Spy Agencies Tap Data Streaming From Phone Apps

James Glanz, Jeff Larson, Andrew W. Lehren

- Jan. 27, 2014

When a smartphone user opens Angry Birds, the popular game application, and starts slinging birds at chortling green pigs, spies could be lurking in the background to snatch data revealing the player's location, age, sex and other personal information, according to secret British intelligence documents.

In their globe-spanning surveillance for terrorism suspects and other targets, the National Security Agency and its British counterpart have been trying to exploit a basic byproduct of modern telecommunications: With each new generation of mobile phone technology, ever greater amounts of personal data pour onto networks where spies can pick it up.

According to dozens of previously undisclosed classified documents, among the most valuable of those unintended intelligence tools are so-called leaky apps that spew everything from the smartphone identification codes of users to where they have been that day.

The N.S.A. and Britain's Government Communications Headquarters were working together on how to collect and store data from dozens of smartphone apps by 2007, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor. Since then, the agencies have traded recipes for grabbing location and planning data when a target uses Google Maps, and for vacuuming up address books, buddy lists, telephone logs and the geographic data embedded in photographs when someone sends a post to the mobile versions of Facebook, Flickr, LinkedIn, Twitter and other Internet services.

The eavesdroppers' pursuit of mobile networks has been outlined in earlier reports, but the secret documents, shared by The New York Times, The Guardian and ProPublica, offer far more details of their ambitions for smartphones and the apps that run on them. The efforts were part of an initiative called "the mobile surge," according to a 2011 British document, an analogy to the troop surges in Iraq and Afghanistan. An N.S.A. analyst's enthusiasm was evident in the breathless title — "Golden Nugget!" — given to a slide for a top-secret talk in 2010 that described iPhones and Android phones as rich resources, another document noted.

The scale and the specifics of the data haul are not clear. The documents show that the N.S.A. and the British agency routinely obtain information from certain apps, particularly those introduced earliest to cellphones. With some newer apps, including Angry Birds, the agencies have a similar ability, the documents show, but they do not make explicit whether the spies have put that into practice. Some personal data, developed in profiles by advertising companies, could be particularly sensitive: A secret British intelligence document from 2012 said that spies can scrub smartphone apps to collect details like a user's "political alignment" and sexual orientation.

President Obama announced new restrictions this month to better protect the privacy of ordinary Americans and foreigners from government surveillance, including limits on how the N.S.A. can view the metadata of Americans' phone calls — the routing information, time stamps and other data associated with calls. But he did not address the information that the intelligence agencies get from leaky apps and other smartphone functions.

And while Mr. Obama expressed concern about advertising companies that collect information on people to send tailored ads to their mobile phones, he offered no hint that American spies have routinely seized that data. Nothing in the secret reports indicates that the companies cooperated with the spy agencies to share the information; the topic is not addressed.

The agencies have long been intercepting earlier generations of cellphone traffic like text messages and metadata from nearly every segment of the mobile network — and, more recently, computer traffic running on Internet pipelines. Because those same networks carry the rush of data from leaky apps, the agencies have a ready-made way to collect and store this new resource. The documents do not address how many users might be affected, whether they include Americans or how often, with so much information collected automatically, analysts would see personal data.

“N.S.A. does not profile everyday Americans as it carries out its foreign intelligence mission,” the agency wrote in response to questions about the program. “Because some data of U.S. persons may at times be incidentally collected in N.S.A.’s lawful foreign intelligence mission, privacy protections for U.S. persons exist across the entire process.” Similar protections, the agency said, are in place for “innocent foreign citizens.”

The British spy agency declined to comment on any specific program, but said all its activities complied with British law.

Two top-secret flow charts produced by the British agency in 2012 showed incoming streams of information skimmed from smartphone traffic by the Americans and the British. The streams were divided into “traditional telephony” — metadata — and others marked “social apps,” “geo apps,” “http linking,” webmail, MMS and traffic associated with mobile ads, among others. (MMS refers to the mobile system for sending pictures and other multimedia, and http is the protocol for linking to websites.)

In charts showing how information flows from smartphones into the agency’s computers, analysts included questions to be answered by the data, like “Where was my target when they did this?” and “Where is my target going?”

As the program accelerated, the N.S.A. nearly quadrupled its budget in a single year, to $767 million in 2007 from $204 million, according to a top-secret analysis written by Canadian intelligence around the same time.

Even sophisticated users are often unaware of how smartphones offer spies a unique opportunity for one-stop shopping for information. “By having these devices in our pockets and using them more and more,” said Philippe Langlois, who has studied the vulnerabilities of mobile phone networks and is the founder of the Paris-based company Priority One Security, “you’re somehow becoming a sensor for the world intelligence community.”

Smartphones almost seem to make things too easy. Functioning as phones to make calls and send texts and as computers to surf the web and send emails, they both generate and rely on data. One secret report showed that just by updating Android software, a user sent more than 500 lines of data about the phone’s history and use onto the network.

