**FCC Consumer Advisory Committee**
**Recommendation Regarding Mobile Device Security**

As more Americans use mobile devices to store and access sensitive information, it is increasingly important to provide tools for data protection and privacy. In addition to personal information, many consumers are using private devices to access workplace data. A recent study shows that 72% of Millennials have connected to a non-password protected public Wi-Fi hotspot in the past month.[1] Consumers are aware of the risks that come with an unsecure device but only 50% are acting to protect their devices.[2]

CTIA[3], the National Cyber Security Alliance[4], device manufacturers, OS platform providers, carriers, local governments and consumer organizations are all working to educate consumers on these issues. Additionally, a number of app developers have created products that assist consumers through security scans, preference settings, and locating and remotely wiping lost and stolen devices.

Mobile device technology is fast-moving and consumers are embracing new features such as mobile wallets and health monitoring. As operating systems update and devices gain new features, consumers need to familiarize themselves with the security needs and privacy concerns of their devices.

Many consumers view cyber security and privacy concerns as one and the same. This creates a need to educate and empower on both topics concurrently. The Consumer Advisory Committee applauds the FCC for its existing efforts in working to educate consumers about mobile device security and privacy, including the upcoming Mobile Device Protection Tutorial event.

In recognition of October as National Cyber Security Awareness Month, the Consumer Advisory Committee recommends that the Federal Communications Commission consider the following measures to increase consumer understanding and interest in mobile device security:

1. Convening a workshop focused on mobile device security and privacy best practices to assist the FCC in developing consumer advisories and education resources;
2. Hosting a "Data Jam" type event with a theme of mobile device security and privacy best practices[5];

[1] http://staysafeonline.org/download/datasets/10610/Raytheon%20survey%202014.pdf
[2] http://www.ctia.org/resource-library/press-releases/archive/wireless-consumers-cyberthreats-protect-themselves
[3] http://www.ctia.org/your-wireless-life/consumer-tips/tips/cybersafety-tips
[4] www.stopthinkconnect.org/resources
[5] http://www.opm.gov/blogs/Director/2014/1/28/OPM-Co-Hosts-Data-Jam/

3. Enhancing the existing FCC Security Checker (http://www.fcc.gov/smartphone-security) web interface to include:

   preselecting the OS when accessed from a mobile device

   adding more detailed tutorials to explain how to adjust the settings

   including accessible video tutorials;
4. Continuing to work with CTIA, device manufacturers, carriers, and OS developers to improve the consumer experience and usability as it relates to security- and privacy-enhancing techniques;
5. Coordinating carefully planned and funded Public Service Announcement campaigns aimed at educating consumers on device security and privacy;
6. Encouraging innovation in mobile device security and privacy;
7. Developing new FCC-hosted education materials on specific topics. These topics could include but are not limited to: mobile payment security best practices, the importance of two factor authentication, security tips when accessing public Wi-Fi hotspots, and the relationship between security and accessibility;
8. Utilizing the FCC Complaint Call Center in Gettysburg and web complaint submission process to direct consumers to existing FCC educational resources on mobile device security and privacy;
9. Considering any recommendations put forth by the FCC's Technological Advisory Council and its Cyber Security Working Group on these topics.

Adopted unanimously: October 20, 2014

Respectfully submitted:
Debra R. Berlyn, Chairperson
FCC Consumer Advisory Committee