

Stingray phone tracker

From Wikipedia, the free encyclopedia

The **StingRay** is an IMSI-catcher, a controversial cellular phone surveillance device, manufactured by Harris Corporation.^[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 the United States^{[3][4]} and possibly covertly in the United Kingdom.^[5] **Stingray** has also become a generic name to describe these kinds of devices.^[6]



A Stingray device in 2013, in Harris's trademark submission.

^[1]

Contents

- 1 Technology
 - 1.1 Active mode operations
 - 1.2 Passive mode operations
 - 1.3 Active (cell site simulator) capabilities
 - 1.3.1 Extracting data from internal storage
 - 1.3.2 Writing metadata to internal storage
 - 1.3.3 Forcing an increase in signal transmission power
 - 1.3.4 Forcing an abundance of signal transmissions
 - 1.3.5 Tracking and locating
 - 1.3.6 Denial of service
 - 1.3.7 Interception of communications content
 - 1.4 Passive capabilities
 - 1.4.1 Base station (cell site) surveys
- 2 Usage by law enforcement
 - 2.1 In the United States
 - 2.2 Outside the United States
- 3 Secrecy
- 4 Criticism
- 5 Countermeasures
- 6 See also
- 7 References
- 8 Further reading

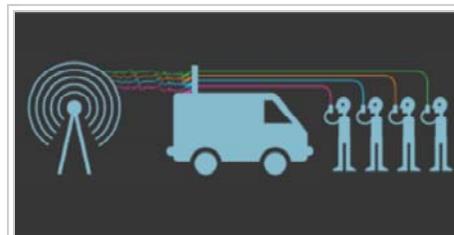
Technology

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.^{[7][8][9]}

The StingRay family of devices can be mounted in vehicles,^[8] on airplanes, helicopters and unmanned aerial vehicles.^[10] Hand-carried versions are referred to under the trade name **KingFish**.^[11]

Active mode operations

1. Extracting stored data such as International Mobile Subscriber Identity ("IMSI") numbers and Electronic Serial Number ("ESN"),^[12]
2. Writing cellular protocol metadata to internal storage
3. Forcing an increase in signal transmission power,^[13]
4. Forcing an abundance of radio signals to be transmitted
5. Interception of communications content
6. Tracking and locating the cellular device user,^[7]
7. Conducting a denial of service attack
8. Encryption key extraction.^[14]
9. Radio jamming for either general denial of service purposes^[15] or to aid in active mode protocol rollback attacks



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.

Passive mode operations

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

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.^[16] 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.^[17] 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

During the process of forcing connections from all compatible cellular devices in a given area, the StingRay operator needs to determine which device is a desired surveillance target. This is accomplished by downloading the IMSI, ESN, or other identifying data from each of the devices connected to the StingRay.^[12] 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.

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.^[18] 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.^[19]

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.^[20] For example, if visual surveillance is being conducted on a group of protestors,^[21] 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.

Writing metadata to internal storage

Forcing an increase in signal transmission power

Cellular telephones are radio transmitters and receivers much like a walkie-talkie. However, the cell phone only communicates with a "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 land-line wires). Radio is used also to transmit a caller's voice/data back to the receiver's cell telephone. The two-way 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 transmit 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.

Coding of all transmissions allows two nearby cell user users no cross talk or interference between the two (this coding is not encryption, which is another, different coding). 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 clandestine 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 clandestine radio being programmed to hide itself from normal detection. The ordinary user can not know if their cell phone is captured via overpower boosts or not. (There are other ways of clandestine capture that need not overpower, too.)

Just as a person shouting drowns out someone whispering, the boost in RF watts 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 only requires more RF watts of power, and thus it is more simple than other types of clandestine controls. 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 clandestine 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.

Forcing an abundance of signal transmissions

Tracking and locating

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.

Denial of service

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.^[22] Instead, the device causes a disruption in service.^[23] 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.

Interception of communications content

By way of software upgrades,^{[14][24]} the StingRay and similar Harris products can be used to intercept 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: (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"^[14] 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"^[14] 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.^[25] 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.^[26] 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 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.^[27] However, GSM also supports an export weakened variant of A5/1 called A5/2. This weaker encryption cypher can be cracked in real-time.^[25] While A5/1 and A5/2 use different cypher strengths, they each use the same underlying encryption key stored on the SIM card.^[26] Therefore, the StingRay performs "GSM Active Key Extraction"^[14] 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.^[28] 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.^[28]

Passive capabilities

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

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

In the United States

The use of the devices has been frequently funded by grants from the Department of Homeland Security.^[29] The Los Angeles Police Department used a Department of Homeland Security grant in 2006 to buy a StingRay for "regional terrorism investigations". However, according to the Electronic Frontier Foundation, the "LAPD has been using it for just about any investigation imaginable."^[30]

In addition to federal law enforcement, military and intelligence agencies, StingRays have in recent years been purchased by local and state law enforcement agencies. According to the American Civil Liberties Union, 42 law enforcement agencies in 17 states own StingRay technology. In November 2014, *Slate* reported that at least 46 state and local police departments, from Sunrise, Florida, to Hennepin County, Minnesota, use cell-site simulators, with a price-tag of US\$16,000 to more than US\$125,000 for each unit.^[31] In 2015, it was reported that the Baltimore Police Department's frequency in using the device was "inexplicably high".^[32] In some states, the devices are made available to local police departments by state surveillance units. The federal government funds most of the purchases with anti-terror grants.

