The Washington Post

www.washingtonpost.com | December 4, 2013

Online Story

NSA tracking cellphone locations worldwide, Snowden documents show

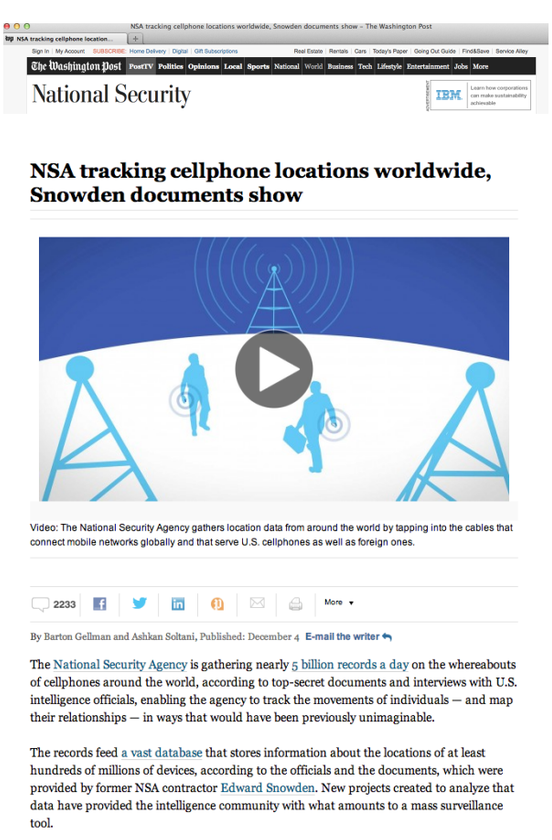
by Barton Gellman and Ashkan Soltani

http://wapo.st/IlaYWp

Copy the above URL into your web browser to view online

The National Security Agency is gathering nearly 5 billion records a day on the whereabouts of cellphones around the world, according to top-secret documents and interviews with U.S. intelligence officials, enabling the agency to track the movements of individuals — and map their relationships — in ways that would have been previously unimaginable.

The records feed a vast database that stores information about the locations of at least hundreds of millions of devices, according to the officials and the documents, which were provided by former NSA contractor Edward Snowden. New projects created to analyze that data have provided the intelligence community with what amounts to a mass surveillance tool.



The NSA does not target Americans' location data by design, but the agency acquires a substantial amount of information on the whereabouts of domestic cellphones "incidentally," a legal term that connotes a foreseeable but not deliberate result.

One senior collection manager, speaking on the condition of anonymity but with permission from the NSA, said "we are getting vast volumes" of location data from around the world by tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones. Additionally, data are often collected from the tens of millions of Americans who travel abroad with their cellphones every year.

In scale, scope and potential impact on privacy, the efforts to collect and analyze location data may be unsurpassed among the NSA surveillance programs that have been disclosed since June. Analysts can find cellphones anywhere in the world, retrace their movements and expose hidden relationships among the people using them.

U.S. officials said the programs that collect and analyze location data are lawful and intended strictly to develop intelligence about foreign targets.

Robert Litt, general counsel for the Office of the Director of National Intelligence, which oversees the NSA, said "there is no element of the intelligence community that under any authority is intentionally collecting bulk cellphone location information about cellphones in the United States."

The NSA has no reason to suspect that the movements of the overwhelming majority of cellphone users would be relevant to national security. Rather, it collects lo-

cations in bulk because its most powerful analytic tools — known collectively as CO-TRAVELER — allow it to look for unknown associates of known intelligence targets by tracking people whose movements intersect.

Still, location data, especially when aggregated over time, are widely regarded among privacy advocates as uniquely sensitive. Sophisticated mathematical techniques enable NSA analysts to map cellphone owners' relationships by correlating their patterns of movement over time with thousands or millions of other phone users who cross their paths. Cellphones broadcast their locations even when they are not being used to place a call or send a text message.

CO-TRAVELER and related tools require the methodical collection and storage of location data on what amounts to a planetary scale. The government is tracking people from afar into confidential business meetings or personal visits to medical facilities, hotel rooms, private homes and other traditionally protected spaces.

"One of the key components of location data, and why it's so sensitive, is that the laws of physics don't let you keep it private," said Chris Soghoian, principal technologist at the American Civil Liberties Union. People who value their privacy can encrypt their e-mails and disguise their online identities, but "the only way to hide your location is to disconnect from our modern communication system and live in a cave."

The NSA cannot know in advance which tiny fraction of 1 percent of the records it may need, so it collects and keeps as many as it can — 27 terabytes, by one account, or more than double the text content of the Library of Congress's print collection.