Detailed Profiles

Such information helps mobile advertising companies, for example, create detailed profiles of people based on how they use their mobile device, where they travel, what apps and websites they open, and other factors. Advertising firms might triangulate web shopping data and browsing history to guess whether someone is wealthy or has children.

The N.S.A. and the British agency busily scoop up this data, mining it for new information and comparing it with their lists of intelligence targets.

One secret British document from 2010 suggested that the agencies collected such a huge volume of “cookies” — the digital traces left on a mobile device or a computer when a target visits a website — that classified computers were having trouble storing it all.

“They are gathered in bulk, and are currently our single largest type of events,” the document said.

The two agencies displayed a particular interest in Google Maps, which is accurate to within a few yards or better in some locations. Intelligence agencies collected so much data from the app that “you’ll be able to clone Google’s database” of global searches for directions, according to a top-secret N.S.A. report from 2007.

“It effectively means that anyone using Google Maps on a smartphone is working in support of a GCHQ system,” a secret 2008 report by the British agency said.

(In December, The Washington Post, citing the Snowden documents, reported that the N.S.A. was using metadata to track cellphone locations outside the United States and was using ad cookies to connect Internet addresses with physical locations.)

In another example, a secret 20-page British report dated 2012 included the computer code needed for plucking the profiles generated when Android users play Angry Birds. The app was created by Rovio Entertainment, of Finland, and has been downloaded more than a billion times, the company has said.

Rovio drew public criticism in 2012 when researchers claimed that the app was tracking users’ locations and gathering other data and passing it to mobile ad companies. In a statement on its website, Rovio says that it may collect its users’ personal data, but that it abides by some restrictions. For example, the statement says, “Rovio does not knowingly collect personal information from children under 13 years of age.”

The secret report noted that the profiles vary depending on which of the ad companies — which include Burstly and Google’s ad services, two of the largest online advertising businesses — compiles them. Most profiles contain a string of characters that identifies the phone, along with basic data on the user like age, sex and location. One profile notes whether the user is currently listening to music or making a call, and another has an entry for household income.

Google declined to comment for this article, and Burstly did not respond to multiple requests for comment. Saara Bergstrom, a Rovio spokeswoman, said the company had no knowledge of the intelligence programs. “Nor do we have any involvement with the organizations you mentioned,” Ms. Bergstrom said, referring to the N.S.A. and the British spy agency.

Another ad company creates far more intrusive profiles that the agencies can retrieve, the report said. The names of the apps that generate those profiles were not given, but the company was identified as Millennial Media, which has its headquarters in Baltimore.

In securities filings, Millennial documented how it began working with Rovio in 2011 to embed ad services in Angry Birds apps running on iPhones, Android phones and other devices.

According to the report, the profiles created by Millennial contain much of the same information as others, but several categories that are listed as “optional,” including ethnicity, marital status and sexual orientation, suggest that much wider sweeps of personal data may take place.

Millennial Media declined to comment for this article.

Possible categories for marital status, the secret report said, include single, married, divorced, engaged and “swinger”; those for sexual orientation are straight, gay, bisexual and “not sure.” It is unclear whether the “not sure” category exists because so many phone apps are used by children, or because insufficient data may be available.

There is no explanation of precisely how the ad company defined the categories, whether users volunteered the information or whether the company inferred it by other means. Nor is there any discussion of why all that information would be useful for marketing — or intelligence.

Unwieldy Heaps

The agencies have had occasional success, at least by their own reckoning, when they start with something closer to a traditional investigative tip or lead. The spies say that tracking smartphone traffic helped break up a bomb plot by Al Qaeda in Germany in 2007, and the N.S.A. boasted that to crack the plot, it wove together mobile data with emails, logins and web traffic. Similarly, mining smartphone data helped lead to the arrests of members of a drug cartel hit squad in the killing of an American Consulate employee in Mexico in 2010.

But the data, whose volume is soaring as mobile devices have begun to dominate the technological landscape, is a crushing amount of information for the spies to sift through. As smartphone data builds up in N.S.A. and British databases, the agencies sometimes seem a bit at a loss on what to do with it all, the documents show. A few isolated experiments provide hints as to how unwieldy the data can be.

In 2009, the American and British spy agencies each undertook a brute-force analysis of a tiny sliver of their cellphone databases. Crunching just one month of N.S.A. cellphone data, a secret report said, required 120 computers and turned up 8,615,650 “actors” — apparently callers of interest. A similar run using three months of British data came up with 24,760,289 actors.

“Not necessarily straightforward,” the report said of the analysis.

The agencies’ extensive computer operations had trouble sorting through the slice of data. Analysts were “dealing with immaturity,” the report said, encountering computer memory and processing problems. The report made no mention of anything suspicious in the data.

Ginger Thompson contributed reporting. Jeff Larson is a reporter at ProPublica.

A version of this article appears in print on Jan. 28, 2014, Section A, Page 1 of the New York edition with the headline: Spy Agencies Tap Data Streaming From Phone Apps. Order Reprints | Today’s Paper | Subscribe