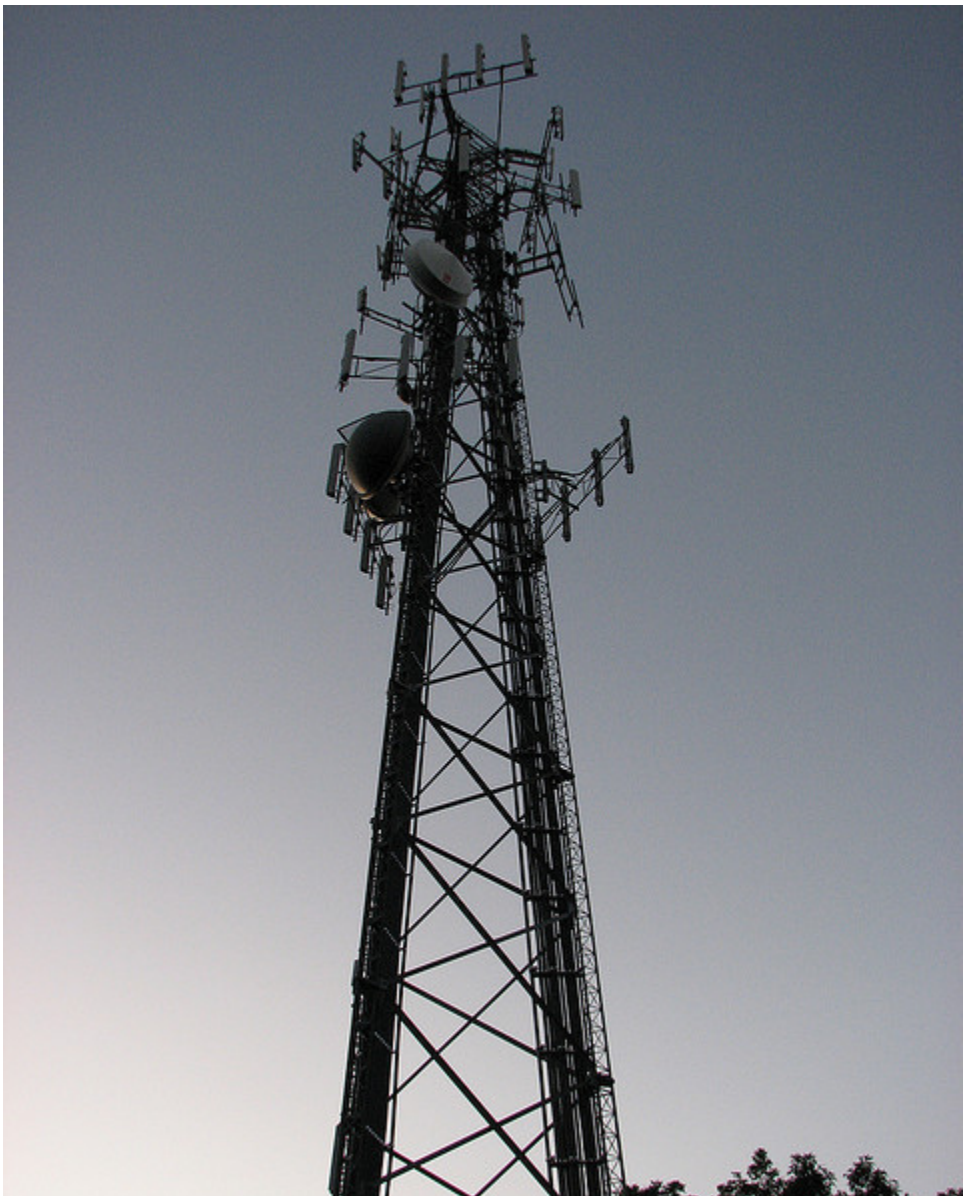
EXHIBIT 11

Federal authorities who used a spy device to spoof a legitimate cellphone tower have conceded that use of the device can be considered a search, in a surprise twist to the government's previous stance.

Threat Level
Privacy, Crime and Security Online
Surveillance

Feds' Use of Fake Cell Tower: Did it Constitute a Search?

By Kim Zetter
11.03.11
5:46 PM



Federal authorities used a fake Verizon cellphone tower to zero in on a suspect's wireless card, and say they were perfectly within their rights to do so, even without a warrant.

But the feds don't seem to want that legal logic challenged in court by the alleged identity thief they nabbed using the spoofing device, known generically as a stingray. So the government is telling a court for the first time that spoofing a legitimate wireless tower in order to conduct surveillance could be considered a search under the Fourth Amendment in this particular case, and that its use was legal, thanks to a court order and warrant that investigators used to get similar location data from Verizon's own towers.

The government is likely using the argument to avoid a court showdown that might reveal how stingrays work and open debate into the tool's legality.

Stingrays spoof a legitimate cellphone tower in order to trick nearby cellphones and other wireless communication devices into connecting to the tower, as they would to a real cellphone tower. When devices connect, stingrays can see and record their unique ID numbers and traffic data, as well as information that points to a device's location. To prevent detection by suspects, the stingray sends the data to a real tower so that traffic continues to flow.

By gathering the wireless device's signal strength from various locations, authorities can pinpoint where the device is being used with much more precision than they can get through data obtained from the mobile network provider's fixed tower location.

