Stingray phone tracker

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Stingray_phone_tracker#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Stingray_phone_tracker#searchInput)

*"StingRay" redirects here. For other uses, see*[*Stingray (disambiguation)*](https://en.wikipedia.org/wiki/Stingray_(disambiguation))*.*

|  |  |  |  |
| --- | --- | --- | --- |
|  | hide**This article has multiple issues.** Please help [**improve it**](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit) or discuss these issues on the [**talk page**](https://en.wikipedia.org/wiki/Talk:Stingray_phone_tracker). *(*[*Learn how and when to remove these template messages*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)*   |  | | --- | | This article **needs additional citations for**[**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). *(April 2017)* |  |  | | --- | | The examples and perspective in this article **deal primarily with the United States and do not represent a**[**worldwide view**](https://en.wikipedia.org/wiki/Wikipedia:WikiProject_Countering_systemic_bias)**of the subject**. *(October 2016)* | |

[](https://en.wikipedia.org/wiki/File:Stingray_Harris_handle_side.jpg)

A Stingray device in 2013, in Harris's trademark submission.[[1]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-Notice,_Acceptance,_Renewal-1)

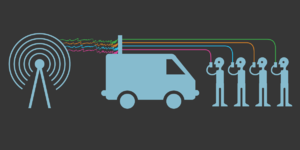
The **StingRay** is an [IMSI-catcher](https://en.wikipedia.org/wiki/IMSI-catcher), a cellular phone surveillance device, manufactured by [Harris Corporation](https://en.wikipedia.org/wiki/Harris_Corporation).[[2]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-wired-sting-2) Initially developed for the military and intelligence community, the StingRay and similar Harris devices are in widespread use by local and state law enforcement agencies across Canada,[[3]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-3) the United States,[[4]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-5) and in the United Kingdom.[[6]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-6)[[7]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-7) **Stingray** has also become a generic name to describe these kinds of devices.[[8]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-8)



**Contents**

* [1Technology](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Technology)
  + [1.1Active mode operations](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Active_mode_operations)
  + [1.2Passive mode operations](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Passive_mode_operations)
  + [1.3Active (cell site simulator) capabilities](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Active_(cell_site_simulator)_capabilities)
    - [1.3.1Extracting data from internal storage](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Extracting_data_from_internal_storage)
    - [1.3.2Forcing an increase in signal transmission power](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Forcing_an_increase_in_signal_transmission_power)
    - [1.3.3Tracking and locating](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Tracking_and_locating)
    - [1.3.4Denial of service](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Denial_of_service)
    - [1.3.5Interception of communications content](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Interception_of_communications_content)
  + [1.4Passive capabilities](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Passive_capabilities)
    - [1.4.1Base station (cell site) surveys](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Base_station_(cell_site)_surveys)
* [2Usage by law enforcement](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Usage_by_law_enforcement)
  + [2.1In the United States](https://en.wikipedia.org/wiki/Stingray_phone_tracker#In_the_United_States)
  + [2.2Outside the United States](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Outside_the_United_States)
* [3Secrecy](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Secrecy)
* [4Criticism](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Criticism)
* [5Countermeasures](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Countermeasures)
* [6See also](https://en.wikipedia.org/wiki/Stingray_phone_tracker#See_also)
* [7References](https://en.wikipedia.org/wiki/Stingray_phone_tracker#References)
* [8Further reading](https://en.wikipedia.org/wiki/Stingray_phone_tracker#Further_reading)

Technology[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=1)]

[](https://en.wikipedia.org/wiki/File:Stingray.png)

When operating in active mode, the Stingray device mimics a wireless carrier cell tower in order to force all nearby mobile phones and other cellular data devices to connect to it.

The StingRay is an IMSI-catcher with both passive (digital analyzer) and active (cell-site simulator) capabilities. When operating in active mode, the device mimics a wireless carrier cell tower in order to force all nearby mobile phones and other cellular data devices to connect to it.[[9]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-wsj-stingray-9)[[10]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-datasheet-1-10)[[11]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-datasheet-2-11)

The StingRay family of devices can be mounted in vehicles,[[10]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-datasheet-1-10) on aeroplanes, helicopters and [unmanned aerial vehicles](https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle).[[12]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-catalog-airborne-12) Hand-carried versions are referred to under the trade name **KingFish**.[[13]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-kingfish-sole-source-justification-fl-1-13)

**Active mode operations**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=2)]

1. Extracting stored data such as [International Mobile Subscriber Identity](https://en.wikipedia.org/wiki/International_Mobile_Subscriber_Identity) ("IMSI") numbers and [Electronic Serial Number](https://en.wikipedia.org/wiki/Electronic_Serial_Number) ("ESN"),[[14]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-morrison-stingray-esn-estraction-14)
2. Writing cellular protocol metadata to internal storage
3. Forcing an increase in signal transmission power[[15]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-kingfish-force-power-increase-15)
4. Forcing an abundance of radio signals to be transmitted
5. Forcing a downgrade to an older and less secure communications protocol if the older protocol is allowed by the target device, by making the Stingray pretend to be unable to communicate on an up-to-date protocol
6. Interception of communications data or metadata
7. Using received signal strength indicators to direction find the cellular device[[9]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-wsj-stingray-9)
8. Conducting a denial of service attack
9. [Radio jamming](https://en.wikipedia.org/wiki/Radio_jamming) for either general denial of service purposes[[16]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-kingfish-denial-of-service-16)[[*failed verification*](https://en.wikipedia.org/wiki/Wikipedia:Verifiability)*–*[*see discussion*](https://en.wikipedia.org/wiki/Talk:Stingray_phone_tracker#Radio_Jamming_Functionality)] or to aid in active mode [protocol rollback attacks](https://en.wikipedia.org/w/index.php?title=Protocol_rollback_attacks&action=edit&redlink=1)

**Passive mode operations**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=3)]

1. conducting base station surveys, which is the process of using over-the-air signals to identify legitimate cell sites and precisely map their coverage areas

**Active (cell site simulator) capabilities**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=4)]

In active mode, the StingRay will force each compatible cellular device in a given area to disconnect from its service provider cell site (e.g., operated by Verizon, AT&T, etc.) and establish a new connection with the StingRay.[[17]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-kingfish-cell-site-emulation-17) In most cases, this is accomplished by having the StingRay broadcast a pilot signal that is either stronger than, or made to appear stronger than, the pilot signals being broadcast by legitimate cell sites operating in the area.[[18]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-hardman-spook-stingray-18) A common function of all cellular communications protocols is to have the cellular device connect to the cell site offering the strongest signal. StingRays exploit this function as a means to force temporary connections with cellular devices within a limited area.

