LAW & DISORDER —

Meet the machines that steal your phone's data

Keeping tabs on civilian phones? There's more than one way to skin that cat.

RYAN GALLAGHER - 9/25/2013, 1:00 PM

Aurich Lawson / HBO

The National Security Agency's spying tactics are being intensely scrutinized following the recent leaks of secret documents. However, the NSA isn't the only US government agency using controversial surveillance methods.

Monitoring citizens' cell phones without their knowledge is a booming business. From Arizona to California, Florida to Texas, state and federal authorities have been quietly investing millions of dollars acquiring clandestine mobile phone surveillance equipment in the past decade.

Earlier this year, a covert tool called the "Stingray" that can gather data from hundreds of phones over targeted areas attracted international attention. Rights groups alleged that its use could be unlawful. But the same company that exclusively manufacturers the Stingray—Florida-based Harris Corporation—has for years been selling government agencies an entire range of secretive mobile

phone surveillance technologies from a catalogue that it conceals from the public on national security grounds.

Details about the devices are not disclosed on the Harris website, and marketing materials come with a warning that anyone distributing them outside law enforcement agencies or telecom firms could be committing a crime punishable by up to five years in jail.

These little-known cousins of the Stingray cannot only track movements—they can also perform denial-of-service attacks on phones and intercept conversations. Since 2004, Harris has earned more than $40 million from spy technology contracts with city, state, and federal authorities in the US, according to procurement records.

In an effort to inform the debate around controversial covert government tactics, Ars has compiled a list of this equipment by scrutinizing publicly available purchasing contracts published on government websites and marketing materials obtained through equipment resellers. Disclosed, in some cases for the first time, are photographs of the Harris spy tools, their cost, names, capabilities, and the agencies known to have purchased them.

What follows is the most comprehensive picture to date of the mobile phone surveillance technology that has been deployed in the US over the past decade.

"Stingray"

The Stingray has become the most widely known and contentious spy tool used by government agencies to track mobile phones, in part due to an Arizona court case that called the legality of its use into question. It's a box-shaped portable device, sometimes described as an "IMSI catcher," that gathers information from phones by sending out a signal that tricks them into connecting to it. The Stingray can be covertly set up virtually anywhere—in the back of a vehicle, for instance—and can be used over a targeted radius to collect hundreds of unique phone identifying codes, such as the International Mobile Subscriber Number (IMSI) and the Electronic Serial Number (ESM). The authorities can then hone in on specific phones of interest to monitor the location of the user in real time or use the spy tool to log a record of all phones in a targeted area at a particular time.

Enlarge

The FBI uses the Stingray to track suspects and says that it does not use the tool to intercept the content of communications. However, this capability does exist. Procurement documents indicate that the Stingray can also be used with software called

"FishHawk," (PDF) which boosts the device's capabilities by allowing authorities to eavesdrop on conversations. Other similar Harris software includes "Porpoise," which is sold on a USB drive and is designed to be installed on a laptop and used in conjunction with transceivers—possibly including the Stingray—for surveillance of text messages.

Similar devices are sold by other government spy technology suppliers, but US authorities appear to use Harris equipment exclusively. They've awarded the company "sole source" contracts because its spy tools provide capabilities that authorities claim other companies do not offer. The Stingray has become so popular, in fact, that "Stingray" has become a generic name used informally to describe all kinds of IMSI catcher-style devices.

First used: Trademark records show that a registration for the Stingray was first filed in August 2001. Earlier versions of the technology—sometimes described as "digital analyzers" or "cell site simulators" by the FBI—were being deployed in the mid-1990s. An upgraded version of the Stingray, named the "Stingray II," was introduced to the spy tech market by Harris Corp. between 2007 and 2008. Photographs filed with the US Patent and Trademark Office depict the Stingray II as a more sophisticated device, with many additional USB inputs and a switch for a "GPS antenna," which is likely used to assist in location tracking.

Cost: $68,479 for the original Stingray; $134,952 for Stingray II.

Agencies: Federal authorities have spent more than $30 million on Stingrays and related equipment and training since 2004, according to procurement records. Purchasing agencies include the FBI, DEA, Secret Service, US Immigration and Customs Enforcement, the Internal Revenue Service, the Army, and the Navy. Cops in Arizona, Maryland, Florida, North Carolina, Texas, and California have also either purchased or considered purchasing the devices, according to public records. In one case, procurement records (PDF) show cops in Miami obtained a Stingray to monitor phones at a free trade conference held in Miami in 2003.

"Gossamer"

The Gossamer is a small portable device that can be used to secretly gather data on mobile phones operating in a target area. It sends out a covert signal that tricks phones into handing over their unique codes—such as the IMSI and TMSI—which can be used to identify users and home in on specific devices of interest. What makes it different from the Stingray? Not only is the Gossamer much smaller, but it can also be used to perform a denial-of-service attack on phone users, blocking targeted people from making or receiving calls, according to marketing materials (PDF) published by a Brazilian reseller of the Harris equipment. The Gossamer has the appearance of a clunky-looking handheld transceiver. One photograph filed with the US Patent and Trademark Office shows it displaying an option for "mobile interrogation" on its small LCD screen, which sits above a telephone-style keypad.

First used: Trademark records show that a registration for the Gossamer was first filed in October 2001.

Cost: $19,696.

Agencies: Between 2005 and 2009, the FBI, Special Operations Command, and Immigration and Customs Enforcement spent more than $1.3 million purchasing Harris' Gossamer technology and upgrading existing Gossamer units, according to procurement records. Most of the $1.3 million was spent by the FBI as part of a large contract in 2005.

Page: 1 2 Next →

READER COMMENTS 95

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars