EXHIBIT 9

A legal fight over the government's use of a secret surveillance tool has provided new insight into how the controversial tool works and the extent to which Verizon Wireless aided federal agents in using it to track a suspect.

Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight

By Kim Zetter
04.09.13
6:30 AM

Image: rmuser/Flickr

A legal fight over the government's use of a secret surveillance tool has provided new insight into how the controversial tool works and the extent to which Verizon Wireless aided federal agents in using it to track a suspect.

Court documents in a case involving accused identity thief Daniel David Rigmaiden describe how the wireless provider reached out remotely to reprogram an air card the suspect was using in order to make it communicate with the government's surveillance tool so that he could be located.

Rigmaiden, who is accused of being the ringleader of a $4 million tax fraud operation, asserts in court documents that in July 2008 Verizon surreptitiously reprogrammed his air card to make it respond to incoming voice calls from the FBI and also reconfigured it so that it would connect to a fake cell site, or stingray, that the FBI was using to track his location.

Air cards are devices that plug into a computer and use the wireless cellular networks of phone providers to connect the computer to the internet. The devices are not phones and therefore don't have the ability to receive incoming calls, but in this case Rigmaiden asserts that Verizon reconfigured his air card to respond to surreptitious voice calls from a landline controlled by the FBI.

The FBI calls, which contacted the air card silently in the background, operated as pings to force the air card into revealing its location.

In order to do this, Verizon reprogrammed the device so that when an incoming voice call arrived, the card would disconnect from any legitimate cell tower to which it was already connected, and send real-time cell-site location data to Verizon, which forwarded the data to the FBI. This allowed the FBI to position its stingray in the neighborhood where Rigmaiden resided. The stingray then "broadcast a very strong signal" to force the air card into connecting to it, instead of reconnecting to a legitimate cell tower, so that agents could then triangulate signals coming from the air card and zoom-in on Rigmaiden's location.

To make sure the air card connected to the FBI's simulator, Rigmaiden says that Verizon altered his air card's Preferred Roaming List so that it would accept the FBI's stingray as a legitimate cell site and not a rogue site, and also changed a data table on the air card designating the priority of cell sites so that the FBI's fake site was at the top of the list.

Rigmaiden makes the assertions in a 369-page document he filed in support of a motion to suppress evidence gathered through the stingray. Rigmaiden collected information about how the stingray worked from documents obtained from the government, as well as from records obtained through FOIA requests filed by civil liberties groups and from open-source literature.

During a hearing in a U.S. District Court in Arizona on March 28 to discuss the motion, the government did not dispute Rigmaiden's assertions about Verizon's activities.

The actions described by Rigmaiden are much more intrusive than previously known information about how the government uses stingrays, which are generally employed for tracking cell phones and are widely used in drug and other criminal investigations.

The government has long asserted that it doesn't need to obtain a probable-cause warrant to use the devices because they don't collect the content of phone calls and text messages and operate like pen-registers and trap-and-traces, collecting the equivalent of header information.

The government has conceded, however, that it needed a warrant in his case alone — because the stingray reached into his apartment remotely to locate the air card — and that the activities performed by Verizon and the FBI to locate Rigmaiden were all authorized by a court order signed by a magistrate.

The Electronic Frontier Foundation and the American Civil Liberties Union of Northern California, who have filed an amicus brief in support of Rigmaiden's motion, maintain that the order does not qualify as a warrant and that the government withheld crucial information from the magistrate — such as identifying that the tracking device they planned to use was a stingray and that its use involved intrusive measures — thus preventing the court from properly fulfilling its oversight function.

"It shows you just how crazy the technology is, and [supports] all the more the need to explain to the court what they are doing," says EFF Staff Attorney Hanni Fakhoury. "This is more than just [saying to Verizon] give us some records that you have sitting on your server. This is reconfiguring and changing the characteristics of the [suspect's] property, without informing the judge what's going on."

The secretive technology, generically known as a stingray or IMSI catcher, allows law enforcement agents to spoof a legitimate cell tower in order to trick nearby mobile phones and other wireless communication devices like air cards into connecting to the stingray instead of a phone carrier's legitimate tower.

When devices connect, stingrays can see and record their unique ID numbers and traffic data, as well as information that points to the device's location.

