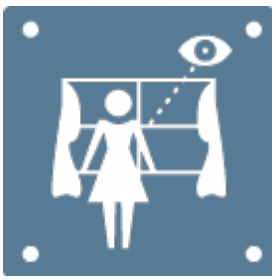
ACLU
AMERICAN CIVIL LIBERTIES UNION of OREGON

Privacy and Surveillance



Why should we care about privacy and surveillance? Some people downplay its importance, saying, "I don't care about privacy. We've already lost it, and I have nothing to hide." Yet, such a statement is essentially an antisocial perspective, because privacy is important to many other people in our communities. When we say we don't care about privacy, we are discounting and disregarding its importance to all of the people around us.

It is also worth challenging the statement "I have nothing to hide." The truth is that all of us have things we hide. Those things aren't necessarily bad things. Instead, they are simply things we don't want to share, based on our own personal comfort level and the matter at hand. So yes, privacy is important to many of us, and feeling like our privacy has been invaded can make us feel violated and vulnerable. But that is not the only reason it is important…

The right to privacy is intertwined with other individual rights…

Free Speech

We should be able to express our minds freely without fear that the government will monitor us, keep a permanent record of our activities, and use that record to harass or coerce us. Recent studies have shown that people are much less likely to express controversial or unpopular opinions when they think government is watching. Interestingly, the people less likely to express themselves when they know they are being watched are the very people who state that they don't care about privacy because they have nothing to hide.

"The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."

U.S. Supreme Court, United States v. U.S. District Court, 407 U.S. 297, 314 (1972)

Free Association

We should be free to live our lives without the fear that our activities and relationships are being monitored. Many people are members of political, religious, business, labor, fraternal, or other organizations. If surveillance of lawful meetings of those organizations is commonplace, some people may choose to avoid these activities altogether, particularly when they are unpopular or disliked.

Profiling and Equal Protection

The government's gaze doesn't always fall on everyone equally, and at times it is targeted at particular groups based on religion, unpopular political views, ethnicity, etc. Historically, surveillance has been used in the United States to disproportionately target communities of color and low income communities, which has contributed to the over-criminalization of communities of color and diminished community trust in law enforcement.

Misuse and Abuse

Once it has been collected, our private information can also be abused. Unfortunately, surveillance technology has being abused to stalk or harass partners, ex-partners, friends, and rivals, and to retaliate against individuals who have reported misconduct. And of course, once data is collected, there is always risk of that data getting into the wrong hands.

This is just a short description of some of the ways that privacy intertwines with other rights and the dangers of unrestrained government surveillance. If you are interested in learning more, please visit https://www.theyarewatching.org/. At this ACLU website, you will find a more in-depth discussion, along with more specific examples of what can go wrong when privacy is not adequately protected.

Stingrays

AKA: 'Cell Site Simulator,' 'IMSI Catcher,' 'Gossamer,' 'Kingfish,' 'AmberJack,' 'Hailstorm'

"Stingrays" can track the location of wireless phones, tablets, and computers that utilize cell phone networks. Some can intercept calls and text messages, and some are suspected to be capable of delivering malicious spyware to personal devices. Law enforcement agencies have given the public very little information about how and when they are being used and have even withheld information from judges and criminal defense attorneys.

WHAT IS IT USED FOR?

Cell site simulators are often called "Stingrays," after the name given to the most popular model on the market. These tools track the locations of wireless mobile devices such as cell phones, mobile tablets, and wireless broadband cards. Police use some models to intercept calls, text messages, or emails sent between different devices. If the government knows which phone to look for, a Stingray can pinpoint its location. However, it collects location data indiscriminately from all the nearby devices that are associated with the particular network the Stingray is impersonating. These devices transmit signals into all nearby homes, cars, bags, and pockets, looking for every device in the area that connects to that network. Police can use it to find out every person in a particular place at a given time, raising serious privacy concerns.

