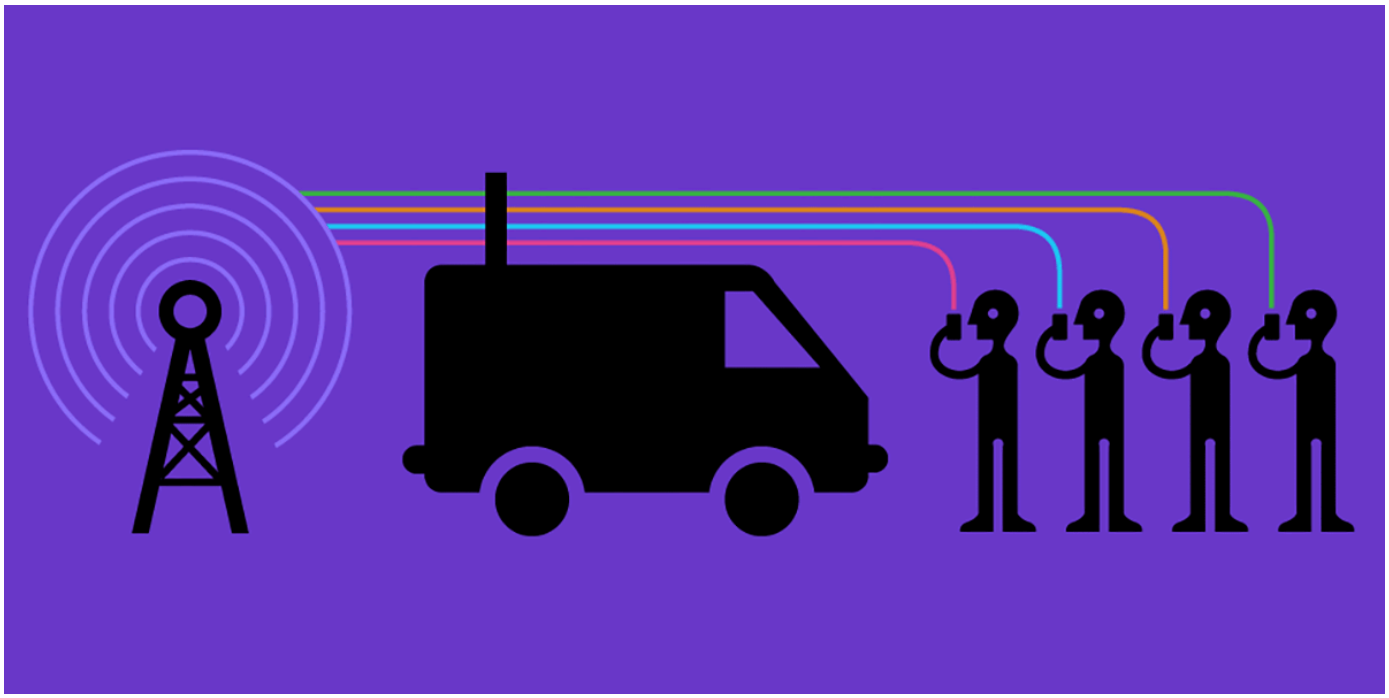
STREET LEVEL SURVEILLANCE



CELL-SITE SIMULATORS/ IMSI CATCHERS

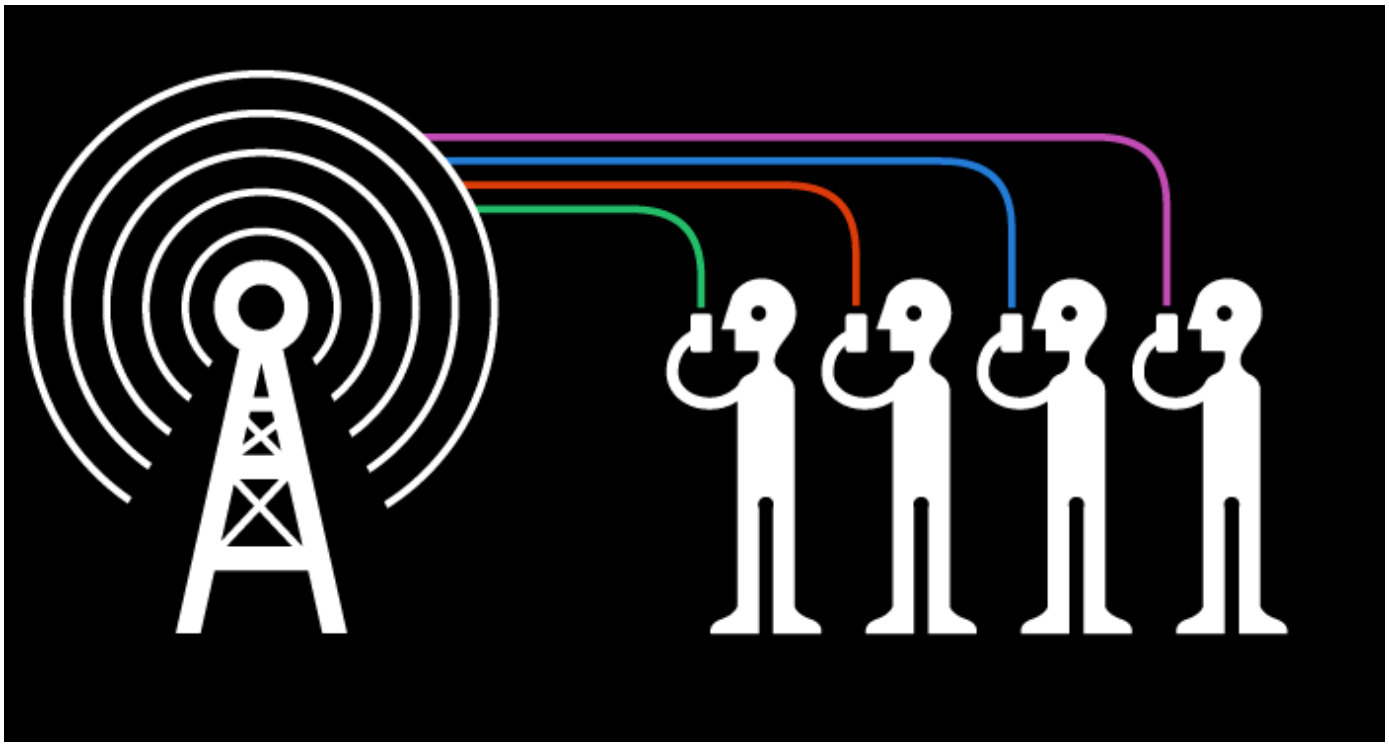
Cell-site simulators, also known as Stingrays or IMSI catchers, are devices that masquerade as legitimate cell-phone towers, tricking phones within a certain radius into connecting to the device rather than a tower.

Cell-site simulators operate by conducting a general search of all cell phones within the device's radius, in violation of basic constitutional protections. Law enforcement use cell-site simulators to pinpoint the location of phones with greater accuracy than phone companies and without needing to involve the phone company at all. Cell-site simulators can also log IMSI numbers, (International Mobile Subscriber Identifiers) unique to each SIM card, of all of the mobile devices within a given area. Some cell-site simulators may have advanced features allowing law enforcement to intercept communications.

How Cell-Site Simulators Work

Standard Communication

by one transceiver, also known as a cell-site or base station. Your phone naturally connects with the closest base station to provide you service as you move through various cells.