**Extracting data from internal storage**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=5)]

During the process of forcing connections from all compatible cellular devices in a given area, the StingRay operator needs to determine which device is the desired surveillance target. This is accomplished by downloading the IMSI, ESN, or other identifying data from each of the devices connected to the StingRay.[[14]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-morrison-stingray-esn-estraction-14) In this context, the IMSI or equivalent identifier is not obtained from the cellular service provider or from any other third-party. The StingRay downloads this data directly from the device using radio waves.[[19]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-19)

In some cases, the IMSI or equivalent identifier of a target device is known to the StingRay operator beforehand. When this is the case, the operator will download the IMSI or equivalent identifier from each device as it connects to the StingRay.[[20]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-kingfish-used-on-known-device-20) When the downloaded IMSI matches the known IMSI of the desired target, the dragnet will end and the operator will proceed to conduct specific surveillance operations on just the target device.[[21]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-21)

In other cases, the IMSI or equivalent identifier of a target is not known to the StingRay operator and the goal of the surveillance operation is to identify one or more cellular devices being used in a known area.[[22]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-kingfish-used-on-unknown-device-22) For example, if visual surveillance is being conducted on a group of protestors,[[23]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-stingray-protestors-23) a StingRay can be used to download the IMSI or equivalent identifier from each phone within the protest area. After identifying the phones, locating and tracking operations can be conducted, and service providers can be forced to turn over account information identifying the phone users.

**Forcing an increase in signal transmission power**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=6)]

|  |  |
| --- | --- |
|  | This section **does not**[**cite**](https://en.wikipedia.org/wiki/Wikipedia:Citing_sources)**any**[**sources**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this section](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Referencing_for_beginners). Unsourced material may be challenged and [removed](https://en.wikipedia.org/wiki/Wikipedia:Verifiability#Burden_of_evidence). *(April 2017) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

Cellular telephones are radio transmitters and receivers much like a [walkie-talkie](https://en.wikipedia.org/wiki/Walkie-talkie). However, the cell phone communicates only with a [repeater](https://en.wikipedia.org/wiki/Repeater) inside a nearby cell tower installation. At that installation, the devices take in all cell calls in its geographic area and repeat them out to other cell installations which repeat the signals onward to their destination telephone (either by radio or landline wires). Radio is used also to transmit a caller's voice/data back to the receiver's cell telephone. The [two-way duplex](https://en.wikipedia.org/wiki/Full_duplex) phone conversation then exists via these interconnections.

To make all that work correctly, the system allows automatic increases and decreases in transmitter power (for the individual cell phone and for the tower repeater, too) so that only the minimum transmit power is used to complete and hold the call active, "on", and allows the users to hear and be heard continuously during the conversation. The goal is to hold the call active but use the least amount of transmitting power, mainly to conserve batteries and be efficient. The tower system will sense when a cell phone is not coming in clearly and will order the cell phone to boost transmit power. The user has no control over this boosting; it may occur for a split second or for the whole conversation. If the user is in a remote location, the power boost may be continuous. In addition to carrying voice or data, the cell phone also transmits data about itself automatically, and that is boosted or not as the system detects need.

Encoding of all transmissions ensures that no [cross talk](https://en.wikipedia.org/wiki/Crosstalk_(electronics)) or interference occurs between two nearby cell users. The boosting of power, however, is limited by the design of the devices to a maximum setting. The standard systems are not "high power" and thus can be overpowered by secret systems using much more boosted power that can then take over a user's cell phone. If overpowered that way, a cell phone will not indicate the change due to the secret radio being programmed to hide from normal detection. The ordinary user can not know if their cell phone is captured via overpowering boosts or not. (There are other ways of secret capture that need not overpower, too.)

Just as a person shouting drowns out someone whispering, the boost in [RF watts](https://en.wikipedia.org/wiki/Radio_frequency#Measurement) of power into the cell telephone system can overtake and control that system—in total or only a few, or even only one, conversation. This strategy requires only more RF power, and thus it is more simple than other types of secret control. Power boosting equipment can be installed anywhere there can be an antenna, including in a vehicle, perhaps even in a vehicle on the move. Once a secretly boosted system takes control, any manipulation is possible from simple recording of the voice or data to total blocking of all cell phones in the geographic area.

**Tracking and locating**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=7)]

A StingRay can be used to identify and track a phone or other compatible cellular data device even while the device is not engaged in a call or accessing data services.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

A Stingray closely resembles a portable cellphone tower. Typically, law enforcement officials place the Stingray in their vehicle with a compatible computer software. The Stingray acts as a cellular tower to send out signals to get the specific device to connect to it. Cell phones are programmed to connect with the cellular tower offering the best signal. When the phone and Stingray connect, the computer system determines the strength of the signal and thus the distance to the device. Then, the vehicle moves to another location and sends out signals until it connects with the phone. When the signal strength is determined from enough locations, the computer system centralizes the phone and is able to find it.

Cell phones are programmed to constantly search for the strongest signal emitted from cell phone towers in the area. Over the course of the day, most cell phones connect and reconnect to multiple towers in an attempt to connect to the strongest, fastest, or closest signal. Because of the way they are designed, the signals that the Stingray emits are far stronger than those coming from surrounding towers. For this reason, all cell phones in the vicinity connect to the Stingray regardless of the cell phone owner's knowledge. From there, the stingray is capable of locating the device, interfering with the device, and collecting personal data from the device.[[24]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-24)[[25]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-25)

**Denial of service**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=8)]

The FBI has claimed that when used to identify, locate, or track a cellular device, the StingRay does not collect communications content or forward it to the service provider.[[26]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-morrison-stingray-denial-of-service-26) Instead, the device causes a disruption in service.[[27]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-27) Under this scenario, any attempt by the cellular device user to place a call or access data services will fail while the StingRay is conducting its surveillance. On August 21, 2018, Senator [Ron Wyden](https://en.wikipedia.org/wiki/Ron_Wyden) noted that Harris Corporation confirmed that Stingrays disrupt the targeted phone's communications. Additionally, he noted that "while the company claims its cell-site simulators include a feature that detects and permits the delivery of emergency calls to [9-1-1](https://en.wikipedia.org/wiki/9-1-1), its officials admitted to my office that this feature has not been independently tested as part of the Federal Communication Commission’s certification process, nor were they able to confirm this feature is capable of detecting and passing-through 9-1-1 emergency communications made by people who are deaf, hard of hearing, or speech disabled using Real-Time Text technology."[[28]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-28)

**Interception of communications content**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=9)]

By way of software upgrades,[[29]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-dea-fishhawk-29) the StingRay and similar Harris products can be used to intercept [GSM](https://en.wikipedia.org/wiki/GSM) communications content transmitted over-the-air between a target cellular device and a legitimate service provider cell site. The StingRay does this by way of the following [man-in-the-middle attack](https://en.wikipedia.org/wiki/Man-in-the-middle_attack): (1) simulate a cell site and force a connection from the target device, (2) download the target device's IMSI and other identifying information, (3) conduct "GSM Active Key Extraction"[[29]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-dea-fishhawk-29) to obtain the target device's stored encryption key, (4) use the downloaded identifying information to simulate the target device over-the-air, (5) while simulating the target device, establish a connection with a legitimate cell site authorized to provide service to the target device, (6) use the encryption key to authenticate the StingRay to the service provider as being the target device, and (7) forward signals between the target device and the legitimate cell site while decrypting and recording communications content.

The "GSM Active Key Extraction"[[29]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-dea-fishhawk-29) performed by the StingRay in step three merits additional explanation. A GSM phone encrypts all communications content using an encryption key stored on its SIM card with a copy stored at the service provider.[[30]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-GSM-intercept-simple-explain-30) While simulating the target device during the above explained man-in-the-middle attack, the service provider cell site will ask the StingRay (which it believes to be the target device) to initiate encryption using the key stored on the target device.[[31]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-GSM-intercept-complex-explain-31) Therefore, the StingRay needs a method to obtain the target device's stored encryption key else the man-in-the-middle attack will fail.