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

Use of the spy technology goes back at least 20 years. In a 2009 Utah case, an FBI agent described using a cell site emulator more than 300 times over a decade and indicated that they were used on a daily basis by U.S, Marshals, the Secret Service and other federal agencies.

The FBI used a similar device to track former hacker Kevin Mitnick in 1994, though the version used in that case was much more primitive and passive.

A 1996 *Wired* story about the Mitnick case called the device a Triggerfish and described it as "a technician's device normally used for testing cell phones." According to the story, the Triggerfish was "a rectangular box of electronics about a half a meter high controlled by a PowerBook" that was essentially "a five-channel receiver, able to monitor both sides of a conversation simultaneously." The crude technology was hauled around in a station wagon and van. A black coaxial cable was strung out of the vehicle's window to connect the Triggerfish to a direction-finding antenna on the vehicle's roof, which had four antenna prongs that reached 30 centimeters into the sky.

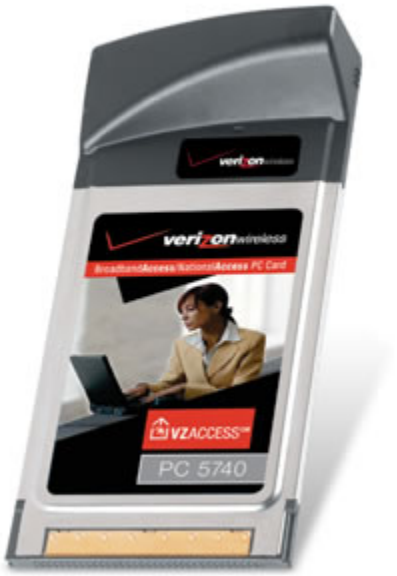
The technology has become much sleeker and less obtrusive since then, but still operates under the same principles.

In Rigmaiden's case, agents apparently used two devices made by a Florida-based company called Harris. One was the company's StingRay system, which is designed to work from a vehicle driven around a neighborhood to narrow a suspect's location to a building. Once agents tracked the signals from Rigmaiden's air card to the Domicilio Apartments complex in Santa Clara, California, they apparently used another device made by Harris called the KingFish — a handheld system that allowed them to walk through the complex and zero-in on Rigmaiden's air card in apartment 1122.

Although a number of companies make stingrays, including Verint, View Systems, Altron, NeoSoft, MMI, Ability, and Meganet, the Harris line of cell site emulators are the only ones that are compatible with CDMA2000-based devices. Others can track GSM/UMTS-based communications, but the Harris emulators can track CDMA2000, GSM and iDEN devices, as well as UMTS. The Harris StingRay and KingFish devices can also support three different communication standards simultaneously, without having to be reconfigured.

Rigmaiden was arrested in 2008 on charges that he was the mastermind behind an operation that involved stealing more than $4 million in refunds from the IRS by filing fraudulent tax returns. He and others are accused of using numerous fake IDs to open internet and phone accounts and using more than 175 different IP addresses around the United States to file the fake returns, which were often filed in bulk as if through an automated process. Rigmaiden

has been charged with 35 counts of wire fraud, 35 counts of identify theft, one count of unauthorized computer access and two counts of mail fraud.



A PC5740 Air Card.

The surveillance of Rigmaiden began in June 2008 when agents served Verizon with a grand jury subpoena asking for data on three IP addresses that were allegedly used to electronically file some of the fraudulent tax returns. Verizon reported back that the three IP addresses were linked to an air card account registered in the name of Travis Rupard — an identity that Rigmaiden allegedly stole. The air card was identified as a UTStarcom PC5740 device that was assigned a San Francisco Bay Area phone number.

A court order was then submitted to Verizon Wireless requiring the company to provide historical cell site data on the account for the previous 30 days to determine what cell towers the air card had contacted and determine its general location. Verizon responded by supplying the government with information that included the latitude and longitude coordinates for five cell sites in San Jose and Santa Clara cities, in the heart of Silicon Valley.

In July, the government served Verizon Wireless with another court order directing the company to assist the FBI in the use and monitoring of a mobile tracking device to locate an unidentified suspect. The order directed Verizon Wireless to provide the FBI with any "technical assistance needed to ascertain the physical location of the [air card]...."

