

Mornay Walters

Chief Executive Officer

Seecrypt Group Inc.

Witch-Hazel Avenue,

1004 Teak Close,

Eco Fusion 5, Block C,

Ground Floor,

Highveld, Centurion

ZA

mornay.walters@seecrypt.com

Seecrypt Secure Voice:

mornay.walters@seecrypt.com

May 30, 2014

Federal Trade Commission

Title: Notice and Request for Public Comments

Subject Category: FTC Invites Further Public Comment on Mobile Security;

Project No. P145408

Seecrypt Group Inc., a privately owned and funded software development company specializing in secure communications technologies tailor-made for everyday use, thanks the Federal Trade Commission for the opportunity to comment on this important topic. Seecrypt has users in more than 215 countries. The development and network operations of SeeCrypt are located in Pretoria, South Africa.

For more information about Seecrypt and SC3, visit www.seecrypt.com, or please read "[The Cost of the Internet: Our Freedom.](#)"

Q: How can platforms create robust development environments while limiting the potential for abuse by privacy-infringing or malicious third-party applications? Commenters may interpret the term "application" broadly to include any mobile software (*e.g.*, native, web-based, etc.) that has access, via a platform, to consumers' personal information or device resources.

Response:

A good example of compliance can be found in the online merchant sector where vendors can be certified as PCI compliant. <https://www.pcisecuritystandards.org/> Depending on the operating system and applications that share information, some applications can gather any information on a mobile phone and without a compliance standard of some sorts; the protection of personal information will continue to be eroded. Examples of compliance could be for children's applications, medical and communication.

Q: Have particular design approaches proven more or less effective than others in protecting consumer privacy and security?

Response:

We don't believe design approaches are to blame for the issue of privacy invasion, but rather the end goal of the product by the developer and how the information that is gathered and stored is protected by the developer / service provider.

Q: What, if any, are the trade-offs between different approaches to providing developers with access to consumers' personal information or device resources?

Response:

With the release of Apple iOS 7, Apple made it difficult for developers to capture certain device information like the IMEI number of a mobile device, which is unique for each device. This approach by Apple made it more difficult for a developer and supplier of the product to pin point if the same device has been used by the user for accessing the application, and now the developer have to rely on different forms of authentication.

While this is a win for privacy from a device perspective, as the vendor no longer has access to a phone device ID, the user may be asked to supply other information for application authentication and tracking which could place the user at more risk.

Secure Distribution Channels:

Q: What role should platforms play in creating secure distribution channels, such as app stores, for mobile applications?

Response:

Review, revoke and certification with grading. Depending on the level of grading, certain applications could be certified "safe for children's use" this certification will cost money but end users would most probably choose to buy safe / certified products as opposed to download free apps with potential malicious content.

Q: Is application review and testing scalable given the explosive growth of mobile applications? What techniques have proven effective in detecting malicious or privacy-infringing applications?

Response:

Yes it is possible to scale test by using automated tests that can determine exactly what information is captured by the application. This however will only assist in the certification and grading process.

Q: Do smaller players in the mobile ecosystem, such as third-party app stores, have the resources to deploy such techniques?

Response:

Yes, and in fact smaller boutique players may follow far more stringent conditions, which may attract vertical applications for a more focused market. i.e. banking sector / children's market.

Q: Does limiting application distribution to a single channel provide substantial security benefits? What, if any, are the trade-offs of this approach?

Response:

To some degree yes, but it places strain on the free market process.

Q: What are potential alternative approaches to detecting or impeding malicious or privacy-infringing applications on end-user devices?

Response:

There are no real alternatives outside vendor certified applications that is suitable for a specific market / application with legal & financial claw back if any breach occurs.

Q: What resources (*e.g.*, application programming interfaces, development guides, testing tools, etc.) are available for third-party developers interested in secure application development?

Response:

Developing a secure application starts with the aptitude towards security and the goal of the application. Plenty of tools, information and best practice examples exist. Some open source, some commercial. It's interesting to note that most of today's security applications contains open source components i.e. open SSL.

Q: Is the developer community taking advantage of these resources? Are they making common security mistakes?

Response:

Those that understand security yes, but sadly many developers and users within the community continue to ignore these issues and warning signs.

Q: Do consumers have the information they need to evaluate the security of an application? Are they aware of potential security risks (*e.g.*, the insecure transmission of data)? Are there ways to make the security of applications more transparent to the end-user?

Response:

It starts with education. The banking sector has been busy educating the market for 20 years yet still faces an uphill battle. It will take a concerted effort of many agencies, industry and commissions to educate the user that one can no longer trust any application on face value.

Q: What more can platforms and other industry players do to ensure that third-party developers have the resources and incentives necessary to implement secure development practices?

Response:

Co-operation and access to security elements. Many times the issue is with the vendor or industry player and not the 3rd party supplier.

Q: What is the security lifecycle of a mobile device – that is, how long is a mobile device supported with respect to security? Do companies distinguish between a mobile device’s general product lifecycle and its security lifecycle? What factors – technical, policy, or business – affect the length of a mobile device’s security lifecycle?

Response:

Depending on economics, hardware and software design average life cycle is 5 years, as phones do get passed on from user to user. In many developing countries older devices are being dumped at discount prices extending the life of these devices past 5 years to as much as 8 years.

Q: What are consumer expectations with respect to the security lifecycle of their mobile devices? Do consumers have the appropriate information (*e.g.*, at the time of purchase) to factor security into their device purchasing decision? Do consumers receive notice when a device has reached “end-of-life” with respect to security support?

Response:

Consumers are currently slaves to brands and have almost no say in the lifecycle or security of their devices. While security updates are in the order of the day, information about the update remains difficult to find while some update will be met with suspicion given the current revelations and as such users may ignore updates.

Q: What are the challenges in creating, testing, and distributing security updates to end-user devices? What, if any, are the implications of slow update cycles? Are there steps that platforms, manufacturers, telecommunications carriers, and other players can take to streamline this process?

Response:

Certification, good information and feedback coupled with forced updates should be considered, but only when users fail to secure or follow the recommendations by a vendor or service provider.

Again, thank you very much for this opportunity to comment.

Sincerely,

Mornay Walters, CEO
Seecrypt