GSM primarily encrypts communications content using the [A5/1](https://en.wikipedia.org/wiki/A5/1) call encryption cypher. In 2008 it was reported that a GSM phone's encryption key can be obtained using $1,000 worth of computer hardware and 30 minutes of cryptanalysis performed on signals encrypted using A5/1.[[32]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-GSM-A51-cryptanalysis-32) However, GSM also supports an export weakened variant of A5/1 called [A5/2](https://en.wikipedia.org/wiki/A5/2). This weaker encryption cypher can be cracked in real-time.[[30]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-GSM-intercept-simple-explain-30) While A5/1 and A5/2 use different cypher strengths, they each use the same underlying encryption key stored on the SIM card.[[31]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-GSM-intercept-complex-explain-31) Therefore, the StingRay performs "GSM Active Key Extraction"[[29]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-dea-fishhawk-29) during step three of the man-in-the-middle attack as follows: (1) instruct target device to use the weaker A5/2 encryption cypher, (2) collect A5/2 encrypted signals from target device, and (3) perform cryptanalysis of the A5/2 signals to quickly recover the underlying stored encryption key.[[33]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-ReferenceA-33) Once the encryption key is obtained, the StingRay uses it to comply with the encryption request made to it by the service provider during the man-in-the-middle attack.[[33]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-ReferenceA-33)

A rogue base station can force unencrypted links, if supported by the handset software. The rogue base station can send a 'Cipher Mode Settings' element (see [GSM 04.08 Chapter 10.5.2.9](http://www.etsi.org/deliver/etsi_gts/04/0408/05.03.00_60/gsmts_0408v050300p.pdf)) to the phone, with this element clearing the one bit that marks if encryption should be used. In such cases the phone display could indicate the use of an unsafe link - but the user interface software in most phones does not interrogate the handset's radio subsystem for use of this insecure mode nor display any warning indication.

**Passive capabilities**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=10)]

In passive mode, the StingRay operates either as a digital analyzer, which receives and analyzes signals being transmitted by cellular devices and/or wireless carrier cell sites or as a radio jamming device, which transmits signals that block communications between cellular devices and wireless carrier cell sites. By "passive mode," it is meant that the StingRay does not mimic a wireless carrier cell site or communicate directly with cellular devices.

**Base station (cell site) surveys**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=11)]

A StingRay and a test phone can be used to conduct base station surveys, which is the process of collecting information on cell sites, including identification numbers, signal strength, and signal coverage areas. When conducting base station surveys, the StingRay mimics a cell phone while passively collecting signals being transmitted by cell-sites in the area of the StingRay.

Base station survey data can be used to further narrow the past locations of a cellular device if used in conjunction with historical cell site location information ("HCSLI") obtained from a wireless carrier. HCSLI includes a list of all cell sites and sectors accessed by a cellular device, and the date and time each access was made. Law enforcement will often obtain HCSLI from wireless carriers in order to determine where a particular cell phone was located in the past. Once this information is obtained, law enforcement will use a map of cell site locations to determine the past geographical locations of the cellular device.

However, the signal coverage area of a given cell site may change according to the time of day, weather, and physical obstructions in relation to where a cellular device attempts to access service. The maps of cell site coverage areas used by law enforcement may also lack precision as a general matter. For these reasons, it is beneficial to use a StingRay and a test phone to map out the precise coverage areas of all cell sites appearing in the HCSLI records. This is typically done at the same time of day and under the same weather conditions that were in effect when the HCSLI was logged. Using a StingRay to conduct base station surveys in this manner allows for mapping out cell site coverage areas that more accurately match the coverage areas that were in effect when the cellular device was used.

Usage by law enforcement[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=12)]

**In the United States**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=13)]

*Main article:*[*Stingray use in United States law enforcement*](https://en.wikipedia.org/wiki/Stingray_use_in_United_States_law_enforcement)

The use of the devices has been frequently funded by grants from the [Department of Homeland Security](https://en.wikipedia.org/wiki/Department_of_Homeland_Security).[[34]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-34) The [Los Angeles Police Department](https://en.wikipedia.org/wiki/Los_Angeles_Police_Department) used a Department of Homeland Security grant in 2006 to buy a StingRay for "regional terrorism investigations".[[35]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-35) However, according to the [Electronic Frontier Foundation](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation), the "LAPD has been using it for just about any investigation imaginable."[[36]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-36)

In addition to federal law enforcement, military and intelligence agencies, StingRays have in recent years been purchased by local and state law enforcement agencies.

In 2006, Harris Corporation employees directly conducted wireless surveillance using StingRay units on behalf the [Palm Bay](https://en.wikipedia.org/wiki/Palm_Bay,_Florida) Police Department — where Harris has a campus[[37]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-37) — in response to a bomb threat against a middle school. The search was conducted without a warrant or Judicial oversight.[[38]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-38)[[39]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-39)[[40]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-40)[[41]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-41)

The American Civil Liberties Union, commonly referred to as the ACLU, confirmed that local police have cell site simulators in Washington, Nevada, Arizona, Alaska, Missouri, New Mexico, Georgia, and Massachusetts. State police have cell site simulators in Oklahoma, Louisiana, and Pennsylvania, and Delaware. Local and state police have cell site simulators in California, Texas, Minnesota, Wisconsin, Michigan, Illinois, Indiana, Tennessee, North Carolina, Virginia, Florida, Maryland, and New York [60]. The police use of cell site simulators is unknown in the remaining states. However, many agencies do not disclose their use of StingRay technology, so these statistics are still potentially an under-representation of the actual number of agencies. According to the most recent information published by the American Civil Liberties Union, 72 law enforcement agencies in 24 states own StingRay technology in 2017. Since 2014, these numbers have increased from 42 agencies in 17 states [60]. The following are federal agencies in the United States that have validated their use of cell site simulators: Federal Bureau of Investigation, Drug Enforcement Administration, US Secret Service, Immigration and Customs Enforcement, US Marshals Service, Bureau of Alcohol, Tobacco, Firearms, and Explosives, US Army, US Navy, US Marine Corps, US National Guard, US Special Command, and National Security Agency [60].[[42]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-42) In the 2010-14 fiscal years, the [Department of Justice](https://en.wikipedia.org/wiki/Department_of_Justice) has confirmed spending “more than $71 million on cell-cite simulation technology,” while the [Department of Homeland Security](https://en.wikipedia.org/wiki/Department_of_Homeland_Security) confirmed spending “more than $24 million on cell-cite simulation technology.”[[43]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-43)

Several court decisions have been issued on the legality of using a Stingray without a warrant, with some courts ruling a warrant is required[[44]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-44)[[45]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-45)[[46]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-46) and others not requiring a warrant.[[47]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-47)

