California police departments capture cellphone data

Gabriel Black
27 March 2014

This March, a San Francisco Bay Area news station uncovered widespread use of “StingRay” devices by Californian police agencies. Their increasing adoption, with no oversight, is further evidence of the spread of police state infrastructure that has and will be used for political repression.

The devices, which indiscriminately collect cellphone communications, are used by at least seven major police departments in California. The devices are also used by federal agencies, such as the FBI, and at least 25 local US law enforcement agencies outside of California.

Local ABC News 10 filed requests with every major San Francisco Bay Area police station, asking them if they were using StingRays. Their request was largely met with silence. The station writes that “none would discuss how StingRays work, or even admit they have them.” The records they did obtain, primarily from the San Jose Police Department, showed that at least seven Californian law enforcement agencies use these devices and two more have recently received grant money to purchase them.

StingRays are essentially fake cellphone towers. Masquerading as a tower, they collect, and can even control, nearby cellphone traffic. Aspects of the device, however, are wholly unknown to the public. Using strict non-disclosure agreements, Harris Corporation, the company that manufactures StingRays, and the government have tried to keep the technology secret.

From what is known, the devices are chiefly used to pinpoint a cellphone’s location. This tracking function is so accurate that it can track a cellphone’s location within two meters. As long as the cellphone is on, police can see exactly where a target is.

Certain versions of the device allow police total access to any data transferred between the cellphone and the fake receptor. This allows police to listen to all phone calls, out-going and incoming, with virtually no threat of being detected. Police are able to access a user’s SMS-text messages. They also receive all metadata for these communications.

Harris Corporation is one of two companies that are licensed to sell this type of device in the United States. The generic term for the StingRay is an IMSI catcher. An IMSI, or International Mobile Subscriber Identity, is a unique identifier on every mobile device.

Before performing the more sophisticated functions of eavesdropping and tracking, IMSI catchers log all incoming cellphone data through IMSI numbers. Police are able to generate a comprehensive list of all cellphone users in an area. From there they can easily generate a list of names, addresses, billing records, etc. After choosing a specific target, police can force a phone to stop using encryption, allowing it to be hacked.

Interceptor, a company located in Israel, discloses several functions of its own IMSI tracker, the IBIS-II, which may or may not be present in Harris’s StingRay model. These functions include “manipulation… user can make fake calls and send fake SMS to/from target” and “selective jamming of communication.” The company also advertises that its devices are “invisible and undetectable,” having “no need for cooperation with network providers.”

The use of StingRay devices, and other IMSI catchers, is completely unregulated. There is no law that bars their purchase, as long as it is to a law enforcement agency.

The devices round up the data of all cellphone users in an area, effectively creating a dragnet. Such a warrantless collection of mass cellphone data is in direct violation of the 4th Amendment, which protects

citizens against warrantless seizure of personal effects.

In a 2011 case in Arizona reported on by the *Wall Street Journal*, the FBI used a StingRay to track down a hacker. The FBI argued in court that they were legally using the StingRay, after being challenged by the defendant. Responding to questioning from the judge, the FBI prosecutor exclaimed that the FBI had a warrant. However, the judge rebutted the prosecutor, asking how a warrant could have been obtained without specifying *anything* about the technology to be used. The FBI replied that this was standard practice.

An FBI spokesman told the *Wall Street Journal* that information about StingRays is "considered law enforcement sensitive, since its public release could harm law enforcement efforts by compromising future use of the equipment." In the 2011 case, the FBI told the judge that disclosing information about the device would make the device "subject to being defeated or avoided or detected."

The American Civil Liberties Union (ACLU) warns that "by keeping courts in the dark about new technologies, the government is essentially seeking to write its own search warrants." In other words, the executive branch is effectively bypassing the judicial branch of the government by using broad, uninformative warrants, if they use them at all.

In California, it is confirmed that StingRays are being used by every major police agency: the San Francisco Police Department, Oakland, Los Angeles, San Diego, Sacramento Sheriff's Department, and Los Angeles Sheriff's Department. A revealed grant application shows that Alameda County District Attorney's Office, in conjunction with the Fremont and Oakland Police Departments, has recently filed to receive federal funds for a StingRay device.

The ABC News 10 report cites *USA Today* for confirming that at least 25 other local law enforcement agencies across the United States are using StingRays or some other IMSI catcher.

All the California cities that have received StingRay devices seem to have been able to do so because of the initiative of the US Department of Homeland Security. The department runs two programs, the Urban Areas Security Initiative (UASI) and the State Homeland Security Program (SHSP), that have dished out millions of dollars of grants to spread the use of StingRays.

The prime reason for purchase stated in StingRay grants was terrorism. However, all the records obtained regarding arrests made via StingRay devices show that they have never been used for terrorism and are simply being integrated into regular police work.

In the early 2000s, the Miami-Dade Police Department acquired a StingRay device. In their request, the police claimed that they needed to monitor protests at the Free Trade Area of the Americas (FTAA) conference. They "anticipated criminal activities" would be organized by phone.

Local ABC News 10 spoke to Hanni Fakhoury, attorney for the Electronic Frontier Foundation, about the Miami protest. Fakhoury warned that a StingRay device would allow the police to "inventory" the protesters "through the identifying of phone numbers of all the people who might be there." Protestors and bystanders would "end up with their personal information and telephone numbers in some FBI file somewhere."

The push by the executive branch, through Homeland Security, to encourage top local police departments to adopt StingRay devices comes amidst ongoing revelations about the CIA spying program against the Senate and the NSA's gargantuan surveillance program. In all of these cases the executive branch is bypassing traditional checks on its power to implement measures that would allow for police state rule.