EXHIBIT 7

National Security


$1.1 trillion spending bill unveiled


THE FIX | Winners, losers of spending bill


Feeling blah? These nutrients can help.


Where are 'Idol' stars now?

Little-known surveillance tool raises concerns by judges, privacy activists

By Ellen Nakashima, Published: March 27, 2013 E-mail the writer

Federal investigators in Northern California routinely used a sophisticated surveillance system to scoop up data from cellphones and other wireless devices in an effort to track criminal suspects — but failed to detail the practice to judges authorizing the probes.

The practice was disclosed Wednesday in documents obtained under the Freedom of Information Act by the American Civil Liberties Union of Northern California — in a glimpse into a technology that federal agents rarely discuss publicly.

The investigations used a device known as a StingRay, which simulates a cellphone tower and enables agents to collect the serial numbers of individual cellphones and then locate them. Although law enforcement officials can employ StingRays and similar devices to locate suspects, privacy groups and some judges have raised concerns that the technology is so invasive — in some cases effectively penetrating the walls of homes — that its use should require a warrant.

The issues, judges and activists say, are twofold: whether federal agents are informing courts when seeking permission to monitor suspects, and whether they are providing enough evidence to justify the use of a tool that sweeps up data not only from a suspect's wireless device but also from those of bystanders in the vicinity.

In Northern California, according to the newly disclosed documents, judges expressed concerns about the invasive nature of the technology.

"It has recently come to my attention that many agents are still using [StingRay] technology in the field although the [surveillance] application does not make that explicit," Miranda Kane, then chief of the criminal division of the Northern

Latest from National Security

Man convicted in terror case seeks evidence from warrantless spying


Ellen Nakashima JAN 13
Oregon man guilty of Christmas tree bombing plot opens door for possible constitutional challenge to NSA program.

Fine Print: Missing a moment of fiscal, nuclear courage

Walter Pincus JAN 13
The Cold War is over, but the expense of that fight is still with us.

A hard-edged defender of spy agencies


Greg Miller and Adam Goldman JAN 12
Attorney Robert S. Litt has led an unusually high-profile response to the Snowden leaks.

Snowden, in interview, says his mission's accomplished


Barton Gellman DEC 23
His leaks have fundamentally altered the U.S. government's relationship with its citizens, the rest of the world.

Full coverage: NSA Secrets


Read all of the stories in The Washington Post's ongoing coverage of the National Security Agency's surveillance programs.

The Post Most: World

1 40 more maps that explain the world 

2 Iranian news: U.S. is run by Nazi space aliens 

3 Here's what it means to be Afghanistan's 'most honest man': Low pay and no pro...

4 40 maps that explain the world 

5 Russia refuses visa to U.S. journalist David Satter; writer banned from country for 5 years

California U.S. attorney's office, said in a May 2011 e-mail obtained by the ACLU.

As a result of that, she wrote, "effective immediately, all . . . applications and proposed orders must be reviewed by your line supervisor before they are submitted to a magistrate judge."

The Justice Department has generally maintained that a warrant based on probable cause is not needed to use a "cell-site simulator" because the government is not employing them to intercept conversations, former officials said. But some judges around the country have disagreed and have insisted investigators first obtain a warrant.

"It's unsettled territory," said one U.S. law enforcement official, who spoke on the condition of anonymity because he was not authorized to speak for the record.

In a statement, Christopher Allen, a spokesman for the FBI, said the bureau advises field offices to "work closely with the relevant U.S. Attorney's Office to adhere to the legal requirements" of their respective districts.

One of the problems is there is "scant law" addressing the issue of cell-site simulators, said Brian L. Owsley, a federal magistrate judge in the Southern District of Texas, who in June wrote a rare public ruling on the issue. He denied an application to use a StingRay, in large part because he felt the investigating agent failed to explain the technology or how it would be used to gather the target's cellphone number.

Moreover, the government did not explain what it would do with the numbers and other data "concerning seemingly innocent cell phone users" that were also picked up.

"Neither the special agent nor the assistant United States attorney appeared to understand the technology very well," Owsley wrote. "At a minimum, they seemed to have some discomfort in trying to explain it."

At a recent conference on cellphone tracking issues at Yale University, Owsley said he thought that "there are magistrate judges around the country that are getting these requests and not realizing what these requests are," in some cases perhaps because the agents are not clear about their intent to use the technology.

"By withholding information about this technology from courts in applications for electronic surveillance orders, the federal government is essentially seeking to write its own search warrants," said Linda Lye, a staff attorney for the ACLU of Northern California.

Judges "need the opportunity to require privacy safeguards, such as rules on how to handle the data of innocent people that may be captured by the devices as well," she said.Lye will be arguing the issue on Thursday in a federal case in Arizona, in support of a defendant charged with tax fraud and identity theft. Daniel Rigmaiden, known as "the Hacker" to acquaintances and federal agents, was tracked in part with the use of a StingRay. He has alleged that investigators did not seek a court's approval to use the technology.

"The main concern we have in Rigmaiden is the government was not being forthright with the magistrate when it was seeking to use this device," said Lye, whose organization is one of several that have filed an amicus brief in the case.

The newly disclosed documents suggest that "Rigmaiden was not an isolated case," she said.

The government said it obtained a warrant to track Rigmaiden, but the ACLU is arguing that the government did not present key information about the surveillance device to the magistrate, rendering the warrant invalid.

Chris Soghoian, the ACLU's principal technologist, said cell-site simulators are being used by local, state and federal authorities.

"No matter how the StingRay is used — to identify, locate or intercept — they always send signals through the walls of homes," which should trigger a warrant requirement, Soghoian said. "The signals always penetrate a space protected by the Fourth Amendment."

170 Comments

Discussion Policy

postfan10 wrote:
3/27/2013 11:42 PM EDT

If the police want to use this kind of tool, they should be getting a warrant.

kritik1 wrote:
3/28/2013 5:25 AM EDT

911 cried for better security. Instead we created a security monster. Our Legislature has undermined the Judiciary and given unprecedented powers to the Executive to act for security and ignore the rights of US Citizens on matters of privacy. Our system has become akin to the defunct KGB and in line with the present Iranian Secret Service, where politics rules supreme not the rights of the people of Iran.

Navy_CTT responds:
3/28/2013 5:39 AM EDT

It wasn't just 9-11. Americans demand that the government keep them protected - from hunger, homelessness, illness, old age; in pregnancy and youth; from ignorance and on and on and on.

Government can't keep you in its womb 24/7/365, safe against anything and everything life can throw at you, without controlling you, no more than your parents did when you were 5. It's the same thing. That's why we use the Latin word for "father" - "pater" - as the root of the description for the kind of government we demand and have: "paternalistic".

Obama to announce changes to NSA surveillance on Jan. 17

Bipartisan group of Md. lawmakers seeks limits on drones, other law-enforcement surveillance

What words did Big Tobacco once use to profile homosexuals? Find out here. YouTube

9 Amazing Military Technologies of the Future Kiplinger

what's this

Top World Stories | **Most Popular Videos**

Five award winners; five crash tests

Tina Fey and Amy Poehler's funniest Golden Globe moments

Fighting in Iraq highlights age-old conflict

Sponsored Links

Visa® Black Card™
Introducing the New Stainless Steel Visa Black Card. Apply Today!
BlackCard.com

Healthy Dessert Maker
Make Tasty, All-Natural Desserts At Home With The Dessert Bullet!
www.DessertBullet.com

Making A Move?
No matter the size of your move. Rent with Budget Truck and save BIG.
BudgetTruck.com/Move

Buy a link here