LOCATION DATA – REAL TIME TRACKING

Although much of the location data is obtained via historical data derived from a device owner's past usage, there are ways to track a device in real time.

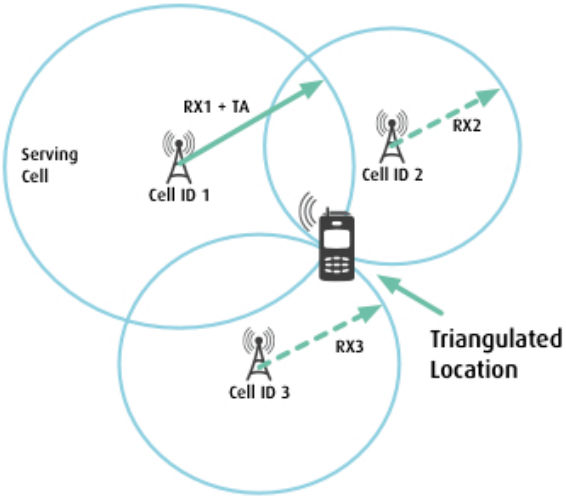
Historical vs. Real Time

Historical location data is derived from records or usage that had occurred in the past, such as historical cell site locations or GPS location data recovered from the device. Real-time location tracking is used to locate the current whereabouts of a device.

Examples of Real-Time Tracking are:

1. Ping (Triangulation)
2. Mobile signal Tracking
3. Malware

CELL PING – TRIANGULATION



The Federal Communications Commission has mandated that the E911 System must automatically identify to emergency dispatchers the location of the device to be accurate to within 100 meters. Using this system an operator can "ping" a device and calculate where a particular subscriber's phone is located whenever the phone is powered on and registered with the network. The ability to do this results from the way the mobile network is built, and is commonly called triangulation. A cell phones signal will often be received simultaneously by more than one cell site when operating in areas with a high concentration of cell sites and overlaps in coverage. When this occurs, a mathematical process called triangulation may determine the phone's location if either: (1) three points receiving the signal are known; or (2) two points receiving the signal are known, along with the direction in which the cell site received the signal.

Accuracy

One way the operator can do this is to observe the signal strength that different towers observe from a particular subscriber's mobile phone, and then calculate where that phone must be located in order to account for these observations. The accuracy with which the operator can figure out a subscriber's location varies depending on many factors, including the technology the operator uses and how many cell sites they have in an area. Very often, it is accurate to about the level of a city block, but in some systems it can be more accurate.

A ping will work as long as the device is on and transmitting signals to an operator's network.

