EXHIBIT 5

WHAT THEY KNOW

'Stingray' Phone Tracker Fuels Constitutional Clash

By JENNIFER VALENTINO-DEVRIES

September 22, 2011

For more than a year, federal authorities pursued a man they called simply "the Hacker." Only after using a little known cellphone-tracking device—a stingray—were they able to zero in on a California home and make the arrest.

A Harris StingRay II, one of several devices dubbed 'stingrays.' *U.S. Patent and Trademark Office*

Stingrays are designed to locate a mobile phone even when it's not being used to make a call. The Federal Bureau of Investigation considers the devices to be so critical that it has a policy of deleting the data gathered in their use, mainly to keep suspects in the dark about their capabilities, an FBI official told The Wall Street Journal in response to inquiries.

A stingray's role in nabbing the alleged "Hacker"— Daniel David Rigmaiden —is shaping up as a possible test of the legal standards for using these devices in investigations. The FBI says it obtains appropriate court approval to use the device.

Stingrays are one of several new technologies used by law enforcement to track people's locations, often without a search warrant. These techniques are driving a constitutional debate about whether the Fourth Amendment, which prohibits unreasonable searches and seizures, but which was written before the digital age, is keeping pace with the times.

On Nov. 8, the Supreme Court will hear arguments over whether or not police need a warrant before secretly installing a GPS device on a suspect's car and tracking him for an extended period. In both the Senate and House, new bills would require a warrant before tracking a cellphone's location.

More

Key Documents in 'Stingray' Case

Digits: How 'Stingray' Devices Work

Digits: How Technology Is Testing the Fourth Amendment

And on Thursday in U.S. District Court of Arizona, Judge David G. Campbell is set to hear a request by Mr. Rigmaiden, who is facing fraud charges, to have information about the government's secret techniques disclosed to him so he can use it in his defense. Mr. Rigmaiden maintains his innocence and says that using stingrays to locate devices in homes without a valid warrant "disregards the United States Constitution" and is illegal.

His argument has caught the judge's attention. In a February hearing, according to a transcript, Judge Campbell asked the prosecutor, "Were there warrants obtained in connection with the use of this device?"

The prosecutor, Frederick A. Battista, said the government obtained a "court order that satisfied [the] language" in the federal law on warrants. The judge then asked how an order or warrant could have been obtained without telling the judge what technology was being used. Mr. Battista said: "It was a standard practice, your honor."

Judge Campbell responded that it "can be litigated whether those orders were appropriate."

On Thursday the government will argue it should be able to withhold details about the tool used to locate Mr. Rigmaiden, according to documents filed by the prosecution. In a statement to the Journal, Sherry Sabol, Chief of the Science & Technology Office for the FBI's Office of General Counsel, says that information about stingrays and related technology is "considered Law Enforcement Sensitive, since its public release could harm law enforcement efforts by compromising future use of the equipment."

The prosecutor, Mr. Battista, told the judge that the government worries that disclosure would make the gear "subject to being defeated or avoided or detected."

A stingray works by mimicking a cellphone tower, getting a phone to connect to it and measuring signals from the phone. It lets the stingray operator "ping," or send a signal to, a phone and locate it as long as it is powered on, according to documents reviewed by the Journal. The device has various uses, including helping police locate suspects and aiding search-and-rescue teams in finding people lost in remote areas or buried in rubble after an accident.

The government says "stingray" is a generic term. In Mr. Rigmaiden's case it remains unclear which device or devices were actually used.

The best known stingray maker is Florida-based defense contractor Harris Corp. A spokesman for Harris declined to comment.

Harris holds trademarks registered between 2002 and 2008 on several devices, including the StingRay, StingRay II, AmberJack, KingFish, TriggerFish and LoggerHead. Similar devices are available from other manufacturers. According to a Harris document, its devices are sold only to law-enforcement and government agencies.

Some of the gadgets look surprisingly old-fashioned, with a smattering of switches and lights scattered across a panel roughly the size of a shoebox, according to photos of a Harris-made StingRay reviewed by the Journal. The devices can be carried by hand or mounted in cars, allowing investigators to move around quickly.

A rare public reference to this type of technology appeared this summer in the television crime drama "The Closer." In the episode, law-enforcement officers use a gadget they called a "catfish" to track cellphones without a court order.

The U.S. armed forces also use stingrays or similar devices, according to public contract notices. Local law enforcement in Minnesota, Arizona, Miami and Durham, N.C., also either possess the devices or have considered buying them, according to interviews and published requests for funding.

The sheriff's department in Maricopa County, Ariz., uses the equipment "about on a monthly basis," says Sgt. Jesse Spurgin. "This is for location only. We can't listen in on conversations," he says.

Sgt. Spurgin says officers often obtain court orders, but not necessarily search warrants, when using the device. To obtain a search warrant from a court, officers as a rule need to show "probable cause," which is generally defined as a reasonable belief, based on factual evidence, that a crime was committed. Lesser standards apply to other court orders.