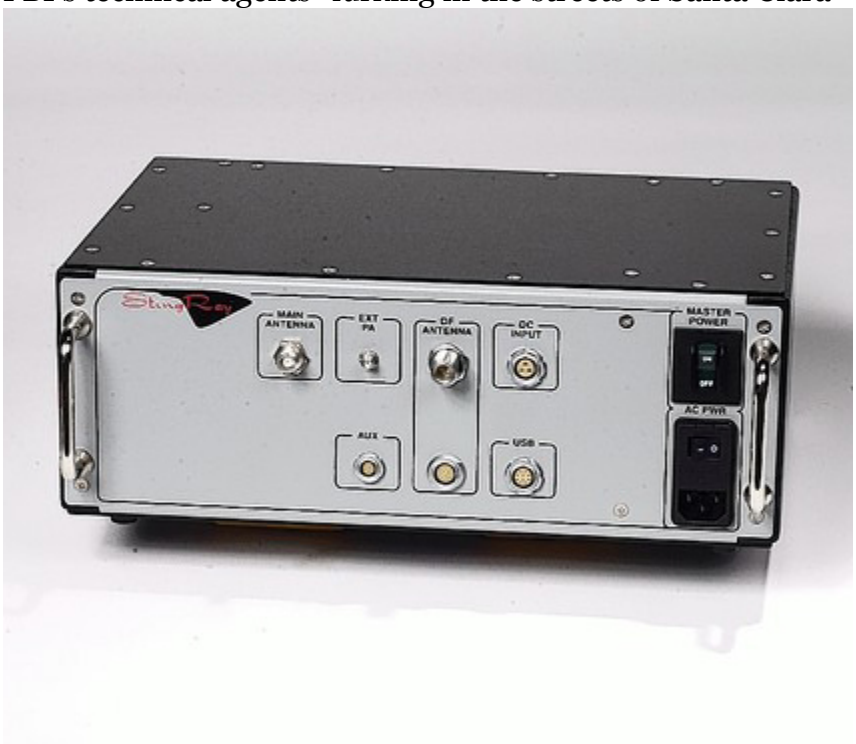
The government has fought hard to suppress information about how it uses stingrays, but in his motion to suppress, Rigmaiden lays out in great detail how the surveillance occurred and the nature of the technical assistance Verizon provided the FBI.

On the morning of July 14, 2008, FBI Agent Killigrew created a cell tower range chart/map consisting of a street map, plotted Verizon Wireless cell site sectors belonging to cell site Nos. 268, 139, and 279, and a triangulated aircard location signature estimate represented by a shaded area. On the chart/map, the total land area collectively covered by cell site Nos. 268, 139, and 279 is approximately 105,789,264 ft^2. FBI Agent Killigrew used triangulation techniques and location signature techniques to eliminate 93.9% of that 105,789,264 ft^2 area resulting in the location estimate being reduced to 6,412,224 ft^2 represented by the shaded area. The shaded area on the cell tower range chart covers the location of apartment No. 1122 at the Domicilio apartment complex.

On July 15, agents with the FBI, IRS and US Postal Service flew to San Jose to triangulate Rigmaiden's location using the stingray. They worked with technical agents from the San Francisco FBI's Wireless Intercept and Tracking Team to conduct the real-time tracking. According to Rigmaiden, the agents drove around the cell site areas gathering information about signal range and radio frequencies for each cell site sector. "The radio frequency information was needed so that the FBI technical agents could properly configure their StingRay and KingFish for use in cell site emulator mode," Rigmaiden writes. "By referencing a list of all the radio frequencies already in use, the FBI was able to choose an unused frequency for use by its emulated cellular network that would not interfere with the various FCC licensed cellular networks already operating in the noted area."

The next day, Verizon Wireless surreptitiously reprogrammed Rigmaiden's air card so that it would recognize the FBI's stingray as a legitimate cell site and connect to it "prior to attempting connections with actual Verizon Wireless cell sites." The FBI needed Verizon to reprogram the device because it otherwise was configured to reject rogue, unauthorized cell sites, Rigmaiden notes.

On July 16, the FBI placed 32 voice calls to the air card between 11am and 5pm. Each time the air card was notified that a call was coming in, it dropped its data connection and went into idle mode. At the same time, it sent real-time cell site location information to Verizon, which forwarded the information to the FBI's DCS-3000 servers, part of the elaborate digital collection system the FBI operates for wiretapping and pen-registers and trap-and-traces. From the FBI's servers, the location data was transmitted wirelessly through a VPN to the FBI's technical agents "lurking in the streets of Santa Clara" with the StingRay.



A stingray, made by Harris Corp. *Image: U.S. Patent and Trademark Office*

At this point, the StingRay took over and began to broadcast its signal to force the air card — and any other wireless devices in the area — to connect to it, so that agents could zoom-in on Rigmaiden's location.

"Because the defendant attempted to keep his aircard continuously connected to the Internet, the FBI only had a very short window of time to force the aircard to handoff its signal to the StingRay after each surreptitious voice call [and] the FBI needed to repeatedly call the aircard

in order to repeatedly boot it offline over the six hours of surreptitious phone calls," Rigmaiden writes. "Each few minute window of time that followed each denial-of-service attack (i.e., surreptitious phone call) was used by the FBI to move its StingRay, while in cell site emulator mode, to various positions until it was close enough to the aircard to force an Idle State Route Update (i.e., handoff)."

Rigmaiden maintains that once the connection was made, the StingRay wrote data to the air card to extend the connection and also began to "interrogate" the air card to get it to broadcast its location. The FBI used the Harris AmberJack antenna to deliver highly-directional precision signals to the device, and moved the StingRay around to various locations in order to triangulate the precise location of the air card inside the Domicilio Apartments complex.

According to Rigmaiden, agents also transmitted Reverse Power Control bits to his air card to get it to transmit its signals at "a higher power than it would have normally transmitted if it were accessing cellular service through an actual Verizon Wireless cell site."

Once agents had tracked the device to the Domicilio Apartments complex, they switched out the StingRay for the handheld KingFish device to locate Rigmaiden's apartment within the complex.

Around 1am on July 17, an FBI agent sent a text message to another FBI agent stating, "[w]e are down to an apt complex...." By 2:42 am, one of the FBI technical agents sent a text message to someone stating that they had "[f]ound the card" and that agents were "working on a plan for arrest."

Agents still didn't know who was in the apartment — since Rigmaiden had used an assumed identity to lease the unit — but they were able to stake out the apartment complex and engage in more traditional investigative techniques to gather more intelligence about who lived in unit 1122. On August 3, while the apartment was still under surveillance, Rigmaiden left the unit. Agents followed him a short distance until Rigmaiden caught on that he was being followed. After a brief foot chase, he was arrested.

Rigmaiden and the American Civil Liberties Union and Electronic Frontier Foundation have argued that the government did not obtain a legitimate warrant to conduct the intrusive surveillance through the stingray. They say it's indicative of how the government has used stingrays in other cases without proper disclosure to judges about how they work, and have asked the court to suppress evidence gathered through the use of the device.

U.S. District Court Judge David Campbell is expected to rule on the motion to suppress within a few weeks.

Pages: 1 2 View All

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.

Post Comment | 210 Comments | Permalink
Back to top

Share on Facebook
5.9k shares
Tweet 1,959 +1 0 1
Reddit Digg Stumble Upon Email

Comments for this thread are now closed.

210 comments

★ 9

Best Community Share Login

flassh81 · 9 months ago
Really verizon? You can do all this remotely, but when I did a *228 upgrade, my phones microphone going out had NOTHING to do with your shitty OTA upgrade? What a pack of dicks.
131 △ ▽ · Share ›

blissfulight · 9 months ago
Why is the FBI always trying to break the law?
134 △ 5 ▽ · Share ›

MustBeSaid > blissfulight · 9 months ago
Because the age of actual police work is long gone. Why do actual work and follow the law when you can just break the law, virtually nobody will challenge you and if they do, nobody in the government is ever held accountable? Saves a lot of time and energy. Too bad it doesn't save any tax money though. The bill to tax payers always seems to go up.

We let these organizations get away with it for so long, they're like a spoiled kid.
106 △ 4 ▽ · Share ›

OG_Locc > MustBeSaid · 9 months ago
Did you even read the story? There was a tremendous amount of "actual police work", and very clever work at that.
27 △ 11 ▽ · Share ›

tom thumb > OG_Locc · 9 months ago
Cleaver being, loos of personal freedoms.