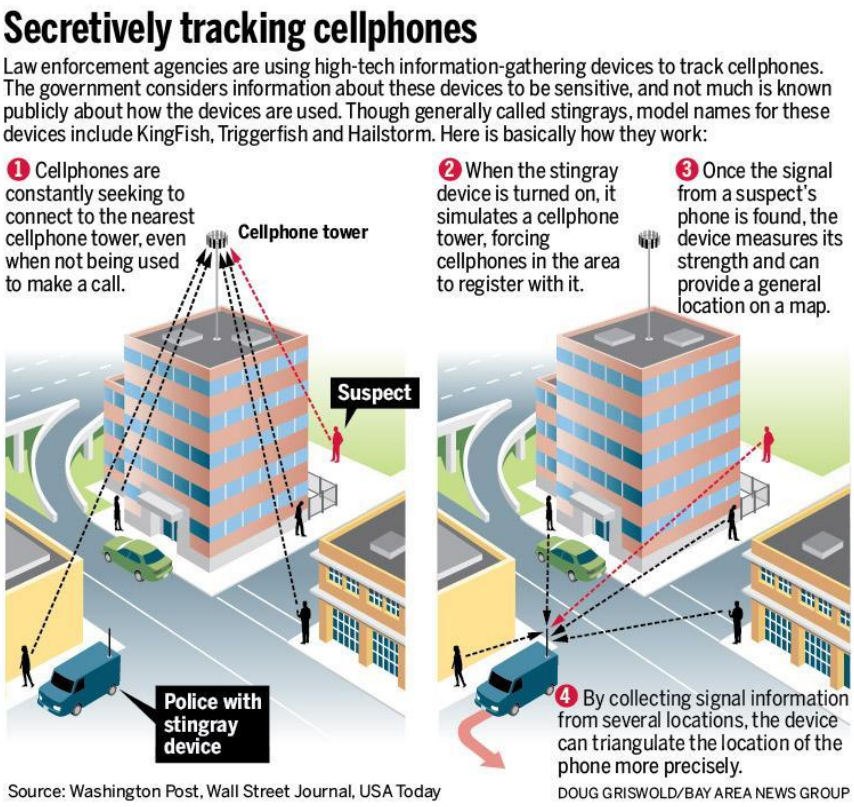
MOBILE SIGNAL TRACKING

Federal and state law enforcement entities across the country are using a powerful cell phone surveillance tool commonly referred to as a "StingRay." These devices are capable of locating a cell phone with extraordinary precision, but to do so they operate in dragnet fashion, scooping up information from a target device, as well as other wireless devices in the vicinity. In addition, these devices can be configured to capture the content of voice and data communications.

StingRay technology is sold by the Harris Corporation. Other Harris cell site simulator models include the TriggerFish, KingFish, and Hailstorm. The more generic term for the technology is IMSI catcher, in reference to the "international mobile subscriber identity" a unique identifier of a wireless device.

The equipment consists of an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. It can be carried by hand or mounted on vehicles or even drones. If the government knows a suspect's location, it can use the device to determine the unique numeric identifier associated with that cell phone

The IMSI catcher needs to be taken to a particular location in order to find or monitor devices at that location.



Constitutional Concerns

First, use of an IMSI catcher triggers Fourth Amendment scrutiny because it constitutes both a search and a seizure within the meaning of the Fourth Amendment.

Second, there is a strong argument that IMSI catchers can never be used consistent with the Fourth Amendment because they engage in the electronic equivalent of a "general search."

Third, law enforcement must at least obtain a warrant; a statutory order does not suffice.

Fourth, even if law enforcement obtained a warrant, it is likely invalid because the data obtained through stingrays may not be disclosed to the defense, because the federal government contends that stingrays are a secret national security technology, and (2) that the orders authorizing the use of stingrays may be sealed, in some cases effectively permanently.

MALWARE

Phones can get viruses and other kinds of malware (malicious software), either because the user was tricked into installing malicious software, or because someone was able to hack into the device using a security flaw in the existing device software. As with other kinds of computing device, the malicious software can then spy on the device's user.

For example, malicious software on a mobile phone could read private data on the device (like stored text messages or photos). It could also activate the device's sensors (such as microphone, camera, GPS) to find where the phone is or to monitor the environment, even turning the phone into a bug.

A further concern is that malicious software could theoretically make a phone pretend to power off, while secretly remaining turned on (and showing a black screen, so that the user wrongly believes that the phone is turned off). This concern has led to some people physically removing the batteries from their devices when having very sensitive conversations.

Malware can read private data and activate the device's sensors.

Precautions based on powering off phones could be noticed by a mobile operator; for example, if ten people all travel to the same building and then all switch off their phones at the same time, the mobile operator, or somebody examining its records, might conclude that those people were all at the same meeting and that the participants regarded it as sensitive. This would be harder to detect if the participants had instead left their phones at home or at the office.

DIGITAL EVIDENCE TOOLBOX

For more topics and information on digital evidence, see our toolbox at:
http://www.irisinvestigations.com/wordpress/iris-digital-evidence-toolbox/

For more information on location evidence, call now and speak with a certified expert. I.R.I.S. LLC is available 24 hours in emergency cases.

cellebrite delivering mobile expertise

WE'RE CERTIFIED.