In 2006, Harris employees directly conducted wireless surveillance using StingRay units on behalf the Palm Bay Police Department — where Harris has a campus^[33] — in response to a bomb threat against a middle school. The search was conducted without a warrant or Judicial oversight.^{[34][35][36][37]}

Outside the United States

Privacy International and *The Sunday Times* reported on the usage of StingRays and IMSI-catchers in Ireland, against the Irish Garda Síochána Ombudsman Commission (GSOC), which is an oversight agency of the Irish police force Garda Síochána.^{[38][39]}

On June 10, 2015 the BBC reported on an investigation by Sky News^{[40][41]} about possible false mobile phone towers being used by the London Metropolitan Police. Commissioner Bernard Hogan-Howe refused comment.

Secrecy

The increasing use of the devices has largely been kept secret from the court system and the public.^[32] In 2014, police in 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] The 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.^[42]

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.^[43] In June 2014, the American Civil Liberties Union published information from court regarding the extensive use of these devices by local Florida police.^[44] After this publication, United States Marshals Service then seized the local police's surveillance records in a bid to keep them from coming out in court.^[45]

In some cases, police have refused to disclose information to the courts citing non-disclosure agreements signed with Harris Corporation.^{[43][46][47]} The FBI defended these agreements, saying that information about the technology could allow adversaries to circumvent it.^[46] 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]

In 2015 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.^[48]

Criticism

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] The Electronic Frontier Foundation has called the devices “an unconstitutional, all-you-can-eat data buffet.”^[49]

In June 2015, WNYC Public Radio published a podcast with Daniel Rigmaiden about the StingRay device.^[50]

In 2016, Professor Laura Moy of the 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, the agencies operating them are in violation of FCC regulation, as they lack the appropriate spectrum licenses.^[51]

Countermeasures

A number of countermeasures to the StingRay and other devices have been developed, for example Crypto phones such as GSMK's Cryptophone have firewalls that can identify and thwart the StingRay's actions or alert the user to IMEI capture.^[52] This can also be done with certain applications.

See also

- Cellphone surveillance
- Mobile phone tracking
- *Kyllo v. United States* (lawsuit re thermal image surveillance)
- *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
- Evil Twin Attack

References

1. "Notice, Acceptance, Renewal". Harris/US PTO. Retrieved 23 January 2016.
2. Zetter, Kim (2014-03-03). "Florida Cops' Secret Weapon: Warrantless Cellphone Tracking". *Wired.com*. Retrieved 2014-06-23.
3. "Stingray Tracking Devices: Who's Got Them?". *aclu.org*. American Civil Liberties Union. Retrieved 29 September 2016.
4. "New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says". *New York Times*. Retrieved 29 September 2016.
5. "Revealed: Bristol's police and mass mobile phone surveillance". *The Bristol Cable*. Retrieved 2016-11-01.
6. Gallagher, Ryan (September 25, 2013). "Meet the machines that steal your phone's data". *Ars Technica*. Condé Nast. Retrieved August 22, 2014.
7. Valentino-Devries, Jen (Sep 22, 2011). "'Stingray' Phone Tracker Fuels Constitutional Clash". *The Wall Street Journal*. Retrieved Aug 22, 2014.
8. Harris WPG (November 29, 2006). "StingRay Cell Site Emulator Datasheet". Archived from the original (PDF) on August 29, 2014. Retrieved August 29, 2014.
9. Harris WPG (November 29, 2006). "StingRay Cell Site Emulator Datasheet". Archived from the original on August 29, 2014. Retrieved August 29, 2014.

10. 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> [PDF p. 4] (last accessed: Mar. 8, 2011) (Airborne DF Kit CONUS for StingRay)
11. 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.").
12. 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.").
13. 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.")
14. 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 original at https://www.fbo.gov/index?s=opportunity&mode=form&id=9aa2169a324ae7a1a747c2ca8f540cb3&tab=core&_cview=0 (last accessed: Aug. 30, 2014). ("The Harris StingRay system 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.")
15. 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/246/5hnnteqb5wro1f14oyplzrqo/10628008302014015243634.PDF> [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.").
16. 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.").
17. Hardman, Heath (May 22, 2014). "THE BRAVE NEW WORLD OF CELL-SITE SIMULATORS". Albany Law School: 11–12. doi:10.2139/ssrn.2440982. Retrieved Aug 24, 2014. "For a cell-site simulator operator to induce a cellphone 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."
18. 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 insure that we are looking at the correct handset.").
19. 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.").
20. 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)).
21. Eördögh, Fruzsina (Jun 13, 2014). "Are Chicago Police Spying on Activists? One Man Sues to Find Out". *Mother Jones*. 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[.]'"