**Outside the United States**[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=14)]

Police in [Vancouver](https://en.wikipedia.org/wiki/Vancouver), BC, Canada admitted after much speculation across the country that they had made use of a Stingray device[[48]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-48) provided by the [RCMP](https://en.wikipedia.org/wiki/RCMP). They also stated that they intended to make use of such devices in the future. Two days later, a statement by [Edmonton](https://en.wikipedia.org/wiki/Edmonton)'s police force had been taken as confirming their use of the devices, but they said later that they did not mean to create what they called a miscommunication.[[49]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-49)

[Privacy International](https://en.wikipedia.org/wiki/Privacy_International) and [*The Sunday Times*](https://en.wikipedia.org/wiki/The_Sunday_Times) reported on the usage of StingRays and IMSI-catchers in [Ireland](https://en.wikipedia.org/wiki/Ireland), against the Irish [Garda Síochána Ombudsman Commission](https://en.wikipedia.org/wiki/Garda_S%C3%ADoch%C3%A1na_Ombudsman_Commission) (GSOC), which is an oversight agency of the Irish police force [Garda Síochána](https://en.wikipedia.org/wiki/Garda_S%C3%ADoch%C3%A1na).[[50]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-50)[[51]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-51) On June 10, 2015 the [BBC](https://en.wikipedia.org/wiki/BBC) reported on an investigation by [Sky News](https://en.wikipedia.org/wiki/Sky_News)[[52]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-BBC_Sky-52)[[53]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-london_met-53) about possible false mobile phone towers being used by the [London Metropolitan Police](https://en.wikipedia.org/wiki/London_Metropolitan_Police). Commissioner Bernard Hogan-Howe refused comment.

Between February 2015 and April 2016, over 12 companies in the United Kingdom were authorized to export IMSI-catcher devices to states including [Saudi Arabia](https://en.wikipedia.org/wiki/Saudi_Arabia), [UAE](https://en.wikipedia.org/wiki/United_Arab_Emirates), and [Turkey](https://en.wikipedia.org/wiki/Turkey). Critics have expressed concern about the export of surveillance technology to countries with poor [human rights records](https://en.wikipedia.org/wiki/Human_rights) and histories of abusing [surveillance technology](https://en.wikipedia.org/wiki/Surveillance_technology).[[54]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-54)

Secrecy[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=15)]

The increasing use of the devices has largely been kept secret from the court system and the public.[[55]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-:0-55) In 2014, police in [Florida](https://en.wikipedia.org/wiki/Florida) revealed they had used such devices at least 200 additional times since 2010 without disclosing it to the courts or obtaining a warrant.[[2]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-wired-sting-2) One of the reasons the Tallahassee police provided for not pursuing court approval is that such efforts would allegedly violate the non-disclosure agreements (NDAs) that police sign with the manufacturer.[[56]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-56) The [American Civil Liberties Union](https://en.wikipedia.org/wiki/American_Civil_Liberties_Union) has filed multiple requests for the public records of Florida law enforcement agencies about their use of the cell phone tracking devices.[[57]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-57)

Local law enforcement and the federal government have resisted judicial requests for information about the use of stingrays, refusing to turn over information or heavily censoring it.[[58]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-yahoo1-58) In June 2014, the American Civil Liberties Union published information from court regarding the extensive use of these devices by local Florida police.[[59]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-59) After this publication, [United States Marshals Service](https://en.wikipedia.org/wiki/United_States_Marshals_Service) then seized the local police's surveillance records in a bid to keep them from coming out in court.[[60]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-60)

In some cases, police have refused to disclose information to the courts citing [non-disclosure agreements](https://en.wikipedia.org/wiki/Non-disclosure_agreements) signed with Harris Corporation.[[58]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-yahoo1-58)[[61]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-nyt1-61)[[62]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-FDLE_NDA-62) The FBI defended these agreements, saying that information about the technology could allow adversaries to circumvent it.[[61]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-nyt1-61) The ACLU has said "potentially unconstitutional government surveillance on this scale should not remain hidden from the public just because a private corporation desires secrecy. And it certainly should not be concealed from judges."[[2]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-wired-sting-2)

In 2015 [Santa Clara County](https://en.wikipedia.org/wiki/Santa_Clara_County) pulled out of contract negotiations with Harris for StingRay units, citing onerous restrictions imposed by Harris on what could be released under public records requests as the reason for exiting negotiations.[[63]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-63)

Criticism[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=16)]

In recent years, legal scholars, public interest advocates, legislators and several members of the judiciary have strongly criticized the use of this technology by law enforcement agencies. Critics have called the use of the devices by government agencies warrantless cell phone tracking, as they have frequently been used without informing the court system or obtaining a warrant.[[2]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-wired-sting-2) The [Electronic Frontier Foundation](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) has called the devices “an unconstitutional, all-you-can-eat data buffet.”[[64]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-64)

In June 2015, WNYC Public Radio published a podcast with Daniel Rigmaiden about the StingRay device.[[65]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-65)

In 2016, Professor Laura Moy of the [Georgetown University Law Center](https://en.wikipedia.org/wiki/Georgetown_University_Law_Center) filed a formal complaint to the FCC regarding the use of the devices by law enforcement agencies, taking the position that because the devices mimic the properties of [cell phone towers](https://en.wikipedia.org/wiki/Cell_site), the agencies operating them are in violation of FCC regulation, as they lack the appropriate [spectrum licenses](https://en.wikipedia.org/wiki/Frequency_allocation).[[66]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-66)

On December 4, 2019, the [American Civil Liberties Union](https://en.wikipedia.org/wiki/American_Civil_Liberties_Union) and the [New York Civil Liberties Union](https://en.wikipedia.org/wiki/New_York_Civil_Liberties_Union) filed a federal [lawsuit](https://en.wikipedia.org/wiki/Lawsuit) against the [Customs and Border Protection](https://en.wikipedia.org/wiki/U.S._Customs_and_Border_Protection) and the [Immigrations and Customs Enforcement](https://en.wikipedia.org/wiki/Immigrations_and_Customs_Enforcement) agencies. According to the ACLU, the union had filed a [Freedom of Information Act](https://en.wikipedia.org/wiki/Freedom_of_Information_Act_(United_States)) request in 2017, but were not given access to documents.[[67]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-:1-67) The NYCLU and ACLU proceeded with the lawsuit under the statement that both CBP and ICE had failed, “to produce a range of records about their use, purchase, and oversight of Stingrays.”[[67]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-:1-67) In an official statement expanding their reasoning for the lawsuit, the ACLU expressed their concern over the Stingrays current and future applications, stating that ICE were using them for “unlawfully tracking journalists and advocates and subjecting people to invasive searches of their electronic devices at the border.”[[67]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-:1-67)

Countermeasures[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=17)]

A number of countermeasures to the StingRay and other devices have been developed, for example [crypto phones](https://en.wikipedia.org/w/index.php?title=Crypto_phone&action=edit&redlink=1) such as GMSK's Cryptophone have firewalls that can identify and thwart the StingRay's actions or alert the user to IMSI capture.[[68]](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_note-wired0914-68)

See also[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=18)]