SOURCE: EFF

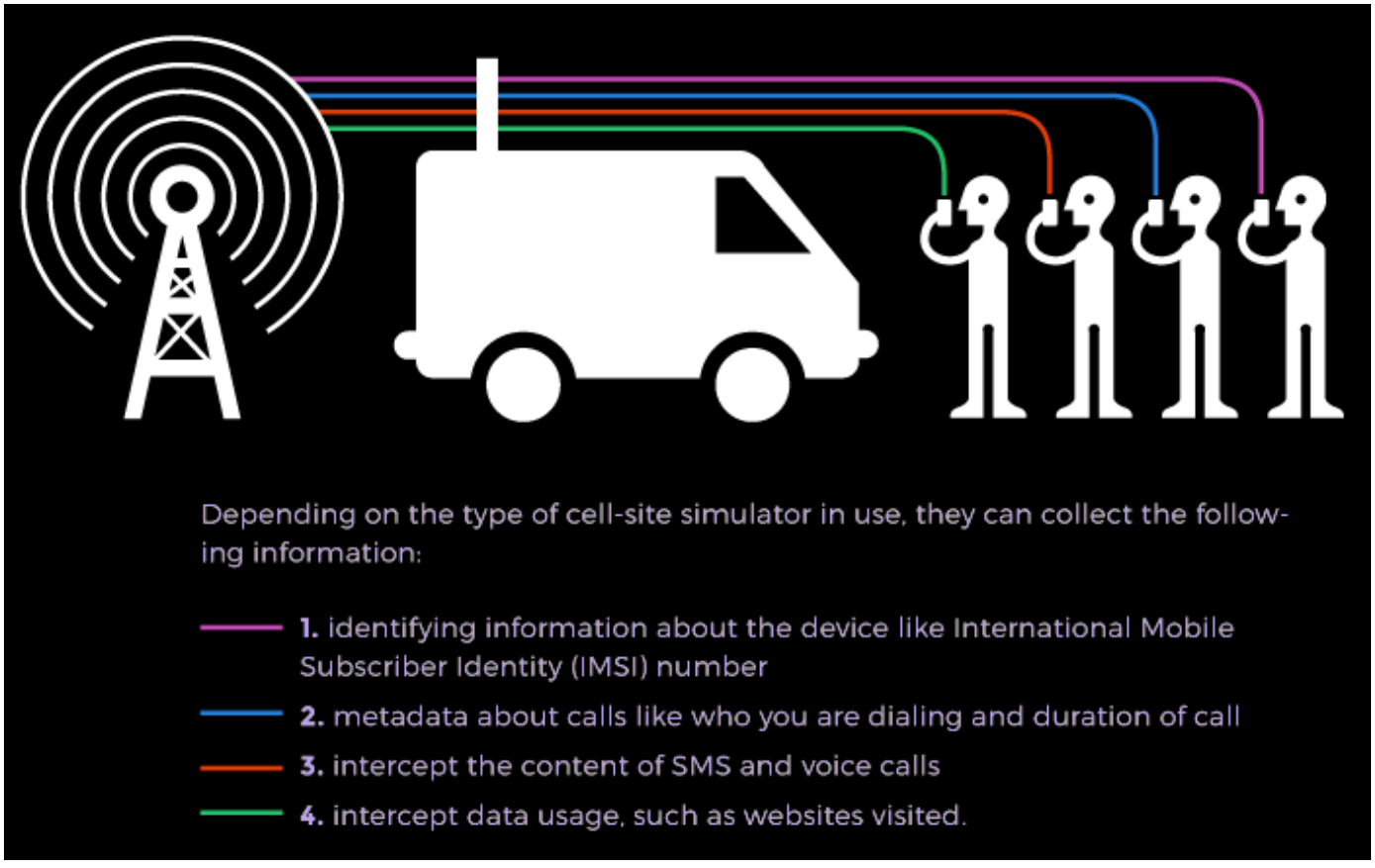
Generally, there are two types of device used by law enforcement that are often referred to interchangeably: passive devices (which we will call IMSI catchers), and active devices (which we will call cell-site simulators.) Passive devices, as a rule, do not transmit any signals. They work by plucking cellular transmissions out of the air, the same way an FM radio works. They then decode (and sometimes decrypt) those signals to find the IMSI of the mobile device and track it.

Active cell-site simulators are much more commonly used by law enforcement, and work very differently from their passive cousins. Cellular devices are designed to connect to the cell site nearby with the strongest signal. To exploit this, cell-site simulators broadcast signals that are either stronger than the legitimate cell sites around them, or are made to appear stronger. This causes devices within range to disconnect from their service providers' legitimate cell sites and to instead establish a new connection with the cell-site simulator. Cell-site simulators can also take advantage of flaws in the design of cellular protocols (such as 2G/3G/4G/5G) to cause phones to disconnect from a legitimate cell-site and connect to the cell-site simulator instead. For the purposes of this article we will focus on active cell-site simulators.

accessed by an active cell-site simulator, and it is impossible for anyone to know if their phone's signals have been accessed by a passive IMSI catcher. Apps for identifying the use of cell-site simulators, such as SnoopSnitch, may not be verifiably accurate. Some more advanced tools have been built, which may be more accurate. For instance, security researchers at the University of Washington have designed a system to measure the use of cell-site simulators across Seattle, and EFF researchers have designed a similar system.

