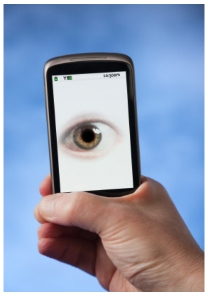
Is Your Mobile Device Watching You?

December 1, 2011 by Vivek Krishnamurthy



A developer for Google's Android mobile phone operating system has exposed what has the potential to be the most significant user privacy security vulnerability ever discovered in any computing device.

In a video posted to YouTube, Connecticut-based developer Trevor Eckhard has demonstrated how a program called Carrier IQ logs an astonishing amount of information about every aspect of mobile device use — from the full-text of SMS messages to the URL of every website visited using the device, not to mention every single keystroke that a user enters into their phone or tablet.

The Carrier IQ software is made by an eponymous company based in Silicon Valley (www.carrieriq.com) and is now known to come preinstalled on Android phones sold by many major carriers, including Sprint in the United States. The software launches automatically whenever a device on which it is installed is powered up, and there appears to be no way to disable or delete the software without "rooting" the device. It has not yet been confirmed whether the software is preinstalled on devices running operating systems other than Android, although this seems very likely given that a media alert issued by Carrier IQ earlier this month explains that its software is used for "counting and measuring operational information in mobile devices" including "feature phones, smart phones and tablets."

In the same media alert, Carrier IQ denied that its software was being used to "record[] keystrokes or provid[e] tracking tools." This denial appears to be contradicted by Mr. Eckhart's YouTube video, although in fairness to Carrier IQ, the video does not actually demonstrate the information collected by the software being transmitted to a mobile phone operator.

It is, of course, entirely possible that the potential the Carrier IQ software seems to provide for tracking nearly everything an individual does on their mobile device cannot actually be realized due to other aspects of the software architecture. If this is the case, Carrier IQ needs to explain that the user tracking potential of its software is the result of a programming oversight and move quickly to patch its software. If, on the other hand, the Carrier IQ software can be used by a mobile phone company to capture keystroke, phone call, SMS, or URL information, the company needs to inform the public immediately. One does not need a very fertile imagination to see what a formidable surveillance tool Carrier IQ might be in the hands of a totalitarian government, and users in such countries ought to know whether their mobile devices can be used to expose intimate personal information.

More generally, the Carrier IQ incident offers an object lesson on the importance of collecting and retaining the least amount of data required to accomplish a given task. There is no reason to doubt Carrier IQ's statement in its media alert that its software is designed to "assist operators and device manufacturers in delivering high-quality products and services to their customers" by "counting and measuring operational information in mobile devices." That being said, there is no reason that keystroke, phone number, URL, or SMS data needs be collected in the level of detail in which Carrier IQ seems capable to optimize mobile devices or their network use. Reducing the amount of data collected to the bare minimum required is not only a good strategy for protecting user privacy and preventing data breaches, but it also helps companies avoid the glare of negative publicity when overbroad data collection capabilities are revealed.