* ***flag***[***United States portal***](https://en.wikipedia.org/wiki/Portal:United_States)
* ***[icon](https://en.wikipedia.org/wiki/File:A_coloured_voting_box.svg)***[***Politics portal***](https://en.wikipedia.org/wiki/Portal:Politics)
* [Authentication and Key Agreement (protocol)](https://en.wikipedia.org/wiki/Authentication_and_Key_Agreement_(protocol))
* [Cellphone surveillance](https://en.wikipedia.org/wiki/Cellphone_surveillance)
* [Evil Twin Attack](https://en.wikipedia.org/wiki/Evil_Twin_Attack)
* [Mobile phone tracking](https://en.wikipedia.org/wiki/Mobile_phone_tracking)
* [*Kyllo v. United States*](https://en.wikipedia.org/wiki/Kyllo_v._United_States) (lawsuit re thermal image surveillance)
* [*United States v. Davis* (2014)](https://en.wikipedia.org/wiki/United_States_v._Davis_(2014)) found warrantless data collection violated constitutional rights, but okayed data use for criminal conviction, as data collected in good faith

References[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=19)]

* 1. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-Notice,_Acceptance,_Renewal_1-0) [*"Notice, Acceptance, Renewal"*](http://tsdr.uspto.gov/documentviewer?caseId=sn76303503&docId=SPE20130404144554#docIndex=0&page=1)*. Harris/US PTO. Retrieved 23 January 2016.*
  2. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-wired-sting_2-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-wired-sting_2-1) [***c***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-wired-sting_2-2) [***d***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-wired-sting_2-3) *Zetter, Kim (2014-03-03).*[*"Florida Cops' Secret Weapon: Warrantless Cellphone Tracking"*](https://www.wired.com/2014/03/stingray/)*.*[*Wired.com*](https://en.wikipedia.org/wiki/Wired.com)*. Retrieved 2014-06-23.*
  3. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-3) [*"RCMP reveals it uses cellphone trackers in wake of CBC report"*](http://www.cbc.ca/news/technology/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750)*. CBC News. Retrieved 2017-07-25.*
  4. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-4) [*"Stingray Tracking Devices: Who's Got Them?"*](https://www.aclu.org/map/stingray-tracking-devices-whos-got-them)*. aclu.org. American Civil Liberties Union. Retrieved 29 September 2016.*
  5. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-5) [*"New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says"*](https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html)*. New York Times. Retrieved 29 September2016.*
  6. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-6) [*"Revealed: Bristol's police and mass mobile phone surveillance"*](https://thebristolcable.org/2016/10/imsi/)*.*[*The Bristol Cable*](https://en.wikipedia.org/wiki/The_Bristol_Cable)*. Retrieved 2016-11-01.*
  7. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-7) [*"Stingrays bought, quietly used by police forces across England"*](https://arstechnica.co.uk/tech-policy/2016/10/stingrays-in-use-across-england-by-police/)*. Ars Technica UK. Retrieved 2017-04-30.*
  8. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-8) *Gallagher, Ryan (September 25, 2013).*[*"Meet the machines that steal your phone's data"*](https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/)*. Ars Technica. Condé Nast. Retrieved August 22, 2014.*
  9. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-wsj-stingray_9-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-wsj-stingray_9-1) *Valentino-Devries, Jen (Sep 22, 2011).*[*"'Stingray' Phone Tracker Fuels Constitutional Clash"*](https://www.wsj.com/articles/SB10001424053111904194604576583112723197574)*. The Wall Street Journal. Retrieved Aug 22, 2014.*
  10. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-datasheet-1_10-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-datasheet-1_10-1) *Harris WPG (November 29, 2006).*[*"StingRay Cell Site Emulator Datasheet"*](https://web.archive.org/web/20140518034759/http:/egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf)*(PDF). Archived from*[*the original*](http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf)*(PDF)on May 18, 2014. Retrieved August 29, 2014.* [Alt URL](https://www.documentcloud.org/documents/1282626-06-11-29-2006-harris-stingray-datasheet-p-1-of-2.html)
  11. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-datasheet-2_11-0) *Harris WPG (November 29, 2006).*[*"StingRay Cell Site Emulator Datasheet"*](https://web.archive.org/web/20140903063301/http:/tsdr.uspto.gov/documentviewer?caseId=sn76303503#docIndex=19&page=26)*. Archived from*[*the original*](http://tsdr.uspto.gov/documentviewer?caseId=sn76303503#docIndex=19&page=26)*on September 3, 2014. Retrieved August 29, 2014.* [Alt URL](https://www.documentcloud.org/documents/1282621-02-07-18-2002-harris-stingray-datasheet-ocr.html)
  12. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-catalog-airborne_12-0) Harris WPG. (Aug. 25, 2008). Harris Wireless Products Group catalog, available at <https://www.documentcloud.org/documents/1282631-08-08-25-2008-harris-wireless-products-group.html> [PDF p. 4] (last accessed: Aug. 29, 2014), archived from original at <http://egov.ci.miami.fl.us/Legistarweb/Attachments/48000.pdf>[[*permanent dead link*](https://en.wikipedia.org/wiki/Wikipedia:Link_rot)][PDF p. 4] (last accessed: Mar. 8, 2011) (Airborne DF Kit CONUS for StingRay)
  13. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-kingfish-sole-source-justification-fl-1_13-0) Harris WPG. (Nov. 29, 2006). KingFish, KingFish GSM S/W, Pocket PC GSM S/W & Training Sole Source Justification for Florida, available at <https://www.documentcloud.org/documents/1282625-06-11-29-2006-harris-kingfish-sole-source.html> [PDF p. 1] (last accessed: Aug. 29, 2014), archived from original at <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34768.pdf>[PDF p. 1] (last accessed: Aug. 29, 2014) ("The KingFish system is the only man-portable battery powered CDMA & GSM Interrogating, Active Location, and Signal Information Collection system currently available.").
  14. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-morrison-stingray-esn-estraction_14-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-morrison-stingray-esn-estraction_14-1) United States v. Rigmaiden, CR08-814-PHX-DGC, Dkt. #0674-1 [Declaration by FBI Supervisory Agent Bradley S. Morrison], ¶ 5, p. 3 (D.Ariz., Oct. 27, 2011), available at <https://www.documentcloud.org/documents/1282619-11-10-17-2011-u-s-v-rigmaiden-cr08-814-phx-dgc.html> [PDF p. 3] (last accessed: Aug. 30, 2014) ("During a location operation, the electronic serial numbers (ESNs) (or their equivalent) from all wireless devices in the immediate area of the FBI device [(i.e., the StingRay)] that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices.").
  15. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-kingfish-force-power-increase_15-0) Florida v. James L. Thomas, No. 2008-CF-3350A, Suppression Hearing Transcript RE: Harris StingRay & KingFish [testimony of Investigator Christopher Corbitt], p. 17 (2nd Cir. Ct., Leon County, FL, Aug. 23, 2010), available at <https://www.documentcloud.org/documents/1282618-10-08-23-2010-fl-v-thomas-2008-cf-3350a.html> [PDF. p. 17] (last accessed: Aug. 30, 2014) ("[O]nce the equipment comes into play and we capture that handset, to make locating it easier, the equipment forces that handset to transmit at full power.")