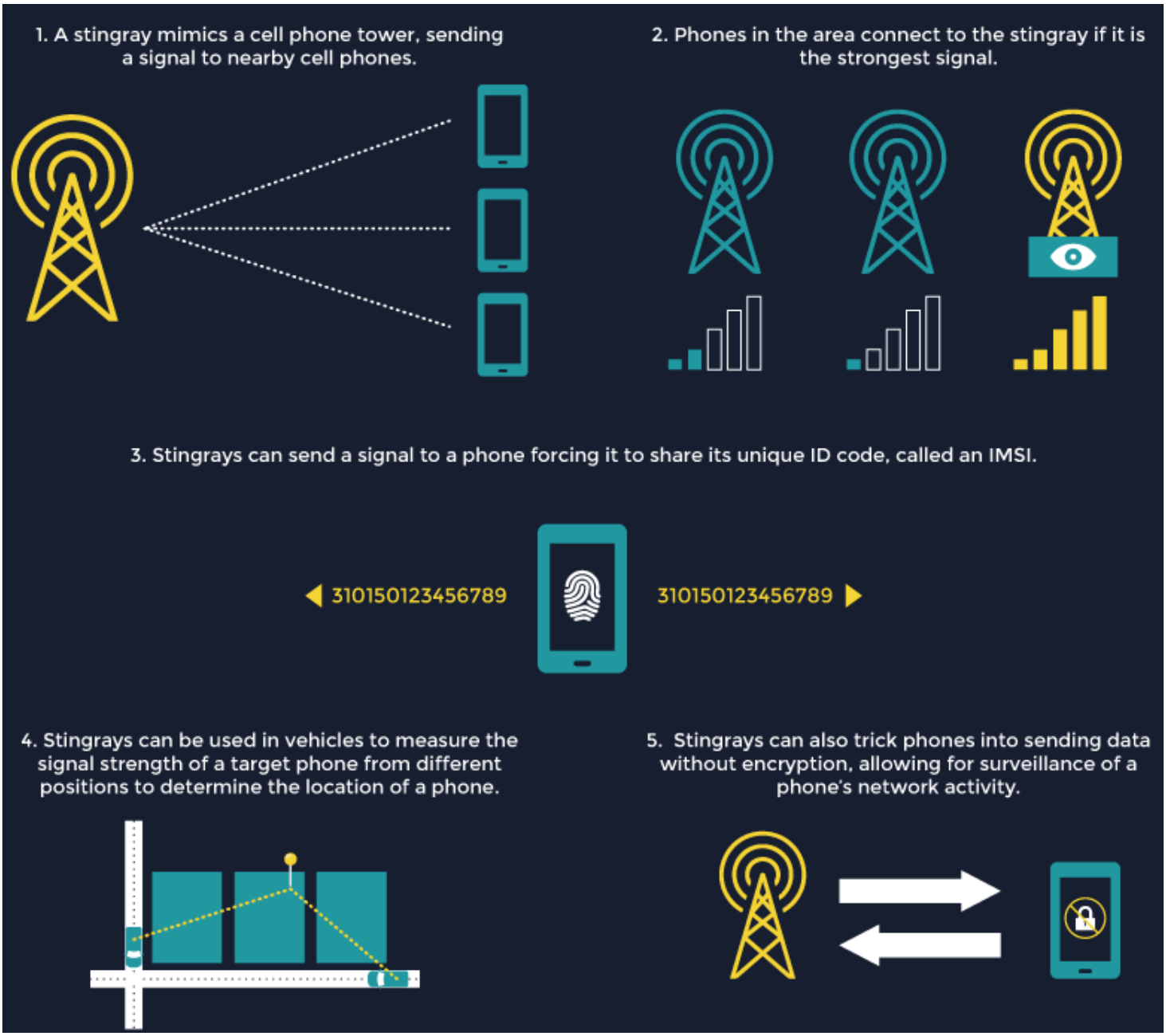
HOW IT WORKS: Stingrays imitate cell towers in order to locate wireless devices.

Several times a minute, your cell phone sends a signal with a unique identifier that connects it to a nearby cell tower. Every mobile network user has a unique International Mobile Subscriber Identity (IMSI), a 12- to 15-digit number. Your cell phone carries this number in its SIM card.

The Stingray deceives cell phones by imitating a cell tower. It entices all mobile phones and wireless broadband cards within range of the device to connect. Once these connections are established, they enable the operator to collect all sorts of sensitive information.

Usually, the Stingray collects location data. When targeting a particular mobile user, police use the Stingray to measure the signal strength of the user's phone to estimate the distance between the two devices. After doing this from several different locations, the Stingray uses the data to triangulate the precise location of the target device. However, the device connects to all phones in range. That means that is can identify and track the movements of all mobile users within a particular area at a particular time. Harris Corp. boasts that one advanced model, the "Triggerfish," tracks the IMSIs of up to 60,000 phones at a time.

Even more troubling, later-generation models can intercept and extract usage information from any device it connects to. Police using this type of Stingray can read your Internet search history, text messages, call records, and even listen to your phone calls. In some cases, these devices may even be capable of delivering malicious software, or spyware, to personal devices.



CIVIL LIBERTIES CONCERNS

Stingrays are indiscriminate – they enable law enforcement to determine the location of not only individuals suspected of criminal activity, but potentially tens of thousands of people at once. Ensuring accountability for law enforcement use of this technology is challenging. Under pressure from Harris Corporation, the most popular manufacturer, many federal agencies and local police departments have refused to provide technical details about the design and function of Stingrays. Some have even signed non-disclosure agreements barring them from confirming or denying that they have bought or leased them. Thus, these devices have been used in secret and have collected information from large numbers of law-abiding people.

HOW PREVALENT IS IT?

Secrecy surrounds these devices. However, public records confirm that federal agencies including the FBI, DEA, and IRS have acquired and used them in criminal investigations. In fact, Justice Department documents have revealed that federal agents sometimes neglect to inform federal judges that they intend to use Stingrays when seeking authorization to recover phone location data. Additionally, privacy advocates have confirmed Stingray use by local police in Arizona, California, and Florida. The ACLU found that the Tallahassee Police Department used its Stingray over 200 times without ever asking for a warrant from a judge.

EXAMPLE OF USE

Stingray Nabs Alleged Wire Fraudster – And Dozens Of His Innocent Neighbors

Location: Santa Clara, CA

The Stingray played a role in the capture of the alleged leader of a tax fraud scheme. The FBI narrowed the location of the unknown suspect's wireless air card to an area of Santa Clara, CA, about 1/4 of a square mile in size. Agents used the Stingray to scan this broad residential area, matching the air card's unique identifying number to inside the suspect's apartment. In doing so, they also captured the location data of phones and computers belonging to numerous innocent people living in the same apartment complex and shopping at a nearby supermarket. In seeking a court order for the operation, the FBI failed to disclose its intent to use the Stingray to pinpoint the suspect's location. Nor did it provide the court a description of the device or note the search would reveal the private information of potentially hundreds of innocent people.

RECOMMENDATIONS

When government agencies consider acquiring and using surveillance systems, communities and their elected officials must both weigh the benefits against the costs to civil liberties and carefully craft policies and procedures that help to limit the negative effects that surveillance will have on fundamental rights.