the exact opposite effect. In the absence of such screening, consumers will likely gravitate to dominate brand leaders while startups risk being negatively impacted since the consumer has no knowledge of their “trustworthiness”.

III. Secure Development Practices:

One of the major challenges consumers are faced with is their inability to evaluate the security of an application. Mechanisms and tools are not readily available or accessible for the typical user. Other than the popularity of an application based on downloads or reviews based on utility and function, users have little knowledge regarding the trustworthiness of a mobile application.

Towards this goal, OTA announced the Online Trust Mobil App Audit. In November 2013, OTA solicited stakeholder feedback from the app developer community, the Federal Trade Commission and the National Telecommunications and Information Administration. Based on this input, OTA published criteria and will initiating an evaluation of leading ecommerce apps in late June 2014. Further aiding developers to enhance their security and privacy best practices, OTA has published summary guidance and third party resources.¹⁶

The goal of the audit is to provide an independent review of best practices highlighting leaders in consumer security, privacy and data stewardship.¹⁷ This effort maps out to the annual OTA Online Trust Audit for commerce, banking and social web sites which OTA has been publishing since 2009.¹⁸

Concurrently trade organizations such as ACT have been raising awareness among the developer community of the importance of security and privacy best practices. These efforts and participation in multi-stakeholder efforts are critical to driving innovation with trusted apps.¹⁹

¹⁴ <http://msdn.microsoft.com/en-us/windowsmobile/dd569931.aspx>

¹⁵ <http://www.symantec.com/code-signing/windows-phone>

¹⁶ <https://otalliance.org/best-practices/mobile-app-privacy-security>

¹⁷ <https://otalliance.org/news-events/press-releases/online-trust-alliance-announces-initiative-promote-mobile-security>

¹⁸ <https://otalliance.org/HonorRoll.html>

¹⁹ <http://actonline.org/projects/privacy-dashboard/>

IV. Security Lifecycle and Updates:

Not unlike managing a web site, the security of mobile apps and devices needs to be on a recurring basis. The life cycle of an app, device and operating system are critical considerations for the mobile ecosystem including support from both the platform and carrier providers. OTA recommends the creation of an industry best practice or standard offering security support for a minimum period beyond the typical purchase contract of the phone. Existing practices are four years, yet according to industry research the majority of Android devices are running the latest OS.²⁰ While there are multiple factors impacting this data including non-upgradable hardware and customized OS versions by carriers, it illustrates the challenges in updating users to current software releases.

Distributing security updates efficiently and effectively continue to plague the industry. Not unlike automatic OS and browser security updates now offered on traditional PCs, mobile security updates should be automatically pushed to users by default. Unfortunately today this is not the common practice in part due to the integration of feature enhancements. Typical security updates require acceptance of new terms of service, and users may potentially lose features or have other default programs installed. Further impeding these efforts is some security updates are subject to data usage charges. Carriers have an opportunity and pivotal role to provide such trust notifications through their direct and recurring consumer relationships leveraging their billing systems and SMS capabilities.

In conclusion we have a shared responsibility to help prevent and detect malicious applications and provide notice to users. As mobile continues to innovate with new features and applications including ad supported services and data driven financial models. Industry must become stewards of consumer data and help ensure their security and privacy.

OTA looks forward to working with the Commission and other stakeholders developing future best practices, industry standards and codes of conduct leveraging our deep security and privacy expertise. Collectively we can enhance online trust and the vitality of line services.

Sincerely,

Craig D. Spiezle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
<https://otalliance.org>
+1 425-455-7400

²⁰ <http://developer.android.com/about/dashboards/index.html>