Written by **Warren Mass** on March 24, 2014

Police Use "StingRay" Device to Monitor Cellphones

Using a device called StingRay, police across America are able to intercept calls and texts from cell phones — often without a warrant. The StingRay simulates a cell tower, prompting cellphones within its range to identify themselves and transmit their signals to the police instead of the nearest mobile network operator's tower.

No one seems to know exactly how many local, state, or federal law enforcement agencies are using Stingray technology, how extensive the monitoring is, or even what information the devices are capable of capturing, such as the contents of phone conversations and text messages.

This information dearth is disturbing to all Americans who value their right to privacy, as protected by the Fourth Amendment's prohibition of "unreasonable searches and seizures." The amendment also prohibits the issuance of search warrants without "probable cause." Yet there are indications that StingRay is commonly being used by police not only without probable cause, but also without a warrant.

Investigations by several news organizations revealed that the most likely reason that police do not want to obtain a warrant or reveal that they are using Stingray is that the device's manufacturer, Harris Corporation of Melbourne, Florida, requires police departments who buy their equipment to sign a non-disclosure agreement.

Under normal operating procedure, when police suspect that an individual is engaged in criminal activity, they must show "probable cause" of such activity to a judge in order to obtain a search warrant. This would be the requirement for police to obtain authorization to tap a suspect's landline phone.

While the same constitutional requirements should obviously apply in order for police to be able to listen to cellphone calls, technology such as StingRay makes it easier for law enforcement (ironically) to circumvent the law. And because the Harris Corporation is so adamant about protecting every detail of Stingray from public scrutiny, it does not want to share any information about the device — not even with the judges responsible for issuing warrants!

Sacramento News 10 (ABC affiliate, KXTV) recently submitted public records requests to every major law enforcement agency in Northern California to find out which departments are using StingRay technology. The station received information from several agencies, but "none would discuss how StingRays work, or even admit they have them," reported News 10.

However, by piecing together brief statements from police officials and studying departmental purchase orders, News 10 was able to determine that StingRay was being used in Northern California.

Information culled from a 2012 grant application submitted to the Bay Area Urban Area Shield Initiative (UASI), indicated that the San Jose Police Department requested feedback from several other agencies

that already use StingRays. The application noted:

> Research of the [StingRay] product included testing by San Jose Police and technology and equipment feedback from the U.S. Marshals Service, (REDACTED), the Oakland Police Department, the Sacramento Sheriff's Department, the San Diego Sheriff's Department, the Los Angeles Police Department, and the Los Angeles Sheriff's Department. This technology is in use at the law enforcement agencies listed [above].

The language in San Jose's grant application was frank in explaining how the technology would be used:

> We will work with the Fusion Center to partner with San Francisco and Oakland to ensure we have the ability to cover all of the Bay Area in deploying cellphone tracking technology in any region of the Bay Area at a moment's notice.

When News 10 contacted law enforcement agencies in Northern California that had (according to public records and purchase orders) acquired StingRay technology, police officials typically were evasive.

For example, following up on a Criminal Investigation Division report that stated that the Oakland Police Department's Targeted Enforcement Task Force made 21 "Electronic Surveillance (StingRay) arrests" in 2007, and on a purchase order that showed that Harris Corporation had a $13,500 maintenance contract with Oakland police to maintain a StingRay S/N 303" in 2009, News 10 asked the department about their use of the StingRay.

However, reported the news outlet, Oakland police would not even admit to owning a StingRay, despite public records indicating that they did.

"Thank you again for your interest in the Oakland Police Department," police spokesperson Johnna Watson replied to News 10 in an e-mail. "We cordially decline to comment further regarding your story."

News 10 received similar runarounds or denials from several other police agencies, including the San Francisco Police Department, which said it could not find its grant application for funds to purchase a StingRay, and the Sacramento County Sheriff's Department, which said it had no records of purchasing a StingRay.

When News 10 again contacted the Sacramento County Sheriff's Department to ask them to explain the discrepancy between their statement and that of the San Jose Police Department, Undersheriff James Lewis e-mailed the station, saying:

> While I am not familiar with what San Jose has said, my understanding is that the acquisition or use of this technology comes with a strict non-disclosure requirement. Therefore it would be inappropriate for us to comment about any agency that may be using the technology.

A December 2013 investigation by *USA Today* found that about one fourth of the more than 125 law enforcement agencies it surveyed had performed "tower dumps," which allow police to request the phone numbers of all phones that connected to a specific tower within a given period of time), and that slightly fewer owned a StingRay. At least 25 of the departments own a StingRay. However, most of the departments denied the newspaper's public-records requests.

Other news organizations across the country — including Palm Springs, Calif.; Tallahassee, Fla.; and Pittsburgh, Pa. — have run into similar roadblocks when asking local law enforcement about StingRay.

"I don't see how public agencies can make up an agreement with a private company that breaks state law," David Cuillier, the director of the University of Arizona's journalism school and a national expert on public-records laws, was quoted as saying by the Associated Press. "We can't have the commercial sector running our governments for us. These public agencies need to be forthright and transparent."

An article in the *Wall Street Journal* on September 22, 2011 noted that the use of devices such as StingRay is prompting 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."

The *Journal* article pointed to the case of Daniel David Rigmaiden, a hacker charged with fraud who was apprehended by law enforcement officers who had used a StingRay. Rigmaiden asked the court to require the government to disclose information about its surveillance techniques so he could use it in his defense. He also asserted that using StingRays to locate devices in homes without a valid warrant "disregards the United States Constitution" and is illegal.

Sherry Sabol, chief of the Science & Technology Office for the FBI's Office of General Counsel, told the *Journal* 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."

An article in ThinkProgress on May 17, 2013, "Meet Stingrays, the Surveillance Tech the Government Doesn't Want to Talk About," mentioned the outcome of a key aspect of the Rigmaiden defense:

> Last week an Arizona judge ruled that a tracking warrant used to deploy the device against Daniel David Rigmaiden, who is accused of collecting millions of dollars in rebates by submitting fraudulent tax returns, was valid despite the fact that the FBI failed to disclose they would be using a stingray or explain how the devices functioned in that warrant.

A report in the *Miami New Times* on March 5 reported that the ACLU had filed several public records requests that week with 29 police forces around Florida asking for detailed information about how often StingRay has been used, whether warrants were obtained, and what cases were affected by the data gathered using the devices. The ACLU also asked a state court to unseal records about its use.

The newspaper noted that the lack of public records about StingRay use suggests that many police forces don't bother with warrants before tracking phones.

"We would expect that if police were going to get warrants and disclose the use it would come up more often in prosecutions," the *Times*' Riptide blog quoted ACLU staff attorney Nathan Freed Wessler as saying. "We suspect there is excessive secrecy around these devices because there simply isn't much information about them in court opinions and public records."

"If police departments are going to use this kind of powerful surveillance technology, they need clear rules in place so they aren't collecting private information," Wessler said.

And those rules need to conform to the Constitution, including the Fourth Amendment.

Photo: AP Images