What Kinds of Data Cell-Site Simulators Collect

Data collected by cell-site simulators can reveal intensely personal information about anyone who carries a phone, whether or not they have ever been suspected of a crime.



SOURCE: EFF

Cell-site simulator surveillance: Cell-site simulators trick your phone into thinking they are base stations.

Once your cellular device has connected to a cell-site simulator, the cell-site simulator can determine your location and trigger your device to transmit its IMSI for later

2G/GSM connection then it can potentially perform much more intrusive acts such as intercepting call metadata (what numbers were called or called the phone and the amount of time on each call), the content of unencrypted phone calls and text messages and some types of data usage (such as websites visited). Additionally, marketing materials produced by the manufacturers of cell-site simulators indicate that they can be configured to divert calls and text messages, edit messages, and even spoof the identity of a caller in text messages and calls on a 2G/GSM network.

How Law Enforcement Uses Cell-Site Simulators

Police can use cell-site simulators to try to locate a person when they already know their phone's identifying information, or to gather the IMSI (and later the identity) of anyone in a specific area. Some cell-site simulators are small enough to fit in a police cruiser, or even on the vest of an officer, allowing law enforcement officers to drive to multiple locations, capturing from every mobile device in a given area—in some cases up to 10,000 phones at a time. These indiscriminate, dragnet searches include phones located in traditionally protected private spaces, such as homes and doctors' offices.

Law enforcement officers have used information from cell-site simulators to investigate major and minor crimes and civil offenses. Baltimore Police, for example, have used their devices for a wide variety of purposes, ranging from tracking a kidnapper to trying to locate a man who took his wife's phone during an argument (and later returned it to her). In one case, Annapolis Police used a cell-site simulator to investigate a robbery involving $56 worth of submarine sandwiches and chicken wings. In Detroit, U.S. Immigration and Customs Enforcement used a cell-site simulator to locate and arrest an undocumented immigrant. In California, the San Bernardino county sheriff's office used their cell-site simulator over 300 times in a little over a year.

Police may have deployed cell-site simulators at protests. The Miami-Dade Police Department apparently first purchased a cell-site simulator in 2003 to surveil protestors at a Free Trade of the Americas Agreement conference. And it is suspected that they have been used more recently than that during protests against police violence in 2020.

Cell-site simulators are used by the FBI, DEA, NSA, Secret Service, and ICE, as well as the U.S. Army, Navy, Marine Corps, and National Guard. U.S. Marshals and the FBI have attached cell-site simulators to airplanes to track suspects, gathering massive amounts of data about many innocent people in the process. The Texas Observer also uncovered airborne cell-site simulators in use by the Texas National Guard. In 2023 it was revealed

without following their own rules on deployment or getting a warrant.

A recent Congressional Oversight Committee report called on Congress to pass laws requiring a warrant before using cell-site simulators. Some states, such as California, already require a warrant, except in emergency situations.

Who Sells Cell-site Simulators

Harris Corporation is the most well known company providing cell-site simulators to law enforcement. Their Stingray product has become the catchphrase for these devices, but they have subsequently introduced other models, such as Hailstorm, ArrowHead, AmberJack, and KingFish. Harris has stopped selling cell-site simulator technology to local law enforcement agencies but still works with the federal government. Digital Receiver Technology, a division of Boeing, is also a common supplier of the technology, often referred to as "dirtboxes."

Other sellers of cell-site simulators include Keyw, Octastic, Tactical Support Equipment, Berkeley Varitronics, Cogynte, X-Surveillance, Atos, Rayzone, Martone Radio Technology, Septier Communication, PKI Electronic Intelligence, Datong (Seven Technologies Group), Ability Computers and Software Industries, Gamma Group, Rohde & Schwarz, Meganet Corporation. Manufacturers Septier and Gamma GSM both provide information on what the devices can capture. The Intercept published a secret, internal U.S. government catalogue of various cellphone surveillance devices, as well as an older cell-site simulator manual made available through a Freedom of Information Act request.

Threats Posed by Cell-Site Simulators

Cell-site simulators invade the privacy of everyone who happens to be in a given area, regardless of the fact that the vast majority have not been accused of committing a crime. These are general searches that violate the Fourth Amendment requirement that warrants "particularly" describe who or what is to be searched.

