Cullen | Dykman

FCC Releases a "Smartphone Security Checker" to Help Consumers Protect Their Mobile Devices

January 11, 2013

In the world of electronic data, the information we send and receive is not limited to solely computer generated files, but also includes information stored on mobile devices. As this technology advances, so does the importance of protecting against unwanted intrusions.

On December 18, 2012, the Federal Communications Commission ("FCC"), and its public and private sector partners, released a new online tool called the "Smartphone Security Checker." The tool was created to help consumers protect their mobile devices from smartphone-related cyber security threats. According to the news release, "[a]lmost half of Americans now own a smartphone and close to 20% have been the victim of mobile cybercrime." Consequently, consumers should be aware of the simple ways— many of which are already built into the phone —to help protect their phones from unwelcome breaches of privacy.

Put simply, the Smartphone Security Checker is a 10-step security checklist for the four major cell phone operating systems: 1) Android; 2) Apple iOS; 3) BlackBerry; 4) and Windows Phone. A majority of the tips provided on the checklist are similar, but the FCC included links to each of the operating system's websites for instructions on how to perform particular tasks. The checklist takes about five minutes to read through, and includes information on how to:

- Set pins and passwords for your smartphone;
- Download security apps that enable remote locating and data wiping;
- Back-up the data on your smartphone if your device is lost or stolen;
- Wipe data on your old phone and where to go to donate, resell or recycle it; and
- Safely use public Wi-Fi networks and what steps to take if your phone is stolen.

A special thanks to Sean R. Gajewski, a law clerk at Cullen and Dykman, for help with this post.