  16. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-kingfish-denial-of-service_16-0) Hennepin County, MN. (Feb. 2, 2010). FY2011 FEDERAL APPROPRIATIONS REQUESTS [Cellular Exploitation System (Kingfish) - $426,150], available at <https://www.documentcloud.org/documents/1282634-10-02-02-2010-kingfish-appropriations-request.html> [PDF p. 6] (last accessed: Aug. 30, 2014), archived from original at <http://board.co.hennepin.mn.us/sirepub/cache/246/5hnnteqb5wro1fl4oyplzrqo/10628008302014015243634.PDF>[[*permanent dead link*](https://en.wikipedia.org/wiki/Wikipedia:Link_rot)][PDF p. 6] (last accessed: Aug. 30, 2014) ("The system acts as a mobile wireless phone tower and has the capability to... deny mobile phones service.").
  17. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-kingfish-cell-site-emulation_17-0) Florida v. James L. Thomas, No. 2008-CF-3350A, Suppression Hearing Transcript RE: Harris StingRay & KingFish [testimony of Investigator Christopher Corbitt], p. 12 (2nd Cir. Ct., Leon County, FL, Aug. 23, 2010), available at <https://www.documentcloud.org/documents/1282618-10-08-23-2010-fl-v-thomas-2008-cf-3350a.html> [PDF. p. 12] (last accessed: Aug. 30, 2014) ("In essence, we emulate a cellphone tower. so just as the phone was registered with the real Verizon tower, we emulate a tower; we force that handset to register with us.").
  18. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-hardman-spook-stingray_18-0) *Hardman, Heath (May 22, 2014). "The Brave New World of Cell-Site Simulators". Albany Law School: 11–12.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.2139/ssrn.2440982*](https://doi.org/10.2139%2Fssrn.2440982)*.*[*SSRN*](https://en.wikipedia.org/wiki/SSRN_(identifier))[*2440982*](https://ssrn.com/abstract=2440982)*. For a cell-site simulator operator to induce a cell phone to camp on his or her cell-site simulator (CSS), all he or she needs to do is become the strongest cell in the target cellphones preferred network.*
  19. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-19) [*"Stingray Tracking Devices - A Tool For Mass Surveillance?"*](http://broadbandlanding.com/research/stingray/)*. broadbandlanding.com. Retrieved 2017-04-13.*
  20. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-kingfish-used-on-known-device_20-0) Florida v. James L. Thomas, No. 2008-CF-3350A, Suppression Hearing Transcript RE: Harris StingRay & KingFish [testimony of Investigator Christopher Corbitt], p. 13 (2nd Cir. Ct., Leon County, FL, Aug. 23, 2010), available at <https://www.documentcloud.org/documents/1282618-10-08-23-2010-fl-v-thomas-2008-cf-3350a.html> [PDF. p. 13] (last accessed: Aug. 30, 2014) ("The equipment will basically decode information from the handset and provide certain unique identifying information about the handset, being a subscriber identity and equipment identity.... We compare that with the information provided from Verizon to ensure that we are looking at the correct handset.").
  21. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-21) Id., p. 14 ("And as the equipment is evaluating all the handsets in the area, when it comes across that handset -- the one that we're looking for, for the information that we put into the box -- then it will hang onto that one and allow us to direction find at that point.").
  22. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-kingfish-used-on-unknown-device_22-0) In the Matter of The Application of the United States of America for An Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012) (Law enforcement sought to use StingRay "to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones (e.g., by transmitting the telephone's serial number and phone number)..." so the "[Subject's] Telephone can be identified." (quoting order application)).
  23. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-stingray-protestors_23-0) *Eördögh, Fruzsina (Jun 13, 2014).*[*"Are Chicago Police Spying on Activists? One Man Sues to Find Out"*](https://web.archive.org/web/20140826161122/http:/motherboard.vice.com/en_ca/blog/man-sues-chicago-police-ISMI-catcher-warrantless-cell-phone-spying)*. Mother Jones. Archived from*[*the original*](http://motherboard.vice.com/en_ca/blog/man-sues-chicago-police-ISMI-catcher-warrantless-cell-phone-spying)*on 2014-08-26. Retrieved Aug 24, 2014. Martinez, who works in the software industry, first wondered about police surveilling his phone in 2012 while he was attending the NATO protests. 'I became suspicious because it was really difficult to use our phones[.]'*
  24. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-24) [*"Stingray, IMSI Catcher: FBI Documents Shine Light On Cellphone Tracking Tool"*](http://www.sagaciousnewsnetwork.com/stingray-imsi-catcher-fbi-documents-shine-light-on-cellphone-tracking-tool/)*. Sagacious News Network. 2013-01-18. Retrieved 2017-05-27.*
  25. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-25) Adam Bates January 25, 2017, and PDF (292.42 KB) EPUB (117.68 KB) MOBI (298.06 KB). "Stingray: A New Frontier in Police Surveillance." Cato Institute. N.p., 25 Jan. 2017. Web. 26 May 2017
  26. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-morrison-stingray-denial-of-service_26-0) United States v. Rigmaiden, CR08-814-PHX-DGC, Dkt. #0674-1 [Declaration by FBI Supervisory Agent Bradley S. Morrison], ¶ 4, p. 2-3 (D.Ariz., Oct. 27, 2011), available at <https://www.documentcloud.org/documents/1282619-11-10-17-2011-u-s-v-rigmaiden-cr08-814-phx-dgc.html> [PDF pp. 2-3] (last accessed: Aug. 30, 2014) ("[T]he [][StingRay] used to locate the defendant's aircard did not capture, collect, decode, view, or otherwise obtain any content transmitted from the aircard, and therefore was unable to pass any information from the aircard to Verizon Wireless.").
  27. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-27) United States v. Rigmaiden, CR08-814-PHX-DGC, Doc. #723, p. 14 (D.Ariz., Jan. 5, 2012) (Noting government concession that the StingRay "caused a brief disruption in service to the aircard.").
  28. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-28) *Quintin, Cooper (2018-08-27).*[*"Sen. Wyden Confirms Cell-Site Simulators Disrupt Emergency Calls"*](https://www.eff.org/deeplinks/2018/08/blog-post-wyden-911-disruption-css)*. Electronic Frontier Foundation. Retrieved 2019-03-25.*
  29. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-dea-fishhawk_29-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-dea-fishhawk_29-1) [***c***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-dea-fishhawk_29-2) [***d***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-dea-fishhawk_29-3) Drug Enforcement Administration. (Aug. 29, 2007). FY2011 FEDERAL APPROPRIATIONS REQUESTS [Sole Source Notice of Harris StingRay FishHawk GSM encryption key extraction and intercept upgrade], available at <https://www.documentcloud.org/documents/1282642-07-08-29-2007-dea-purchase-of-stingray-fishhawk.html> [PDF p. 1] (last accessed: Aug. 30, 2014), archived from the original at <https://www.fbo.gov/index?s=opportunity&mode=form&id=9aa2169a324ae7a1a747c2ca8f540cb3&tab=core&_cview=0> (last accessed: Aug. 30, 2014). ("The Tech 2 Me w/FishHawk GSM Intercept S/W upgrade is the only portable standard + 12VDC powered over the air GSM Active Key Extraction and Intercept system currently available.")