The use of cell-site simulators have been shrouded in government secrecy. Police have used cell-site simulators to track location data without a warrant, by deceptively obtaining "pen register" orders from courts without explaining the true nature of the surveillance. In Baltimore, a judge concluded that law enforcement had intentionally withheld the information from the defense, in violation of their legal disclosure

secret from not just the public but also the court system, withholding information from defense attorneys and judges—likely due in part to non-disclosure agreements with Harris Corporation. Prosecutors have accepted plea deals to hide their use of cell-site simulators and have even dropped cases rather than revealing information about their use of the technology. U.S. Marshalls have driven files hundreds of miles to thwart public records requests. Police have tried to keep information secret in Sarasota, Florida, Tacoma, Washington, Baltimore, Maryland, and St. Louis, Missouri.

To preserve this secrecy, the FBI told police officers to recreate evidence from the devices, according to a document obtained by the nonprofit investigative journalism outlet Oklahoma Watch.

Cell-site simulators often disrupt cell phone communications within as much as a 500-meter radius of the device, interrupting important communications and even emergency phone calls. Cell-site simulators have been shown to disproportionately affect low-income communities and communities of color. In Baltimore, the use of cell-site simulators disproportionately impacted African-American communities, according to a map included in an FCC complaint that overlaid where Baltimore Police were using stingrays over census data on the city's black population.

Cell-site simulators can also disrupt emergency calls, such as 911 in the US, making them not only a menace to privacy but to public safety as well.

Cell-site simulators rely on vulnerabilities in our communications system that the government should help fix rather than exploit.

EFF's Work on Cell-Site Simulators

For the reasons above, EFF opposes police use of cell site simulators. Insofar as law enforcement agencies are using cell-site simulators in criminal investigations, EFF argues that use should be limited in the following ways:

1. Law enforcement should obtain individualized warrants based on probable cause;
2. Cell-site simulators should only be used for serious, violent crimes;
3. Cell-site simulators should only be used for identifying location of a particular phone;

are not the targets of the investigation.

5. Companies making cell-site simulators must confirm that their technology does not disrupt calls to emergency services.

Litigation

We filed a Freedom of Information Act lawsuit to expose and shine light on the U.S. Marshals Service's use of cell-site simulators on planes.

Along with the ACLU and ACLU of Maryland, we filed an amicus brief in the first case in the country where a judge threw out evidence obtained as a result of using a cell-site simulator without a warrant.

We filed an amicus brief, along with the ACLU, pointing a court to facts indicating that the Milwaukee Police Department secretly used a cell-site simulator to locate a defendant through his cell phone without a warrant in U.S. vs. Damian Patrick. (The government then admitted to having used it.)

Legislation

We were original co-sponsors of the California Electronic Communications Privacy Act (CalECPA), along with the ACLU and the California Newspaper Publisher Association. This law requires California police to get a warrant before using a cell-site simulator. Any evidence obtained from a cell-site simulator without a warrant is inadmissible in court.

EFF supported S.B. 741, which requires transparency measures regarding the use of cell-site simulators. We collected many of these policies.

Further Research

We have written a report on the technical means possibly used by cell-site simulators called "Gotta Catch 'em All", and we have developed a proof of concept technical means of detecting cell-site simulators called Crocodile Hunter.

EFF Cases

U.S. v. Damian Patrick

EFF v. U.S. Department of Justice

Suggested Additional Reading

Stingray Tracking Devices: Who's Got Them? (ACLU)

Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy (Harvard Journal of Law and Technology)

Examining Law Enforcement Use of Cell Phone Tracking Devices (House Oversight Committee)

The Relentless "Eye" Local Surveillance: Its Impact on Human Rights and Its Relationship to National and International Surveillance (Center for Media Justice and others)

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (U.S. Department of Justice)

Long-Secret Stingray Manuals Detail How Police Can Spy on Phones (The Intercept)

A Secret Catalogue of Government Gear for Spying on Your Cellphone (The Intercept)

Cops Turn to Canadian Phone-Tracking Firm After Infamous 'Stingrays' Become 'Obsolete' (Gizmodo)

Most recently updated March 29th, 2023