JANUARY 2, 2015

eff.org

Stingrays Go Mainstream: 2014 in Review

We've long worried about the government's use of IMSI catchers or cell site simulators. Commonly known as a "Stingray" after a specific device manufactured by the Harris Corporation, IMSI catchers masquerade as a legitimate cell phone tower, tricking phones nearby to connect to the device in order to track a phone's location in real time. We're not just worried about how invasive these devices can be but also that the government has been less than forthright with judges about how and when they use IMSI catchers.

This year the public learned just how desperately law enforcement wanted to keep details about Stingrays secret thanks to a flurry of public records act requests by news organizations across the country. The results are shocking.

The public learned that Harris requires police departments sign a non-disclosure agreement promising not to reference Stingrays. Federal agencies like the US Department of Justice and the US Marshals Service have instructed local cities and police to keep details of Stingray surveillance secret, with the

Marshals physically intervening in one instance to prevent information from becoming public. There have been repeated instances of police agencies across the country hiding their use of IMSI catchers from the judges entrusted to provide police oversight:

- In Sarasota, Florida internal police emails revealed officers concealed their use of Stingrays from judges, having one officer withdraw a warrant affidavit that mentioned the use of an IMSI catcher, and describing a policy of referring to Stingrays as a "source" in official documents.
- Judges in Tacoma, Washington signed more than 170 orders unknowingly authorizing Stingray use from 2009 to 2014 because police officers did not disclose the orders would be used to operate an IMSI catcher. Judges first learned they were approving IMSI catchers from local newspaper reporting.
- In a robbery case in Baltimore, Maryland, prosecutors abandoned their use of Stingray evidence after a judge threatened to hold a police officer in contempt for refusing to testify about the device.

It's not just local police. The *Wall Street Journal* reported on a secret US Marshals surveillance program that attaches IMSI catchers called "DRTboxes" to airplanes to track suspects, gathering data about scores of innocent people in the process. The report prompted a letter from US senators to the Justice Department and the Department of Homeland Security demanding more information.

Continuing last year's trend, state courts and legislators continued to push back. In Tacoma, judges now require police specifically note they plan to use an IMSI catcher and promise not to store data collected from people who are not investigation targets. The Florida and Massachusetts state Supreme Courts ruled warrants were necessary for real time cell phone tracking. Eight states —Illinois, Indiana, Maryland, Minnesota, Tennessee, Utah, Virginia and Wisconsin—passed laws specifically requiring police use a warrant to track a cell phone in real time.

As we continue to learn about Stingrays in 2015, we hope more courts and legislatures confront these dangerous tools and work to enact privacy safeguards to protect the data of innocent people who have the bad fortune of being nearby when the police use one.

This article is part of our *Year In Review* series; read other articles about the fight for digital rights in 2014. Like what you're reading? EFF is a member-supported nonprofit, powered by donations from individuals around the world.

Join us today and defend free speech, privacy, and innovation.

** A pervious version of this post incorrectly noted that Colorado passed a statute in 2014 to require police use a warrant to track a phone in real time. The Colorado statute also allows police to use a subpoena or court order to track a phone in real time.*

TAGS:

CELL-SITE SIMULATORS STINGRAYS

STREET LEVEL SURVEILLANCE

JOIN EFF LISTS

Discover more.

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

SUBMIT

RELATED UPDATES

ELECTRONIC FRONTIER FOUNDATION

DEEPLINKS BLOG BY KATITZA RODRIGUEZ | JULY 20, 2023

First Draft of UN Cybercrime Convention Drops Troubling Provisions, But Dangerous And Open-Ended Cross Border Surveillance Powers Are Still on the Table

DEEPLINKS BLOG BY INDIA MCKINNEY, ANDREW CROCKER | JULY 20, 2023

Amended Cooper Davis Act Is a Direct Threat to Encryption

DEEPLINKS BLOG BY JASON KELLEY | JULY 18, 2023

You Can Help Stop These Bad Internet Bills

Brazil's Platform Regulation Debate: Robust Checks, Balances and Due

DEEPLINKS BLOG BY VERIDIANA ALIMONTI, AGNERIS SAMPIERI | JULY 7, 2023

Process Safeguards for Exceptional Measures in Crisis Situations

DEEPLINKS BLOG BY VERIDIANA ALIMONTI, AGNERIS SAMPIERI | JULY 7, 2023

Brazil's Platform Regulation Debate: Proper Independent and Participative Oversight Structure

DEEPLINKS BLOG BY VERIDIANA ALIMONTI, AGNERIS SAMPIERI | JULY 7, 2023

Brazil's Platform Regulation Debate: Clear Safeguards Against Incrementing Surveillance and Related Security Risks

Brazil's Platform Regulation Debate: Review Problematic Immunity for Public Officials

DEEPLINKS BLOG BY VERIDIANA ALIMONTI, AGNERIS SAMPIERI | JULY 7, 2023

DEEPLINKS BLOG BY VERIDIANA ALIMONTI, DALY BARNETT, AGNERIS SAMPIERI | JULY 7, 2023

Settled Human Rights Standards as Building Blocks for Platform Accountability and Regulation: A Contribution to the Brazilian Debate

DEEPLINKS BLOG BY VERIDIANA ALIMONTI, AGNERIS SAMPIERI | JULY 7, 2023

Brazil's Platform Regulation Debate: Concerning Duty of Care Obligations

Brazil's Platform Regulation Debate: Repel Rules and Interpretations That Can Lead to Content Monitoring Obligations

DEEPLINKS BLOG BY VERIDIANA ALIMONTI, DALY BARNETT, AGNERIS SAMPIERI | JULY 7, 2023