22. *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.").
23. *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.").
24. 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> [PDF p. 4] (last accessed: Mar. 8, 2011) (GSM Software Intercept Package for StingRay and StingRay II)
25. Green, Matthew. "On cellular encryption". *A Few Thoughts on Cryptographic Engineering*. Retrieved Aug 29, 2014.
26. Barkan, Elad; Biham, Eli; Keller, Nathan. "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communications" (PDF): 12–13.
27. Schneier, Bruce. "Cryptanalysis of A5/1". *Schneier on Security*. Retrieved Aug 29, 2014.
28. *Id.*
29. "Police use cellphone spying device". Associated Press. 2014-05-30. Retrieved 2014-06-23.
30. Campbell, John (2013-01-24). "LAPD Spied on 21 Using StingRay Anti-Terrorism Tool". *LA Weekly*. Retrieved 2014-06-23.
31. Klonick, Kate (2014-11-10). "Stingrays: Not Just for Feds!". *Slate Magazine*. The Slate Group, a Graham Holdings Company. Retrieved 2014-11-13.
32. Fenton, Justin (April 20, 2015). "Baltimore Police say Stingray phone tracking use exceeds 25,000 instances". *The Baltimore Sun*. Retrieved April 20, 2015. "David Rocah, a staff attorney with the American Civil Liberties Union of Maryland, said the 25,000 figure seemed "inexplicably high.""
33. Nail, Derrol (23 February 2015). "Harris Corporation opens new tech center in Palm Bay". *myfoxorlando.com*. WOFL, Fox Broadcasting Company. Retrieved 4 April 2015.
34. Farivar, Cyrus (25 February 2015). "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."
35. Detective M. J. Pusatere. "03.05.2014 PBPD Stingray Records (Bates Stamped) redacted" (PDF). *aclu.org*. Palm Bay Police Department, American Civil Liberties Union. p. 3. Retrieved 24 March 2015.
36. Aaronson, Trevor (23 February 2015). "ACLU Releases Florida StingRay Documents". *fcir.org*. Florida Center for Investigative Reporting. Retrieved 4 April 2015.
37. Rivero, Daniel (18 March 2015). "It's now a trend: third court orders the release of phone-tracking Stingray documents". *fusion.net*. Fusion. Retrieved 4 April 2015.
38. Mooney, John (9 February 2014). "GSOC under high-tech surveillance". *The Sunday Times*.
39. Tynan, Dr. Richard (15 February 2014). "Beirtear na IMSIs: Ireland's GSOC surveillance inquiry reveals use of mobile phone interception systems". Privacy International.
40. "Mass snooping fake mobile towers uncovered in UK". British Broadcasting Corporation. 10 June 2015.
41. Cheshire, Tom (10 June 2015). "Fake Mobile Phone Towers Operating In The UK". *Sky News*.
42. Wessler, Nathan Freed. "U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information From Public". *American Civil Liberties Union*. Retrieved 2014-06-23.
43. Gillum, Jack (2014-03-22). "Police keep quiet about cell-tracking technology". *News.yahoo.com*. Retrieved 2014-06-23.
44. Wessler, Nathan Freed (2014-06-03). "Transcription of Suppression Hearing (Complete)" (PDF). *American Civil Liberties Union*. Retrieved 2014-06-23.
45. Zetter, Kim (2014-06-03). "U.S. Marshals Seize Cops' Spying Records to Keep Them From the ACLU". *Wired.com*. Retrieved 2014-06-23.
46. "A Police Gadget Tracks Phones? Shhh! It's Secret". *The New York Times*. March 15, 2015.
47. Florida Department of Law Enforcement; Harris Corporation (8 June 2010). "FDLE non-disclosure agreement with the Harris Corporation" (PDF). *American Civil Liberties Union*. Retrieved 28 March 2015.
48. Farivar, Cyrus (7 May 2015). "In rare move, Silicon Valley county gov't kills stingray acquisition". *Ars Technica*. Retrieved 9 May 2015. "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"
49. Timm, Trevor (2013-02-12). "As Secretive "Stingray" Surveillance Tool Becomes More Pervasive, Questions Over Its Illegality Increase". *Electronic Frontier Foundation*. Retrieved 2014-06-23.
50. Zomorodi, Manoush (2015-06-19). "When Your Conspiracy Theory Is True". *WNYC*. Retrieved 2015-07-03.
51. Farivar, Cyrus (August 16, 2016). "Baltimore police accused of illegal mobile spectrum use with stingrays". *Ars technica*. Retrieved 2016-08-16.
52. Zetter, Kim (2014-09-03). "Phone Firewall Identifies Rogue Cell Towers Trying to Intercept Your Calls". *Wired*. Condé Nast. Retrieved 13 July 2016.

Further reading

- 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) ACLU of Northern California.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Stingray_phone_tracker&oldid=747417898"

Categories: Telecommunications equipment | Surveillance | Mobile security | Telephone tapping
| Telephony equipment | Law enforcement equipment

- This page was last modified on 2 November 2016, at 08:08.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.