Cell Site Simulators ("CSSs")

Also Known as:

- IMSI catchers
- digital analyzers
- Brand names include:
  - Stingrays
  - Hailstorm
  - Triggerfish
  - Kingfish
  - Arrow-Head
  - Amberjack
  - Harpoon
  - WITT (FBI’s “Wireless Intercept Tracking Team”) devices
Cell Site Simulators ("CSSs")

What they are & how they work:

- CSSs are devices that law enforcement uses to locate and identify suspects.

- CSSs masquerade as legitimate cell phone towers, tricking all phones nearby into connecting to the device instead of a legitimate cell phone tower.
Cell Site Simulators ("CSSs")

What they are & how they work:

- CSSs log the IMSI numbers (a unique identifying number) of all mobile phones within range, including non-target data.
- CSSs can pinpoint a phone’s location in real time with much greater precision than CSLI from the phone company.
- Helpful video from Vocativ: https://eff.org/CSSvideo
How they work:
Cell Site Simulators ("CSSs")

In the Wild – What to Look for

Cell Towers

SECRET SPY PROGRAM TARGETS U.S. CELLPHONES

HOW IT WORKS:
1. Planes equipped with "dirtbox" devices pick up cellphone signals to track criminal suspects
2. Track and locate suspect phones; "lets go" of non-suspect phones
3. Find the strongest signals to help locate a suspect
4. Use data collected to catch suspect

Unconfirmed reports of body-worn CSS
Who Can Track Your Phone?

Police departments known to have purchased stingrays

- City police
- Local police
- County police
- State police

City police: (17 states, 32 cities)
- CA 7
- FL 5
- NC 5
- MD 4
- DC 2
- IL 2
- MO 2
- NV 2
- TX 2
- ID 1
- IN 1
- MA 1
- TN 1
- VA 1
- WA 1

Local police: (4 states, 9 cities)
- AZ 6
- CA 4
- AK 1
- AL 1

County police: (8 states, 17 counties)
- CA 13
- MD 6
- GA 2
- MN 2
- NY 2
- CO 1
- FL 1
- VA 1

State police: (17 states)
- CA 2
- DE 3
- FL 3
- IL 2
- IN 2
- LA 2
- MD 3
- MI 4
- MN 2
- NY 3
- NC 3
- OK 2
- PA 3
- TN 2
- TX 2
- VA 3
- WI 2
<table>
<thead>
<tr>
<th>City police</th>
<th>Local police:</th>
<th>County police:</th>
<th>State police:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(17 states, 32 cities)</td>
<td>(4 states, 9 cities)</td>
<td>(8 states, 17 counties)</td>
<td>(17 states)</td>
</tr>
<tr>
<td>CA 7</td>
<td>TX 2</td>
<td>CA 13</td>
<td>CA 2</td>
</tr>
<tr>
<td>FL 5</td>
<td>ID 1</td>
<td>MD 6</td>
<td>NY 3</td>
</tr>
<tr>
<td>NC 5</td>
<td>IN 1</td>
<td>GA 2</td>
<td>DE 3</td>
</tr>
<tr>
<td>MD 4</td>
<td>MA 1</td>
<td>MN 2</td>
<td>FL 3</td>
</tr>
<tr>
<td>DC 2</td>
<td>TN 1</td>
<td>NY 2</td>
<td>OK 2</td>
</tr>
<tr>
<td>IL 2</td>
<td>VA 1</td>
<td>CO 1</td>
<td>IL 2</td>
</tr>
<tr>
<td>MO 2</td>
<td>WA 1</td>
<td>FL 1</td>
<td>IN 2</td>
</tr>
<tr>
<td>NV 2</td>
<td>WI 1</td>
<td>VA 1</td>
<td>TN 2</td>
</tr>
<tr>
<td>NY 2</td>
<td></td>
<td></td>
<td>LA 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TX 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MD 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VA 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MI 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WI 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MN 3</td>
</tr>
</tbody>
</table>
Cell Site Simulators ("CSSs")

What can CSSs do?

- Pinpoint location within a few meters.
- Capture metadata like phone numbers dialed or received, identity of sender or receiver, or date, time and frequency of communications.
- May be configured to capture some content such as texts, calls, and unencrypted communications.
Cell Site Simulators ("CSSs")

How do I protect myself and my clients?

• At this point, there is no way for a phone to be configured to avoid sharing its unique identifying number with a CSS.
• It is also very difficult to tell from the cell phone itself whether its information has been compromised by a CSS, and there is no notification that encryption on the phone has been subverted or is no longer operating.
Cell Site Simulators ("CSSs")

How do I protect myself and my clients?

- End-to-end encrypted apps should still provide some protection.
- Use Full Disk Encryption
- Log out of apps and put the cellphone in airplane mode or turn off when it’s not in use.
Cell Site Simulators ("CSSs")

How do I know if cops used a CSS in my case?

- Be on the lookout for search warrants referring to a “confidential informant” used to identify a suspect’s location.
- Lookout for any CSS device brand names.
- Look for language that tracks the DOJ’s model CSS warrant application, which uses terms like: “target cell phone”, “pen register” and “trap and trace.”
- Review the DOJ’s CSS policy.
How do I challenge CSS evidence?

- File a **motion to compel discovery** on the CSS tech specs – many LEAs will dismiss a case rather than reveal how it works.
- File a MTS – most CSS use was without a warrant prior to the Sept 2015 change in DOJ/DHS policy: [eff.org/CSSDOJ](http://eff.org/CSSDOJ)
- Review the scathing House Oversight Committee report: [eff.org/CSSHOGHR](http://eff.org/CSSHOGHR)
- Review the leading **CSS cases**
Cell Site Simulator Cases

- **SCOTUS: Carpenter v. U.S.,** 585 U.S. __, 138 S. Ct. 2206 (2018): Held seizure of 7 days or more of CSLI is a search requiring PC SW; TPD does not defeat REP in CSLI. [EFF SCOTUS Amicus](https://www.eff.org/)

- **U.S. v. Damian Patrick,** 842 F.3d 540 (7th Cir. 2016): Rejected a motion to suppress argument that cell-site simulator use required a warrant. Rehearing *en banc* denied. [eff.org/CSSPatrick](https://www.eff.org/)
Cell Site Simulator Cases

Cell Site Simulator Cases


Where do I learn more?

- eff.org/defense/CSS
- eff.org/CSSFAQ
- eff.org/CSSACLU – guide for Criminal Defense Attys
- eff.org/CSSmanuals – from Intercept article
- eff.org/CSSBaltimore – racially biased CSS use
- eff.org/CSSFCC – FCC complaint filed in Baltimore, PA, against cop use of CSSs
Stephanie Lacambra
Criminal Defense
Staff Attorney
415-436-9333 x130
stephanie@eff.org