The location programs have brought in such volumes of information, according to a May 2012 internal NSA briefing, that they are "outpacing our ability to ingest, process and store" data. In the ensuing year and a half, the NSA has been transitioning to a processing system that provided it with greater capacity.

The possibility that the intelligence community has been collecting location data, particularly of Americans, has long concerned privacy advocates and some lawmakers. Three Democratic senators — Ron Wyden (Ore.), Mark Udall (Colo.) and Barbara A. Mikulski (Md.) — have introduced an amendment to the 2014 defense spending bill that would require U.S. intelligence agencies to say whether they have ever collected or made plans to collect location data for "a large number of United States persons with no known connection to suspicious activity."

NSA Director Keith B. Alexander disclosed in Senate testimony in October that the NSA had run a pilot project in 2010 and 2011 to collect "samples" of U.S. cellphone location data. The data collected were never available for intelligence analysis purposes, and the project was discontinued because it had no "operational value," he said.

Alexander allowed that a broader collection of such data "may be something that is a future requirement for the country, but it is not right now."

The number of Americans whose locations are tracked as part of the NSA's collection of data overseas is impossible to determine from the Snowden documents alone, and senior intelligence officials declined to offer an estimate.

"It's awkward for us to try to provide any specific numbers," one intelligence official said in a telephone interview. An NSA spokeswoman who took part in the call cut in to say the agency has no way to calculate such a figure.

An intelligence lawyer, speaking with his agency's permission, said location data are obtained by methods "tuned to be looking outside the United States," a formulation he repeated three times. When U.S. cellphone data are collected, he said, the data are not covered by the Fourth Amendment, which protects Americans against unreasonable searches and seizures.

According to top-secret briefing slides, the NSA pulls in location data around the world from 10 major "sigads," or signals intelligence activity designators.

A sigad known as STORMBREW, for

example, relies on two unnamed corporate partners described only as ARTIFICE and WOLFPOINT. According to an NSA site inventory, the companies administer the NSA's "physical systems," or interception equipment, and "NSA asks nicely for tasking/updates."

STORMBREW collects data from 27 telephone links known as OPC/DPC pairs, which refer to originating and destination points and which typically transfer traffic from one provider's internal network to another's. That data include cell tower identifiers, which can be used to locate a phone's location.

The agency's access to carriers' networks appears to be vast.

"Many shared databases, such as those used for roaming, are available in their complete form to any carrier who requires access to any part of it," said Matt Blaze, an associate professor of computer and information science at the University of Pennsylvania. "This 'flat' trust model means that a surprisingly large number of entities have access to data about customers that they never actually do business with, and an intelligence agency — hostile or friendly — can get 'one-stop shopping' to an expansive range of subscriber data just by compromising a few carriers."

Some documents in the Snowden archive suggest that acquisition of U.S. location data is routine enough to be cited as an example in training materials. In an October 2012 white paper on analytic techniques, for example, the NSA's counterterrorism analysis unit describes the challenges of tracking customers who use two different mobile networks, saying it would be hard to correlate a user on the T-Mobile network with one on Verizon. Asked about that, a U.S. intelligence official said the example was poorly chosen and did not represent the program's foreign focus. There is no evidence that either company cooperates with the NSA, and both declined to comment.

The NSA's capabilities to track location are staggering, based on the Snowden documents, and indicate that the agency is able to render most efforts at communications security effectively futile.

Like encryption and anonymity tools online, which are used by dissidents, journalists and terrorists alike, security-minded behavior — using disposable cellphones and switching them on only long enough to make brief calls — marks a user for special scrutiny. CO-TRAVELER takes note, for example, when a new telephone connects to a cell tower soon after another nearby device is used for the last time.

Side-by-side security efforts — when nearby devices power off and on together over time — "assist in determining whether co-travelers are associated … through behaviorally relevant relationships," according to the 24-page white paper, which was developed by the NSA in partnership with the National Geospatial-Intelligence Agency, the Australian Signals Directorate and private contractors.

A central feature of each of these tools is that they do not rely on knowing a particular target in advance, or even suspecting one. They operate on the full universe of data in the NSA's FASCIA repository, which stores trillions of metadata records, of which a large but unknown fraction include locations.

The most basic analytic tools map the date, time, and location of cellphones to look for patterns or significant moments of overlap. Other tools compute speed and trajectory for large numbers of mobile devices, overlaying the electronic data on transportation maps to compute the likely travel time and determine which devices might have intersected.

To solve the problem of un¬detectable surveillance against CIA officers stationed overseas, one contractor designed an analytic model that would carefully record the case officer's path and look for other mobile devices in steady proximity.

"Results have not been validated by operational analysts," the report said.

Julie Tate contributed to this report. Soltani is an independent security researcher and consultant.