  30. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-GSM-intercept-simple-explain_30-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-GSM-intercept-simple-explain_30-1) *Green, Matthew.*[*"On cellular encryption"*](http://blog.cryptographyengineering.com/2013/05/a-few-thoughts-on-cellular-encryption.html)*. A Few Thoughts on Cryptographic Engineering. Retrieved Aug 29, 2014.*
  31. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-GSM-intercept-complex-explain_31-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-GSM-intercept-complex-explain_31-1) *Barkan, Elad; Biham, Eli; Keller, Nathan.*[*"Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communications"*](https://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf)*(PDF): 12–13.*
  32. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-GSM-A51-cryptanalysis_32-0) *Schneier, Brude.*[*"Cryptanalysis of A5/1"*](https://www.schneier.com/blog/archives/2008/02/cryptanalysis_o_1.html)*. Schneier on Security. Retrieved Aug 29, 2014.*
  33. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-ReferenceA_33-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-ReferenceA_33-1) Id.
  34. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-34) [*"Police use cellphone spying device"*](https://web.archive.org/web/20140701152046/http:/www.myfoxny.com/story/25597191/police-use-cellphone-spying-device)*.*[*Associated Press*](https://en.wikipedia.org/wiki/Associated_Press)*. 2014-05-30. Archived from*[*the original*](http://www.myfoxny.com/story/25597191/police-use-cellphone-spying-device)*on 2014-07-01. Retrieved 2014-06-23.*
  35. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-35) *Campbell, John (2013-01-24).*[*"LAPD Spied on 21 Using StingRay Anti-Terrorism Tool"*](http://www.laweekly.com/news/lapd-spied-on-21-using-stingray-anti-terrorism-tool-2612739)*.*[*LA Weekly*](https://en.wikipedia.org/wiki/LA_Weekly)*. Retrieved 2014-06-23.*
  36. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-36) [*"As Secretive "Stingray" Surveillance Tool Becomes More Pervasive, Questions Over Its Illegality Increase"*](https://www.eff.org/deeplinks/2013/02/secretive-stingray-surveillance-tool-becomes-more-pervasive-questions-over-its)*. Electronic Frontier Foundation. 2013-02-12. Retrieved 2017-03-12.*
  37. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-37) *Nail, Derrol (23 February 2015).*[*"Harris Corporation opens new tech center in Palm Bay"*](https://web.archive.org/web/20150409014938/http:/www.myfoxorlando.com/story/28181324/harris-corporation-opens-new-tech-center-in-palm-bay)*. myfoxorlando.com.*[*WOFL*](https://en.wikipedia.org/wiki/WOFL)*,*[*Fox Broadcasting Company*](https://en.wikipedia.org/wiki/Fox_Broadcasting_Company)*. Archived from*[*the original*](http://www.myfoxorlando.com/story/28181324/harris-corporation-opens-new-tech-center-in-palm-bay)*on 9 April 2015. Retrieved 4 April 2015.*
  38. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-38) *Farivar, Cyrus (25 February 2015).*[*"Powerful "stingrays" used to go after 911 hangup, ATM burglary"*](https://arstechnica.com/tech-policy/2015/02/powerful-stingrays-used-to-go-after-911-hangup-atm-burglary/)*. Ars Technica. Retrieved 25 March 2015. ...Palm Bay Police Department simply borrowed a stingray directly from its manufacturer, the Harris Corporation—located down the road in Melbourne, Florida—to respond to a 2006 bomb threat at a school, absent any judicial oversight.*
  39. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-39) *Detective M. J. Pusatere.*[*"03.05.2014 PBPD Stingray Records (Bates Stamped) redacted"*](https://www.aclu.org/files/assets/floridastingray/03.05.2014%20-%20PBPD%20Stingray%20Records%20excerpt_Redacted.pdf)*(PDF). aclu.org. Palm Bay Police Department, American Civil Liberties Union. p. 3. Retrieved 24 March 2015.*
  40. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-40) *Aaronson, Trevor (23 February 2015).*[*"ACLU Releases Florida StingRay Documents"*](http://fcir.org/2015/02/23/aclu-releases-florida-stingray-documents/)*. fcir.org. Florida Center for Investigative Reporting. Retrieved 4 April 2015.*
  41. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-41) *Rivero, Daniel (18 March 2015).*[*"It's now a trend: third court orders the release of phone-tracking Stingray documents"*](http://fusion.net/story/105521/courts-ordering-the-release-of-stingray-documents-is-now-a-trend/)*. fusion.net.*[*Fusion*](https://en.wikipedia.org/wiki/Fusion_(TV_channel))*. Retrieved 4 April 2015.*
  42. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-42) Stingray Tracking Devices: Who's Got Them?" American Civil Liberties Union. American Civil Liberties Union, n.d. Web. 24 May 2017
  43. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-43) *House Committee on Oversight and Government Reform (December 19, 2016).*[*"House Oversight Committee Report on Law Enforcement Use of Cell-Site Simulation Technologies"*](https://publicintelligence.net/us-cell-site-simulator-privacy/)*. Public Intelligence. Retrieved February 18, 2020.*
  44. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-44) *Fenton, Justin.*[*"Key evidence in city murder case tossed due to stingray use"*](http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-stingray-murder-evidence-suppressed-20160425-story.html)*. baltimoresun.com. Retrieved 2017-09-23.*
  45. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-45) *Emmons, Alex (2016-03-31).*[*"Maryland Appellate Court Rebukes Police for Concealing Use of Stingrays"*](https://theintercept.com/2016/03/31/maryland-appellate-court-rebukes-police-for-concealing-use-of-stingrays/)*. The Intercept. Retrieved 2017-09-23.*
  46. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-46) *Jackman, Tom (2017-09-21).*[*"Police use of 'StingRay' cellphone tracker requires search warrant, appeals court rules"*](https://www.washingtonpost.com/news/true-crime/wp/2017/09/21/police-use-of-stingray-cellphone-tracker-requires-search-warrant-appeals-court-rules/)*. Washington Post.*[*ISSN*](https://en.wikipedia.org/wiki/ISSN_(identifier))[*0190-8286*](https://www.worldcat.org/issn/0190-8286)*. Retrieved 2017-09-23.*
  47. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-47) [*"Appeals court: It doesn't matter how wanted man was found, even if via stingray"*](https://arstechnica.com/tech-policy/2016/11/appeals-court-it-doesnt-matter-how-wanted-man-was-found-even-if-via-stingray/)*. Ars Technica. Retrieved 2017-09-23.*
  48. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-48) [*"Vancouver police admit"*](http://www.cbc.ca/news/canada/british-columbia/vancouver-police-stingray-use-cellphone-tracking-civil-liberties-1.3713042)*. Canadian Broadcast Corp (CBC). 9 August 2016.*
  49. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-49) [*"Edmonton police backtrack after admitting to using controversial cellphone surveillance device"*](https://edmontonjournal.com/news/crime/edmonton-police-backtrack-after-admitting-to-using-controversial-cellphone-surveillance-device)*. Edmonton Journal. 12 August 2016. Retrieved 11 December 2016.*
  50. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-50) *Mooney, John (9 February 2014).*[*"GSOC under high-tech surveillance"*](http://www.thesundaytimes.co.uk/sto/news/ireland/article1373695.ece)*. The Sunday Times.*
  51. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-51) *Tynan, Dr. Richard (15 February 2014).*[*"Beirtear na IMSIs: Ireland's GSOC surveillance inquiry reveals use of mobile phone interception systems"*](https://web.archive.org/web/20140624015718/https:/www.privacyinternational.org/blog/beirtear-na-imsis-irelands-gsoc-surveillance-inquiry-reveals-use-of-mobile-phone-interception)*. Privacy International. Archived from*[*the original*](https://www.privacyinternational.org/blog/beirtear-na-imsis-irelands-gsoc-surveillance-inquiry-reveals-use-of-mobile-phone-interception)*on 2014-06-24. Retrieved 2014-08-25.*
  52. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-BBC_Sky_52-0) [*"Mass snooping fake mobile towers uncovered in UK"*](https://www.bbc.com/news/business-33076527)*. British Broadcasting Corporation. 10 June 2015.*
  53. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-london_met_53-0) *Cheshire, Tom (10 June 2015).*[*"Fake Mobile Phone Towers Operating In The UK"*](http://news.sky.com/story/1499258/fake-mobile-phone-towers-operating-in-the-uk)*. Sky News.*
  54. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-54) *Cox, Joseph (26 August 2016).*[*"British Companies Are Selling Advanced Spy Tech to Authoritarian Regimes"*](https://motherboard.vice.com/en_us/article/the-uk-companies-exporting-interception-tech-around-the-world)*. Motherboard.*[*Vice*](https://en.wikipedia.org/wiki/Vice_Media)*. Retrieved 1 May 2017.*
  55. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-:0_55-0) *Fenton, Justin (April 20, 2015).*[*"Baltimore judge allows police use of Stingray phone tracking in murder case"*](http://www.baltimoresun.com/news/maryland/crime/blog/bs-md-ci-stingray-new-disclosures-20150420-story.html)*. The Baltimore Sun. Retrieved April 22, 2017. Police outlined for the first time this month their usage of the stingray, pegging it at more than 4,300 times — a figure experts called a "huge number" compared to a trickle of disclosures in other cities.*
  56. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-56) Monahan, Torin (2016) [Built to Lie: Investigating Technologies of Deception, Surveillance, and Control](http://publicsurveillance.com/papers/Built-to-lie.pdf). The Information Society 32(4): 229-240.
  57. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-57) *Wessler, Nathan Freed.*[*"U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information From Public"*](https://www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-seize-local-cops-cell-phone-tracking-files)*.*[*American Civil Liberties Union*](https://en.wikipedia.org/wiki/American_Civil_Liberties_Union)*. Retrieved 2014-06-23.*
  58. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-yahoo1_58-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-yahoo1_58-1) *Gillum, Jack (2014-03-22).*[*"Police keep quiet about cell-tracking technology"*](https://news.yahoo.com/police-keep-quiet-cell-tracking-technology-070618821--finance.html)*. News.yahoo.com. Retrieved 2014-06-23.*
  59. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-59) *Wessler, Nathan Freed (2014-06-03).*[*"Transcription of Suppression Hearing (Complete)"*](https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf)*(PDF).*[*American Civil Liberties Union*](https://en.wikipedia.org/wiki/American_Civil_Liberties_Union)*. Retrieved 2014-06-23.*
  60. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-60) *Zetter, Kim (2014-06-03).*[*"U.S. Marshals Seize Cops' Spying Records to Keep Them From the ACLU"*](https://www.wired.com/2014/06/feds-seize-stingray-documents/)*.*[*Wired.com*](https://en.wikipedia.org/wiki/Wired.com)*. Retrieved 2014-06-23.*
  61. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-nyt1_61-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-nyt1_61-1) [*"A Police Gadget Tracks Phones? Shhh! It's Secret"*](https://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0)*. The New York Times. March 15, 2015.*
  62. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-FDLE_NDA_62-0) [*Florida Department of Law Enforcement*](https://en.wikipedia.org/wiki/Florida_Department_of_Law_Enforcement)*; Harris Corporation (8 June 2010).*[*"FDLE non-disclosure agreement with the Harris Corporation"*](https://www.aclu.org/files/assets/floridastingray/03.27.2014%20-%20FDLE%20Stingray%20Records%20Non-Disclosure%20Agreement%20with%20Harris%20Corp.pdf)*(PDF). American Civil Liberties Union. Retrieved 28 March 2015.*
  63. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-63) *Farivar, Cyrus (7 May 2015).*[*"In rare move, Silicon Valley county gov't kills stingray acquisition"*](https://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/)*. Ars Technica. Retrieved 9 May2015. What happened was, we were in negotiations with Harris, and we couldn't get them to agree to even the most basic criteria we have in terms of being responsive to public records requests*
  64. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-64) *Timm, Trevor (2013-02-12).*[*"As Secretive "Stingray" Surveillance Tool Becomes More Pervasive, Questions Over Its Illegality Increase"*](https://www.eff.org/deeplinks/2013/02/secretive-stingray-surveillance-tool-becomes-more-pervasive-questions-over-its)*.*[*Electronic Frontier Foundation*](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation)*. Retrieved 2014-06-23.*
  65. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-65) *Zomorodi, Manoush (2015-06-19).*[*"When Your Conspiracy Theory Is True"*](http://www.wnyc.org/story/stingray-conspiracy-theory-daniel-rigmaiden-radiolab/)*.*[*WNYC*](https://en.wikipedia.org/wiki/WNYC)*. Retrieved 2015-07-03.*
  66. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-66) *Farivar, Cyrus (August 16, 2016).*[*"Baltimore police accused of illegal mobile spectrum use with stingrays"*](https://arstechnica.com/tech-policy/2016/08/baltimore-police-accused-of-illegal-mobile-spectrum-use-with-stingrays/)*.*[*Ars Technica*](https://en.wikipedia.org/wiki/Ars_Technica)*. Retrieved 2016-08-16.*
  67. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-:1_67-0) [***b***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-:1_67-1) [***c***](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-:1_67-2) *Ramirez, Alexia (December 11, 2019).*[*"ICE and CBP Are Secretly Tracking Us Using Stingrays. We're Suing"*](https://www.aclu.org/news/privacy-technology/ice-and-cbp-are-secretly-tracking-us-using-stingrays-were-suing/)*. ACLU.org. Retrieved February 18, 2020.*
  68. [**^**](https://en.wikipedia.org/wiki/Stingray_phone_tracker#cite_ref-wired0914_68-0) *Zetter, Kim (2014-09-03).*[*"Phone Firewall Identifies Rogue Cell Towers Trying to Intercept Your Calls"*](https://www.wired.com/2014/09/cryptophone-firewall-identifies-rogue-cell-towers/)*. Wired. Condé Nast. Retrieved 13 July 2016.*

Further reading[[edit](https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&action=edit&section=20)]

* *Lye, Linda (2014).*[*"StingRays: The Most Common Surveillance Tool the Government Won't Tell You About"*](https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About_0.pdf)*(PDF).*[*ACLU*](https://en.wikipedia.org/wiki/ACLU)*Northern California.*
* IMSI catchers, and specifically the Harris Stingray, are extensively used in the Intelligence Support Activity/Task Force Orange thriller written by J. T. Patten, a former counterterrorism intelligence specialist. Patten, J. T., *Buried in Black*. A Task Force Orange novel. Lyrical Press/Penguin, 2018.