

# **EXHIBIT 13**

# LAW & DISORDER / CIVILIZATION & DISCONTENTS

## Meet the machines that steal your phone's data

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

by Ryan Gallagher Sept 25 2013, 1:00pm EDT

INTERNET CRIME NATIONAL SECURITY 93



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 manufactures 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](#)



Software Engineer Object Oriented Programming JavaScript HTML5 CSS3 SQL Java GitHub C# .Net AJAX Visual Studio Computer Science JQuery Lead Developer Relational Databases J2EE Application Servers Software Engineer Object Oriented Programming

Software Engineer Object Oriented Programming JavaScript HTML5 CSS3 SQL Java GitHub C# .Net AJAX Visual Studio Computer Science JQuery Lead Developer Relational Databases

### TOP FEATURE STORY



#### FEATURE STORY (2 PAGES)

## How QuarkXPress became a mere afterthought in publishing

In the early '90s, Quark boasted 95% market share. In '99, InDesign arrived...

### WATCH ARS VIDEO



## Steam OS in Corporeal Form

Gaming editor Kyle Orland on Valve's big reveal.

### STAY IN THE KNOW WITH



### LATEST NEWS



**The battle for the home: Why Nest is really Google's new smart home division**



**Acceptance of global warming rises on warm days**



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 (ESN). 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.

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 hone 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



[Enlarge](#)



How the FCC screwed up its chance to make ISP blocking illegal

GAMING & ENTERTAINMENT

Valve's SteamVR is Steam—for your head-mounted display

ONE STEP FORWARD, ONE STEP BACK

As part of budget deal, Congress blocks light bulb efficiency standards

THIS LOOKS FAMILIAR

Moto G Google Play edition replaces near-stock Android with stock Android

Introducing

[www.google.c](http://www.google.c)  
Capture the moments  
the new phone from G  
now.

(Free) Cell

Desktop Mana  
Suite

"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 ▲ 93

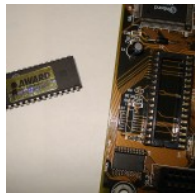
945 945 147 716

Like Share +1 Tweet



← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE ▲



Your USB cable, the spy: Inside the NSA's catalog of surveillance magic



Report: Obama set to approve "public advocate" position, more NSA reforms



The body-worn "IMSI catcher" for all your covert phone snooping needs



NZ judge: Kim Dotcom is likely still being spied upon



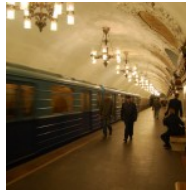
Report: NSA bulk metadata collection has "no discernible impact"



The top four tech legal cases to watch in 2014



Syrian Electronic Army hacks Skype's Twitter to warn of ongoing surveillance



Moscow Metro says new tracking system is to find stolen phones; no one believes them

SITE LINKS

- [About Us](#)
- [Advertise with us](#)
- [Contact Us](#)
- [Reprints](#)

SUBSCRIPTIONS

[Subscribe to Ars](#)

MORE READING

- [RSS Feeds](#)
- [Newsletters](#)

CONDE NAST SITES

- [Reddit](#)
- [Wired](#)
- [Vanity Fair](#)
- [Style](#)
- [Details](#)

Visit our sister sites ▼

Subscribe to a magazine ▼

[VIEW MOBILE SITE](#)

# LAW & DISORDER / CIVILIZATION & DISCONTENTS

## Meet the machines that steal your phone's data

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

by Ryan Gallagher Sept 25 2013, 1:00pm EDT

INTERNET CRIME NATIONAL SECURITY 93

### “Triggerfish”

The Triggerfish is an eavesdropping device. It allows authorities to covertly intercept mobile phone conversations in real time. This sets it apart from the original version of the Stingray, which marketing documents suggest was designed mainly for location monitoring and gathering metadata (though software can allow the Stingray to eavesdrop). The Triggerfish, which looks similar in size to the Stingray, can also be used to identify the location from which a phone call is being made. It can gather large amounts of data on users over a targeted area, allowing authorities to view identifying codes of up to 60,000 different phones at one time, according to marketing materials.



[Enlarge](#)

**First used:** Trademark records [show](#) that a registration for the Triggerfish was filed in July 2001, though its “first use anywhere” is listed as November 1997. It is not clear whether the Triggerfish is still for sale or whether its name has recently changed, as the trademark on the device was canceled in 2008, and it does not appear on Harris' current federal price lists.