A spokeswoman with the Bureau of Criminal Apprehension in Minnesota says officers don't need to seek search warrants in that state to use a mobile tracking device because it "does not intercept communication, so no wiretap laws would apply."

FBI and Department of Justice officials have also said that investigators don't need search warrants. Associate Deputy Attorney General James A. Baker and FBI General Counsel Valerie E. Caproni both said at a panel at the Brookings Institution in May that devices like these fall into a category of tools called "pen registers," which require a lesser order than a warrant. Pen registers gather signals from phones, such as phone numbers dialed, but don't receive the content of the communications.

To get a pen-register order, investigators don't have to show probable cause. The Supreme Court has ruled that use of a pen register doesn't require a search warrant because it doesn't involve interception of conversations.

But with cellphones, data sent includes location information, making the situation more complicated because some judges have found that location information is more intrusive than details about phone numbers dialed. Some courts have required a slightly higher standard for location information, but not a warrant, while others have held that a search warrant is necessary.

The prosecution in the Rigmaiden case says in court documents that the "decisions are made on a case-by-case basis" by magistrate and district judges. Court records in other cases indicate that decisions are mixed, and cases are only now moving through appellate courts.

The FBI advises agents to work with federal prosecutors locally to meet the requirements of their particular district or judge, the FBI's Ms. Sabol says. She also says it is FBI policy to obtain a search warrant if the FBI believes the technology "may provide information on an individual while that person is in a location where he or she would have a reasonable expectation of privacy."

Experts say lawmakers and the courts haven't yet settled under what circumstances locating a person or device constitutes a search requiring a warrant. Tracking people when they are home is particularly sensitive because the Fourth Amendment specifies that people have a right to be secure against unreasonable searches in their "houses."

"The law is uncertain," says Orin Kerr, a professor at George Washington University Law School and former computer-crime attorney at the Department of Justice. Mr. Kerr, who has argued that warrants should be required for some, but not all, types of location data, says that the legality "should depend on the technology."

In the case of Mr. Rigmaiden, the government alleges that as early as 2005, he began filing fraudulent tax returns online. Overall, investigators say, Mr. Rigmaiden electronically filed more than 1,900 fraudulent tax returns as part of a $4 million plot.

Federal investigators say they pursued Mr. Rigmaiden "through a virtual labyrinth of twists and turns." Eventually, they say they linked Mr. Rigmaiden to use of a mobile-broadband card, a device that lets a computer connect to the Internet through a cellphone network.

Investigators obtained court orders to track the broadband card. Both orders remain sealed, but portions of them have been quoted by the defense and the prosecution.

These two documents are central to the clash in the Arizona courtroom. One authorizes a "pen register" and clearly isn't a search warrant. The other document is more complex. The prosecution says it is a type of search warrant and that a finding of probable cause was made.

But the defense argues that it can't be a proper search warrant, because among other things it allowed investigators to delete all the tracking data collected, rather than reporting back to the judge.

Legal experts who spoke with the Journal say it is difficult to evaluate the order, since it remains sealed. In general, for purposes of the Fourth Amendment, the finding of probable cause is most important in determining whether a search is reasonable because that requirement is specified in the Constitution itself, rather than in legal statutes, says Mr. Kerr.

But it is "odd" for a search warrant to allow deletion of evidence before a case goes to trial, says Paul Ohm, a professor at the University of Colorado Law School and a former computer-crime attorney at the Department of Justice. The law governing search warrants specifies how the warrants are to be executed and generally requires information to be returned to the judge.

Even if the court finds the government's actions acceptable under the Fourth Amendment, deleting the data is "still something we might not want the FBI doing," Mr. Ohm says.

The government says the data from the use of the stingray has been deleted and isn't available to the defendant. In a statement, the FBI told the Journal that "our policy since the 1990s has been to purge or 'expunge' all information obtained during a location operation" when using stingray-type gear.

As a general matter, Ms. Sabol says, court orders related to stingray technology "will include a directive to expunge information at the end of the location operation."

Ms. Sabol says the FBI follows this policy because its intent isn't to use the data as evidence in court, but rather to simply find the "general location of their subject" in order to start collecting other information that can be used to justify a physical search of the premises.

In the Rigmaiden example, investigators used the stingray to narrow down the location of the broadband card. Then they went to the apartment complex's office and learned that one resident had used a false ID and a fake tax return on the renter's application, according to court documents.

Based on that evidence, they obtained a search warrant for the apartment. They found the broadband card connected to a computer.

Mr. Rigmaiden, who doesn't confirm or deny ownership of the broadband card, is arguing he should be given information about the device and about other aspects of the mission that located him.

In the February hearing, Judge Campbell said he might need to weigh the government's claim of privilege against the defendant's Fourth Amendment rights, and asked the prosecution, "How can we litigate in this case whether this technology that was used in this case violates the Fourth Amendment without knowing precisely what it can do?"

Write to Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com