According to an affidavit submitted to the court (.pdf) by the chief of the FBI's Tracking Technology Unit, the stingray is designed to capture only the equivalent of header information — such as the phone or account number assigned to the aircard as well as dialing, routing and address information involved in the communication. As such, the government has maintained that the device is the equivalent of devices designed to capture routing and header data on e-mail and other internet communications, and therefore does not require a search warrant.

The device, however, doesn't just capture information related to a targeted phone. It captures data from "all wireless devices in the immediate area of the FBI device that subscribe to a particular provider" — including data of innocent people who are not the target of the investigation, according to the affidavit. FBI policy requires agents purge all data stored in the surveillance tool at the conclusion of an operation, so that the FBI is not collecting "information about individuals who are not the subject of criminal or national security investigations," the affidavit added.

The device in this case was used to track an aircard allegedly used by Daniel David Rigmaiden, a 30-year-old self-described hacker suspected of being the ringleader of an identity theft group that stole millions of dollars by filing bogus tax returns under the names and Social Security numbers of other people.

The thieves operated their scheme for at least three years from January 2005 to April 2008, allegedly filing more than 1,900 fraudulent tax returns involving about $4 million in refunds. The conspirators used more than 175 different IP addresses around the U.S. to file the fake returns.

According to court documents, authorities used a variety of other avenues to track Rigmaiden, including obtaining video footage taken at a Verizon payment kiosk in San Francisco. This presumably was to help identify who had paid in person for an account belonging to a person named Travis Rupard — one of the identities Rigmaiden allegedly used during his crime spree.

Investigators used the stingray to trace the aircard to an apartment complex in Santa Clara, California, according to the FBI affidavit. Court documents indicate the device led investigators "to the general proximity of defendant's usage of the aircard," allowing authorities to narrow the air card's location to three or four apartments in a residential complex.

Rigmaiden has been in custody since May 2008 and is representing himself at the U.S. District Court of Arizona, after dismissing multiple attorneys. The government's assertion about the spy tool comes in response to a motion for discovery that Rigmaiden filed requesting, in part, details of how authorities tracked him.

The government has so far refused to provide information about how the device worked or the techniques they used to monitor the air card, calling such "sensitive investigative techniques" privileged information.

Until now, the U.S. government has asserted that the use of stingray devices does not violate Fourth Amendment rights, and Americans don't have a legitimate expectation of privacy for data sent from their mobile phones and other wireless devices to a cell tower.

But authorities changed their tone in the Rigmaiden case after the defendant argued that using the device to locate a wireless aircard inside an apartment constituted a search, and therefore required a valid search warrant, which he asserts authorities didn't have.

After the judge indicated he'd seek more information about the device, prosecutors conceded that in this case its use could be considered a search. They also argued that its use was covered by a court order and a warrant that authorities used to obtain near real-time tracking information directly from Verizon Wireless. A separate tracking warrant, prosecutors say, wasn't necessary for its fake tower.

Despite the apparent shift in the government's argument in this specific case, it still maintains that stingray devices do not violate American's privacy, since the target doesn't "have a reasonable expectation of privacy in his general location or in the cell site records he transmitted wirelessly to Verizon."

The Metropolitan police in London have used similar technology which takes the surveillance a bit further, according to a recent story in the *Guardian*. The British device can be used to identify all mobile phones in a given area, capture and record the content of calls and remotely disable phones.

Photo: Keith Survell / Flickr

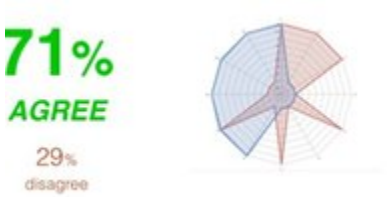
Kim Zetter is a senior reporter at Wired covering cybercrime, privacy, security and civil liberties.

Read more by Kim Zetter

Follow @KimZetter and @ThreatLevel on Twitter.

Female Passenger Groped by TSA Gropes Back, Charged with Battery

Stop Wearing Your Earphones the Wrong Way



Lies, Damned Lies and Data Visualization

- CULTUREAMP

Tags: Surveillance
Post Comment | 49 Comments | Permalink
Back to top

Comments for this thread are now closed.

49 comments

★ 14

Best Community Share Login

dcx_2 · 2 years ago
First they would go after suspected terrorists without warrants. And I did nothing, because I was not a suspected terrorist.

Then they went after garden-variety criminals without warrants. And I did nothing, because I was not a garden variety criminal.

Then they came for the dissidents without warrants. And by this time, it was too late; the precedent had already been set.

Big Brother is watching you.

89 △ | ▽ · Share ›

JB210 · 2 years ago
From the FBI to the Verizon customer living next door: "Well, sure you're in your home, and you're not the subject of our investigation but we're capturing your data anyway, but we promise we won't really look at it, and we promise we'll throw it out when our investigation is done. Trust us. If you don't have anything to hide, why would you even think about any expectation of privacy in your own home?" America - home of the free.

50 △ | ▽ · Share ›

JohnGaltWasHere · 2 years ago
So is it legal for me to put up my own fake cell tower?

20 △ | ▽ · Share ›

smrollins > JohnGaltWasHere · 2 years ago
If it's illegal for any normal (non-government agent) person to set up an interception tower, then it's illegal for any government agent/agency unless they have permission from a court (wiretapping warrant).