**Cost:** Between \$90,000 and \$102,000.

**Agencies:** The Bureau of Alcohol, Tobacco, Firearms, and Explosives; the DEA; and county cops in Miami-Dade invested in Triggerfish technology prior to 2004, according to procurement records. However, the [procurement records](#) (PDF) also show that the Miami-Dade authorities complained that the device “provided access” only to Cingular and AT&T wireless network carriers. (This was before the two companies merged.) To remedy that, the force complemented the Triggerfish tool with additional Harris technology, including the Stingray and Amberjack, which enabled monitoring of Metro PCS, Sprint, and Verizon. This gave the cops “the ability to track approximately ninety percent of the wireless industry,” the procurement documents state.

### “Kingfish”

The Kingfish is a surveillance transceiver that allows authorities to track and mine information from mobile phones over a targeted area. The device does not appear to enable interception of communications; instead, it can covertly gather unique identity codes and show connections between phones and numbers being dialed. It is smaller than the Stingray, black and gray in color, and can be controlled wirelessly by a conventional notebook PC using Bluetooth. You can even conceal it in a discreet-looking briefcase, according to marketing brochures.



[Enlarge](#)

**First used:** Trademark records [show](#) that a registration for the Kingfish was filed in August 2001. Its “first use anywhere” is listed in records as December 2003.

**Cost:** \$25,349.

**Agencies:** Government agencies have spent about \$13 million on Kingfish technology since 2006, sometimes as part of what is described in procurement documents as a “vehicular package” deal that includes a Stingray. The US Marshals Service; Secret Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Army; Air Force; state cops in Florida; county cops in Maricopa, Arizona; and Special Operations Command have all purchased a Kingfish in recent years.

### TOP FEATURE STORY ▾

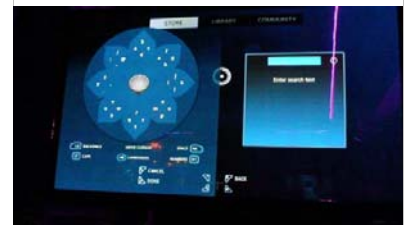


**FEATURE STORY (2 PAGES)**

### How QuarkXPress became a mere afterthought in publishing

In the early '90s, Quark boasted 95% market share. In '99, InDesign arrived...

### WATCH ARS VIDEO ▾



### Steam OS in Corporeal Form

Gaming editor Kyle Orland on Valve's big reveal.

### STAY IN THE KNOW WITH ▾

### LATEST NEWS ▾



**The battle for the home: Why Nest is really Google's new smart home division**



**Acceptance of global warming rises on warm days**



**How the FCC screwed up its chance to make ISP blocking illegal**

### GAMING & ENTERTAINMENT

**Valve's SteamVR is Steam—for your head-mounted display**

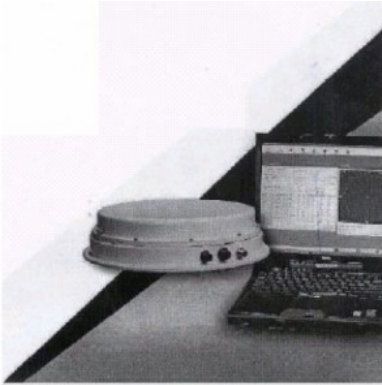
### ONE STEP FORWARD, ONE STEP BACK

**As part of budget deal, Congress blocks light bulb efficiency standards**

### THIS LOOKS FAMILIAR

### “Amberjack”

The Amberjack is an antenna that is used to help track and locate mobile phones. It is designed to be used in conjunction with the Stingray, Gossamer, and Kingfish as a “[direction-finding system](#)” (PDF) that monitors the signal strength of the targeted phone in order to home in on the suspect’s location in real time. The device comes inbuilt with magnets so it can be attached to the roof of a police vehicle, and it has been designed to have a “low profile” for covert purposes. A photograph of the Amberjack filed with a trademark application reveals that the device, which is metallic and circular in shape, comes with a “tie-down kit” to prevent it from falling off the roof of a vehicle that is being driven at “highway speeds.”



**First used:** Trademark records [show](#) that a registration for the Amberjack was filed in August 2001 at the same time as the Stingray. Its “first use anywhere” is listed in records as October 2002.

**Cost:** \$35,015

**Agencies:** The DEA; FBI; Special Operations Command; Secret Service; the Navy; the US Marshals Service; and cops in North Carolina, Florida, and Texas have all purchased Amberjack technology, according to procurement records.



[Enlarge](#)

### “Harpoon”

The Harpoon is an “[amplifier](#)” (PDF) that can boost the signal of a Stingray or Kingfish device, allowing it to project its surveillance signal farther or from a greater distance depending on the location of the targets. A photograph filed with the US Patent and Trademark Office shows that the device has two handles for carrying and a silver, metallic front with a series of inputs that allow it to be connected to other mobile phone spy devices.



