Post-Snowden, iPhone 6 encryption fans safety debate

September 28 2014, by Nancy Owano

Encryption technology in the iPhone 6 has taken root in a scales-of-justice debate between privacy supporters and public safety officials. Apple is using a more advanced encryption technology.

A person's e-mails, contacts, images, bank account numbers, and other sensitive information have a level of protection in the iPhone 6 that

would make it difficult for government agencies to access the information. As one side of the argument goes, that is all quite good for the worker who can go about his business with the confidence that nobody will see his communications, but who may suffer a change of heart if his child were to be abducted and officials told him they recovered a phone but could not decode it. An encrypted personal messaging device is an attractive thought but, viewed in opposing arguments, may also be a haven for terrorists and criminals. A key voice on the public side has been FBI Director James Comey. "I am a huge believer in the rule of law," he said, "but I also believe that no one in this country is beyond the law," in addressing reporters last week. "What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law."

A report by David Sanger and Brian Chen in The *New York Times* that talks about how law enforcement agencies feel about the iPhone 6 security and what the technology entails indicates arguments that are not easy to dismiss no matter which side one takes over privacy rights and public safety. A key concern among law enforcement officials is that, said The New York Times, "the smartphone is the first of a post-Snowden generation of equipment that will disrupt their investigative abilities." The Washington Post similarly said last week that "The rising use of encryption is already taking a toll on the ability of law enforcement officials to collect evidence from smartphones. Apple in particular has been introducing tough new security measures for more than two years that have made it difficult for police armed with cracking software to break in. The new encryption is significantly tougher, experts say."

Apple said that on devices running iOS 8, personal information such as photos, messages (including attachments), mail, contacts, call history and reminders is placed under the protection of your passcode. The phone encrypts mail, photos and contacts based on a complex mathematical

algorithm that uses a code created by, and unique to, the phone's user, reported Sanger and Chen.

"Apple has never worked with any government agency from any country to create a 'back door' in any of our products or services. We have also never allowed any government access to our servers. And we never will," said the company's privacy statement. "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."

An iOS forensics expert, Jonathan Zdziarski, praised Apple for adopting its privacy posture, saying it meant improved security by marrying encryption to the PIN. At the same time, he said, law enforcement would not find it impossible to go after information they wanted.

"Apple has done a great job of breaking a number of law enforcement forensics tools and features with the release of iOS 8. Some existing features are still likely to work, however." As important, Zdziarski attempted to examine both sides of the coin, from privacy to law enforcement forensics. Consider, he said, that by improving the security of their products, Apple has improved it for everyone, including judges, the military and many others. "If you're going to weaken security to make forensics possible, you're also weakening it for everyone, opening the door for foreign governments and cyber criminals to attack all of us. For the sake of privacy and overall security, the only logical solution is to make products as secure as possible, and let good detective work do the crime solving, rather than an easy button."

No doubt this is not the last we will hear on this debate. Google has said it too is planning to enable an encryption system by default on the next version of Android.