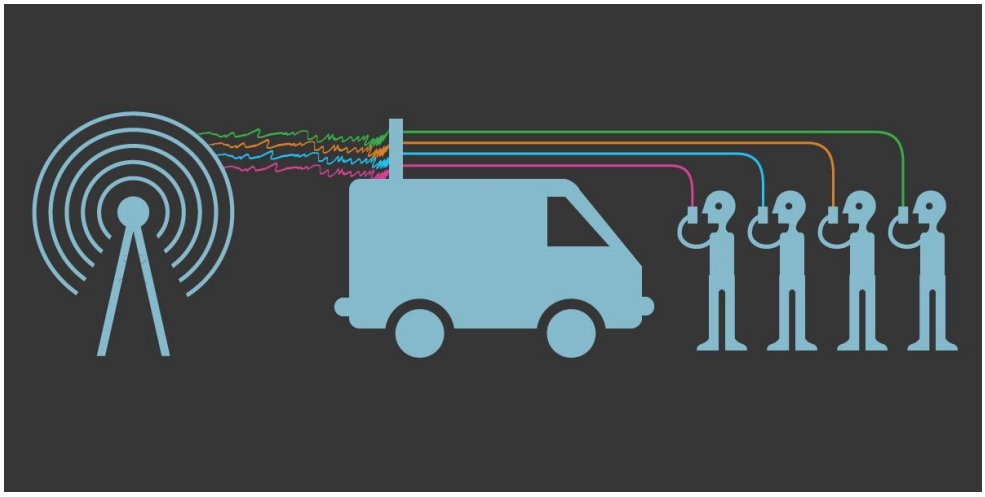
ELECTRONIC FRONTIER FOUNDATION

Cell-Site Simulators Resources

Extra Materials for Criminal Defense Attorneys



EFF One-Pager
Revised 4.10.18

Learn more:
eff.org/
CSSFA

Support our work on Cell Site Simulators:
eff.org/donate

EFF Briefs

EFF Litigation Briefs

- *EFF v. County of San Bernardino*, (Case No. CIVDS 1827591, 2018) in the superior court of California, County of San Bernardino, our writ of mandate urges the court to enforce the California Public Records Act by disclosing the case numbers for 6 search warrants and supporting affidavits that authorized the use of cell site simulators in San Bernardino county in 2017.

EFF Amicus Briefs

- *U.S. v. Daniel Rigmaiden*, 2013 WL 1932800 (D. Ariz. 2013) in the United States District Court of Arizona, our amicus brief urged the court to exclude evidence collected by warrantless CSS use.
- *State of Maryland v. Kerron Andrews*, 227 Md.App.350 (Md. Ct. Spec. App. 2015) in the Court of Special Appeals in Maryland, our amicus brief explained why warrantless CSS use violates the Fourth Amendment.
- *U.S. v. Damian L. Patrick*, 842 F.3d 540 (7th Cir. 2016) in the United States Court of Appeals for the Seventh Circuit, our amicus brief explained why the Fourth Amendment protects location privacy.

    - January 25, 2016 EFF press release— https://www.eff.org/press/releases/eff-aclu-court-accessing-cell-phone-location-records-without-warrant-violates
    - March 23, 2016, Department of Justice letter admitting that the Milwaukee Police Department used a cell-site simulator— https://www.eff.org/document/us-v-patrick-government-letter-admitting-stingray-use
- *Prince Jones v. U.S.*, Case No. 15-CF-322 (DC Cir. 2017) in the District of Columbia Court of Appeals, February 24, 2016, our amicus brief explained why CSS use violates the Fourth Amendment, and should at the very least require a warrant with minimization rules.

EFF Blogs and Press Releases

- US Marshals Airborne IMSI Catchers
- Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About - Oct. 22, 2012
- As Secretive "Stingray" Surveillance Tool Becomes More Pervasive, Questions Over Its Illegality Increase - Feb. 12, 2013
- When a Secretive Stingray Cell Phone Tracking "Warrant" Isn't a Warrant - March 28, 2013
- Justice Department Must Provide Records of Aircraft-mounted Cell Tower Simulators — Feb. 10, 2015
- DOJ Reverses Course and Requires Warrants for Stingrays! — Sept. 3, 2015
- New FOIA Documents Confirm FBI Used Dirtboxes on Planes Without Any Policies or Legal Guidance — March 9, 2016
- Here are 79 California Surveillance Tech Policies. But Where Are the Other 90? — April 11, 2016,
- Illinois Sets New Limits On Cell-Site Simulators — Aug. 11, 2016
- Civil Rights Coalition files FCC Complaint Against Baltimore Police Department for Illegally Using Stingrays to Disrupt Cellular Communications— Aug. 17, 2016
    - Baltimore FCC complaint re: CSS use
- FCC Helped Create the Stingray Problem, Now it Needs to Fix It — Oct. 6, 2016
- Congressional Oversight Committee Wants Warrants to Rein in Police Abuse of Cell-Site Simulators — February 22, 2017
- No Hunting Undocumented Immigrants with Stingrays — May 19, 2017
- EFF Sues San Bernardino County Sheriff's Department to Obtain Records About Use of Privacy Invasive Cell-Site Simulator — October 23, 2018

