VIAFORENSICS
innovative digital forensics and security

1000 Lake Street, Suite 203
Oak Park, IL 60301
Tel: +1 312-878-1100

April 2, 2012

Honorable Larry Strickland, Assistant Secretary
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230`

Dear Assistant Secretary Larry Strickland,

viaForensics respectfully submits this response to the National Telecommunications and Information Administration request for comments ("RFC"), dated March 5, 2012.[1] viaForensics is a CompTIA member company that specializes in cutting edge forensic science[2]. Our areas of focus include computer forensics, mobile forensics, mobile app security, enterprise security, and forensics training. We are the leading experts on Android and iPhone forensics and have developed a suite of unique and innovative enterprise security tools to help corporations reduce risk and protect themselves against data theft, fraud and other threats.

In response to NTIA's "RFC", we are providing comments on issues "associated with mobile apps in general." Comments addressing some alternative issues outlined in the "RFC" have been submitted by CompTIA.

I. Background

Mobile applications have become increasingly popular in the smart phone user community. There are over 500,000 applications in the App Store alone, let alone the Android Market, BlackBerry App World, and other application repositories. While some apps do not deal with personal user information, there are many out there that contain extremely sensitive data.

Various research has been done in the mobile application security realm, and studies have shown that many popular downloaded apps are storing sensitive information insecurely on the actual device. In July 2011, viaForensics analyzed 100 popular iPhone and Android applications to determine whether they were storing sensitive user data unencrypted. Each app was assigned a 'Pass', 'Warn', or 'Fail', depending on the sensitivity of the information that was recovered. Out of 100 applications, only 17 received a Pass rating. The failing apps were found to store user passwords, partial credit card numbers, names and addresses, private e-mail or message content, or GPS location data (viaForensics, 2011).

[1] Federal Register / Vol. 77, No. 43 / Monday, March 5, 2012 / Notice
[2] The Computing Technology Industry Association has filed separate comments dated April 2, 2012.

VIAFORENSICS
innovative digital forensics and security

1000 Lake Street, Suite 203
Oak Park, IL 60301
Tel: +1 312-878-1100

From these and other findings, it is clear that data security is not always taken into consideration during the application development cycle. One option to remedy this is to perform extensive security audits against an application prior to its release to the public. The following sections outline some of the most common issues in mobile device and application security, as well as some recommendations for both consumers and application developers.

II. Accountability mechanisms (to enable companies to demonstrate how they are implementing the Consumer Privacy Bill of Rights)

viaForensics works with numerous companies, helping them to identify how to create a secure mobile environment, of which privacy is one of the main concerns. We support a self-regulatory approach and invite these companies to implement a variety of security measures. Here is a list of the most common security issues that are seen when forensically analyzing mobile applications.

Caching personal data: As mentioned in the introduction, app developers will often store sensitive data in plain text on the device. This can include usernames, passwords, financial account numbers and balances, and more.

GPS Location data: Some applications may ask the user whether they wish to store their current location. As an example, a bank application might use GPS coordinates in order to determine which ATM or branch locations are closest to the user. In some instances, the application might be storing the approximate location of the device as well as the date and time that it was in that location.

Network Attacks: If the device is connected to Wi-Fi, there are some trivial network attacks that could potentially intercept the data being sent from the application server to the mobile device. If proper settings are not in place, an attacker could retrieve user credentials and any other information that can be seen within the application.

Platform Specific Issues: In some instances, even though the application was developed in a secure manner, the device it is running on could introduce vulnerabilities. For example, some smart phones will actually capture what is being displayed on the screen and save these images as pictures on the device. While the application developer is not explicitly caching this information, it can still be forensically recovered.

Lack of peer review and security testing: Finally, one of the most common security issues is that applications are being released to the public without extensive peer review or third party security audits being performed.

1000 Lake Street, Suite 203
Oak Park, IL 60301
Tel: +1 312-878-1100

viaForensics believes that in order to create an environment where companies are able to honor the privacy practices that they may have listed. Above are various types of security issues that need to be addressed before a company can make adequate privacy claims.

III. Recommendations/"Best Practices"

Here is what we recommend that every company undertake in terms of security in application development in order to protect consumer privacy.

1. **Peer code review**: Perform a peer code review to check for common programming mistakes or insecure data storage
2. **Security testing**: Have your mobile app audited by a third party to thoroughly analyze the data that is being stored or transmitted.
3. **Avoid caching data**: If it is absolutely necessary to store data on the device, encrypt that data, then make certain that the encryption keys cannot easily be located.
4. **Education**: Seek training in *secure* mobile development. It is important to gain an understanding of each platform in order to be aware of the vulnerabilities for each device (i.e. the platform specific issues mentioned earlier).
5. **Utilize 2-factor**: For applications that contain sensitive data, it is advised that two-factor authentication be implemented. This provides an added layer of security for the user.
6. **Eliminate poor choices the user might make:** Consider strategies which eliminate, or at least limit, the chance of a user making a poor decision when it comes to security (i.e. offering a "Remember me" option for user credentials, which will often times store these items on the device).

We further recommend that consumers take various precautions to protect personal information that might be stored on his/her mobile device.

1. **Use a passcode**: Not only does setting a device passcode/PIN prevent an unauthorized user from gaining access to your data, on some phones, enabling a passcode will even take the added step of encrypting your user data. The longer and more complex the passcode, the less chance there is of an attacker being able to use techniques to bypass it.
2. **Avoid "Remember me" option when logging into apps**: Some applications will allow the user to remember or save the username (and sometimes password). If a particular application contains sensitive data, avoid using these options.
3. **Avoid "Use current location" unless necessary**: Many applications will ask the user for permission to use their current location. While this information is typically required in order to use a certain feature within the app, be aware that this information will likely be stored on your device (including GPS coordinates and a date and time for each).

VIAFORENSICS
innovative digital forensics and security

1000 Lake Street, Suite 203
Oak Park, IL 60301
Tel: +1 312-878-1100

4. **Always use a trusted data network:** When connecting to Wi-Fi access points, ensure that you are connecting to a "known" access point at work, home, or elsewhere. Connecting to untrusted, public networks will increase the chance of an attacker intercepting personal data being sent to or from your device.
5. **Know your apps**: Understand the type of data that is potentially being stored insecurely on your device. If you see it on your screen, assume that it can be recovered.

IV. Closing Remarks

viaForensics applauds the Department of Commerce and NTIA for its leadership in undertaking the very important task of identifying ways to create a more secure mobile application development process as well as seeking suggestions for relevant and timely privacy topics. As a company who focuses much research and development in the area of mobile device and application security, viaForensics is very interested participating in the multistakeholder process in coordination with CompTIA to provide our expertise and industry insights to develop solutions to the important issues raised in the RFC.

Bibliography

viaForensics. (2011, July). *Mobile App Security Study.* Retrieved March 30, 2012, from https://viaforensics.com/resources/white-papers/appwatchdog-findings-mobile-app-security-iphone-android/