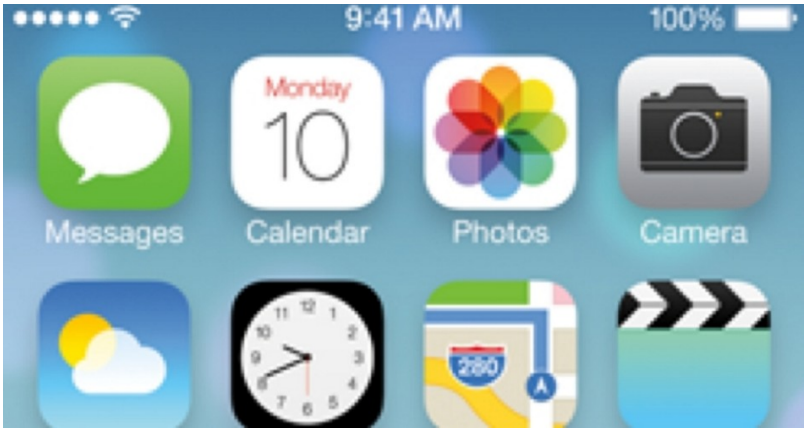
New American

Written by **Joe Wolverton, II, J.D.** on September 11, 2013

All Smartphone Data Exploited by Specialized NSA Teams



The National Security Agency (NSA) has teams devoted to cracking and monitoring every type of smartphone, including the iPhone, Android devices, and the Blackberry, according to a report published by the German magazine *Der Spiegel*.

Once the team has bypassed security measures built into these popular devices, all user data stored on them is instantly accessible to the surveillance squad.

Based on information gleaned from a cache of documents produced by the NSA and its British counterpart, GCHQ, the magazine reports that the intelligence agencies have mustered specialized teams assigned to work on developing advanced surveillance measures particular to the type of phone.

The full panoply of data stored on the phone is then susceptible to the surveillance and being stored by the snoops; this includes call logs, contact lists, text messages, notes, and GPS location markers.

According to its analysis of the internal documents, *Der Spiegel* reports that there is nothing in the information it obtained indicating that the NSA is conducting the type of wholesale, dragnet surveillance of smartphones as was revealed earlier this summer by Edward Snowden.

This capability exposes millions of people worldwide to the constant view of agents of the NSA. As reported by *Der Spiegel*:

> In Germany, more than 50 percent of all mobile phone users now possess a smartphone; in the UK, the share is two-thirds. About 130 million people in the US have such a device. The mini-computers have become personal communication centers, digital assistants and life coaches, and they often know more about their users than most users suspect.

The documents cited in the magazine's story indicate that the NSA scrambled to keep up with the proliferation of smartphones. As the devices were adopted by more and more telecommunications customers, the spies initiated new programs specifically created to crack the technologically advanced phones. *Der Spiegel* describes the push to put the popular devices under the NSA's ever-watchful eye:

> The NSA tackled the issue at the same speed with which the devices changed user behavior. According to the documents, it set up task forces for the leading smartphone manufacturers and operating systems. Specialized teams began intensively studying Apple's iPhone and its iOS operating system, as well as Google's Android mobile operating system. Another team worked on ways to attack BlackBerry, which had been seen as an impregnable fortress until then.

Apparently, unlike PRISM and other NSA programs, the agency didn't work with the device manufacturers or suppliers to help with the smartphone hacking. Both Blackberry and Google were quoted in the story as saying that they don't participate with government surveillance and that there is no "backdoor access" granted to the NSA or any other spy organization.

In this case, then, it seems that the vulnerability comes not from the maker, but from the user. The magazine reports that a majority of smartphone users take a very "carefree approach" to the security

they employ on their device. Perhaps more frightening than the lackadaisical attitude of the end user of the smartphones is the frank tone to the NSA's instructions on how to exploit their "targets"' lack of safeguards.

> According to one NSA presentation, smartphone users demonstrate "nomophobia," or "no mobile phobia." The only thing many users worry about is losing reception. A detailed NSA presentation titled, "Does your target have a smartphone?" shows how extensive the surveillance methods against users of Apple's popular iPhone already are.

For so long, iPhones were thought to be a safer choice than the myriad devices in the same category that run on Google's Android operating system. Apparently, there is no hiding from the never-blinking eye of the Obama administration.

In fact, the scope of the NSA's ability to retrieve and examine information stored on the iPhone is remarkable even in this era of daily disclosures of NSA violations of privacy. Again, from *Der Spiegel*:

> Given the targets it defines, the NSA can select a broad spectrum of user data from Apple's most lucrative product, at least if one is to believe the agency's account.
>
> The results the intelligence agency documents on the basis of several examples are impressive. They include an image of the son of a former defense secretary with his arm around a young woman, a photo he took with his iPhone. A series of images depicts young men and women in crisis zones, including an armed man in the mountains of Afghanistan, an Afghan with friends and a suspect in Thailand.

Typically, many Americans will respond to these revelations with "I have nothing to fear because I've done nothing wrong." But "wrong" in the eyes of the federal government includes things that might cause discomfort were they to be put out to the public.

Imagine, all the photos and all the text messages stored on your smartphone being accessed and archived by the federal government. While likely there is nothing illegal, there may in fact be something potentially embarrassing. Next, imagine that every bit of compromising content was held by the federal government and liable to be published one way or another in a way that threatens your family, your career, and your well-being.

Not to mention the fact that by its very definition, freedom means being free from government monitoring of the lives of people not suspected of committing any crime. This sort of unwarranted dragnet surveillance is not only unconstitutional (and it is), but it is immoral and antithetical to the basic tenets of individual liberty upon which this Republic was founded. A watched society is a prison society, and every member of that society is no longer a citizen, but a suspect.

Joe A. Wolverton, II, J.D. is a correspondent for The New American *and travels frequently nationwide speaking on topics of nullification, the NDAA, and the surveillance state. He can be reached at jwolverton@thenewamerican.com*