

# THE CHRISTIAN POST

## Is NSA Spying on Your Angry Birds Game?

By [Tyler O'Neil](#) , CP Reporter

January 28, 2014 | 4:50 pm

The National Security Agency (NSA) has the capability to access to the personal information of millions of Americans via apps on smartphones, according to documents leaked by former NSA contractor Edward Snowden. A civil liberties expert denounced the misuse of this technology as a violation of the Fourth Amendment.

"Monitoring someone through an app is as valid a means as any other to spy on a legitimate target; monitoring everyone – whether through their apps, their web browsing, or their phone records — is dangerous," Julian Sanchez, [research fellow at the Cato Institute](#), told The Christian Post in a Tuesday statement.

According to reports from The New York Times, the Guardian, and ProPublica, the NSA can discover a person's location, political leanings, and even sexual orientation through mobile mapping, gaming, and social networking apps common to the world's estimated 1 billion smartphones. The documents do not say whether or not NSA has used this capability.

"The size and scope of the program isn't publicly known, but the reports suggest that U.S. and British intelligence easily get routine access to data generated by apps such as the Angry Birds game franchise or the Google Maps navigation service," [NBC reported](#).

"It's important not to get too distracted by the specific technical means of data collection, when what's most important — and not, alas, entirely clear from recent stories — is the scale of and standard for collection," Sanchez told CP. He argued that, so long as the government is monitoring "specific targets subject to court orders," it does not matter how the information is discovered.

The data mining becomes a problem, some privacy advocates believe, when the NSA collects data from everyone, regardless of reasonable cause for suspicion. Sanchez attacked "the larger tendency we've seen in the intelligence community to indiscriminately siphon up reams of data, mostly from innocent people, in order to comb through it later." This, he argued, likely violates the Fourth Amendment.

Sanchez delved into the legal distinctions of the problem. If the NSA pulls the data "live off the wire in transit, rather than obtaining it from the companies," this spying amounts to a wiretap, "which is supposed to be subject to more stringent standards."

On the other hand, a great deal of NSA data collection, Sanchez explained, has been based on the "third party doctrine," where the government requests information from companies. The doctrine assumes that "when you turn information over to a 'third party' — like the phone company or an internet service — you surrender your Fourth Amendment rights in that data," the expert wrote.

The Supreme Court ruling which initiated the doctrine, *Smith v. Maryland*, "turned critically on the idea that people knowingly and voluntarily provide that information," Sanchez explained, arguing that "everyone understands that dialing phone numbers provides the phone company with a record of those numbers."

The Angry Birds situation, Sanchez argued, is much different. While "some smartphone operating systems may ask users to approve general categories of permissions for apps they install, data collection through apps is really pretty opaque." He reported that security researchers have been amazed at the amount of seemingly irrelevant personal information apps collect and transmit.

"Most users probably have no idea exactly what data all their apps collect — and they certainly aren't actively and volitionally providing it even when they do," Sanchez wrote. He argued that this new development, along with other recent situations involving internet privacy, is "an indication that the 'third party doctrine' is long overdue for an overhaul."