**First used:** Trademark records [show](#) that a filing for the Harpoon was filed in June 2008.

**Cost:** \$16,000 to \$19,000.

[Enlarge](#)

**Agencies:** The DEA; state cops in Florida; city cops in Tempe, Arizona; the Army; and the Navy are among those to have purchased Harpoons since 2009.

### “Hailstorm”

The Hailstorm is the latest in the line of mobile phone tracking tools that Harris Corp. is offering authorities. However, few details about it have trickled into the public domain. It can be purchased as a standalone unit or as an upgrade to the Stingray or Kingfish, which suggests that it has the same functionality as these devices but has been tweaked with new or more advanced capabilities. [Procurement documents](#) (PDF) show that Harris Corp. has, in at least one case, recommended that authorities use the Hailstorm in conjunction with software made by Nebraska-based surveillance company [Pen-Link](#). The Pen-Link software appears to enable authorities deploying the Hailstorm to directly communicate with cell phone carriers over an Internet connection, possibly to help coordinate the surveillance of targeted individuals.

**First used:** Unknown.

**Cost:** \$169,602 as a standalone unit. The price is reduced when purchased as an upgrade.

**Agencies:** Public records show that earlier this year, the Baltimore Police Department, county cops in Oakland County, Michigan, and city cops in Phoenix, Arizona, each separately entered the procurement process to obtain the Hailstorm equipment. The Baltimore and Phoenix forces each set aside about \$100,000 for the device, and they purchased it as an upgrade to Stingray II mobile phone spy technology. The Phoenix cops spent an additional \$10,000 on Hailstorm training sessions

### Moto G Google Play edition replaces near-stock Android with stock Android

Software Engineer Object Oriented Programming  
JavaScript HTML5 CSS3 SQL Java GitHub C# .Net  
AJAX Visual Studio Computer Science JQuery Lead  
Developer Relational Databases J2EE Application  
Servers Software Engineering Object Oriented  
Programming  
**ars jobs**  
Science JQuery Lead Developer Relational Databases  
J2EE Application Servers Software Engineer Object  
Oriented Programming JavaScript HTML5 CSS3 SQL  
Java GitHub C# .Net AJAX Visual Studio Computer  
Science JQuery Lead Developer Relational Databases

### 2014 Top Security Systems

[www.homesecuritycomparison.net](http://www.homesecuritycomparison.net)

View Our Side-By-Side Comparison Of 2014's Best Home Security Systems!

### Desktop Management Suite

### Catch Your Cheater Spouse

conducted by Harris Corp. in Melbourne, Florida, and Oakland County authorities said they obtained a grant from the Department of Homeland Security to help finance the procurement of the Hailstorm tool. The Oakland authorities noted that the device was needed for "pinpoint tracking of criminal activity." It is highly likely that other authorities—particularly federal agencies—will invest in the Hailstorm too, with procurement records eventually surfacing later this year or into 2014.

### No one's talking

Ars contacted the agencies most frequently referenced above, including the FBI; the DEA; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Secret Service; and Immigration and Customs Enforcement. Our requests for comment were either not returned or rebuffed on the grounds that the topic is "law enforcement sensitive." Harris Corp. also turned down an interview request and declined to answer any questions for this story.

The FBI has [previously](#) stated in response to questions about the Stingray device that it "strives to protect our country and its people using every available tool" and that location data in particular is a "vital component" of investigations. But when it comes to discussing specific surveillance equipment, it is common for the authorities to remain tight-lipped because they don't want to reveal tactics to criminals.

The code of silence shrouding the above tools, however, is highly contentious. Their use by law enforcement agencies is in a legal gray zone, particularly because interference with communications signals is supposed to be prohibited under the federal [Communications Act](#). In May, an Arizona court [ruled](#) that the FBI's use of a Stingray was lawful in a case involving conspiracy, wire fraud, and identity theft. But according to the American Civil Liberties Union (ACLU), when seeking authorization for the use of the Stingray tool, the feds have sometimes unlawfully [withheld information](#) from judges about the full scope of its capabilities. This means that judges across the country are potentially authorizing the use of the technology without even knowing what it actually does.

That's not all. There is another significant issue raised by the Harris spy devices: security. According to Christopher Soghoian, chief technologist at the ACLU, similar covert surveillance technology is being manufactured by a host of companies in other countries like China and Russia. He believes the US government's "state secrecy" on the subject is putting Americans at risk.

"Our government is sitting on a security flaw that impacts every phone in the country," Soghoian says. "If we don't talk about Stingray-style tools and the flaws that they exploit, we can't defend ourselves against foreign governments and criminals using this equipment, too."

PAGE: 1 2

READER COMMENTS ▲ 93

← OLDER STORY

NEWER STORY →

YOU MAY ALSO LIKE ▲