EFF Freedom of Information Act Work

- EFF filed a complaint against the San Bernardino Sheriffs' Department for failing to produce the case numbers for 6 search warrants that authorized CSS use in 2017.
- Following a 2014 Wall Street Journal report that revealed that U.S. Marshals attached cell-site simulators to small aircraft for a U.S. spy program, EFF sued the Department of Justice to learn more. EFF wrote a blog about the documents we received in 2016. Here are responses to our Freedom of Information Act request.
    - "DRTbox" FOIA documents from the Office of the General Counsel for the FBI, CELL 466-502

- "DRTbox" FOIA documents from the Office of the General Counsel for the FBI, CELL 1145-1319
- "DRTbox" FOIA documents from the Office of the General Counsel for the FBI, CELL 5-29
- "DRTbox" FOIA documents from the FBI, CELL 175-223
- "DRTbox" FOIA documents from the FBI, CELL 224-278

Academic Articles and Research

- **Legal**
  - "Stingray: A New Frontier in Police Surveillance" by Adam Bates of the CATO Institute"
  - "The Stingray is Exactly Why the Fourth Amendment was Written" by Olivia Donaldson
  - "The Latest 4th Amendment Privacy Conundrum: Stingrays" by Max Bulinski, University of Michigan Journal of Law
  - "TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions" by Brian L. Owsley

- **Technical**
  - "Easy 4G/LTE IMSI Catchers for Non-Programmers" by Stig F. Mjølsnes and Ruxandra F. Olimid
  - "White-Stingray: Evaluating IMSI Catchers Detection Applications" by Ravishankar Borgaonkar, Andrew Martin, Shinjo Park, Altaf Shaik, and Jean-Pierre Seifert
  - "LTE security, protocol exploits and location tracking experimentation with low-cost software radio" by Roger Piqueras Jover
  - "SeaGlass: Enabling City-Wide IMSI-Catcher Detection" by Peter Ney, Ian Smith, Gabriel Cadamuro, and Tadayoshi Kohno
  - "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada" by Tamir Israel and Christopher Parsons
  - "IMSI Catchers and Mobile Security" by Joseph Ooi
  - "Defeating IMSI Catchers" by Fabian van den Broek, Roel Verdult, Joeri de Ruiter
  - "Rapidly Mixing Gibbs Sampling for a Class of Factor Graphs Using Hierarchy Width" by Christopher De Sa, Ce Zhang, Kunle Olukotun, and Christopher Ré
  - "Detecting IMSI-Catcher Using Soft Computing" Thanh van Do, Hai Thanh Nguyen, Nikolov Momchil, Van Thuan Do
  - "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers" by Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, Edgar Weippl
  - "Location Leaks on the GSM Air Interface" by Denis Foo Kune, John Koelndorfer, Nicholas Hopper, and Yongdae Kim
  - Technical Videos
  - "LTE & IMSI Catcher Myths" published by Black Hat
  - "Camp++ 0x7e0 // FOS LTE IMSI catcher by Domi" published by Budapest Hackerspace
  - "DEF CON 23 - Ian Kline - LTE Recon and Tracking with RTLSDR," published by DEFCON Conference
  - "Understanding IMSI Privacy" published by Black Hat

- "DEF CON 18 - Chris Paget - Practical Cellphone Spying" published by DEFCON Conference
- "BlackHat 2011 - Femtocells: a Poisonous Needle in the Operator's Hay Stack" published by blackhattish

Legislation

- **Federal**
  - Electronic Communications Privacy Act, 18 U.S.C. § 2510, et. seq.
  - Federal Wiretap Act, 18 U.S.C. § 2701, et. seq.
  - Pen Registers and Trap and Trace Devices Act, 18 U.S.C. § 3121, et. seq.
  - Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801, et. seq.
  - Federal DOJ Policy: Though not legislation, the Department of Justice announced a policy change in 2015 that required federal agents to obtain a probable cause warrant before using cell-site simulators in investigations. The Department of Homeland Security, its components, and the Internal Revenue Service adopted similar policies the same year.
- **State**
  - California Email Communications Privacy Act, California Penal Code § 1546, et. seq.
    - SCA & CalECPA Prezi presentation by EFF staff attorneys Stephanie Lacambra and Lee Tien
    - California Peace Officers' Association CalECPA factsheet
    - Santa Clara CCOPS, EFF blog "A California County Breaks New Ground for Surveillance Transparency"
    - Proposed City of Oakland ordinance
  - California Cellular Communications Interception statute, California Government Code § 53166
  - Illinois Citizen Privacy Protection Act
  - Florida statute, Title 33, Chapter 501, Consumer Protection, 501.171 Security of Confidential personal information
  - Illinois Citizen Privacy Protection Act
  - Florida statute, Title 33, Chapter 501, Consumer Protection, 501.171 Security of Confidential personal information

Known Manufacturers

- Pen-Link Ltd., of Lincoln, Nebraska.
- Harris Corp., of Melbourne, Florida.
  - Makers of the Stingray, KingFish, AmberJack, Hailstorm, Harpoon, etc.
- Telesoft Technologies, of Blandford Forum, United Kingdom.
  - Maker of the HINTON Abis Probe device.
- Rayzone Group, of Tel Aviv, Israel.
  - Maker of the Piranha device.
- PKI Electronic Intelligence GmbH, of Lütjensee, Schleswig-Holstein, Germany
  - Maker of several digital and communications surveillance devices.
- GammaGroup
  - Maker of FinFisher, a remote spyware tool that has been sold to autocratic governments.