*“…40% of Americans own a cell phone — So they can hear everythin' that you say when you ain't home I guess Michael Jackson was right — "You Are Not Alone” — Rock your hardhat, Black, 'cause you in the Terrordome”*

*-Mos Def*
*“Mathematics” - 1999*

# $whoami

# $whoami

## Ki Rodriguez

- @dreadloc__

- Appsec Analyst - Security hobbyist
- High-tech-low-life

$loading..


LEGAL
EAGLE

Accessing a system that you do not own without permission may result in you being prosecuted under the Computer Fraud and Abuse act


ELECTRONIC
FRONTIER
FOUNDATION


Will Greenberg
*Senior Staff Technologist*

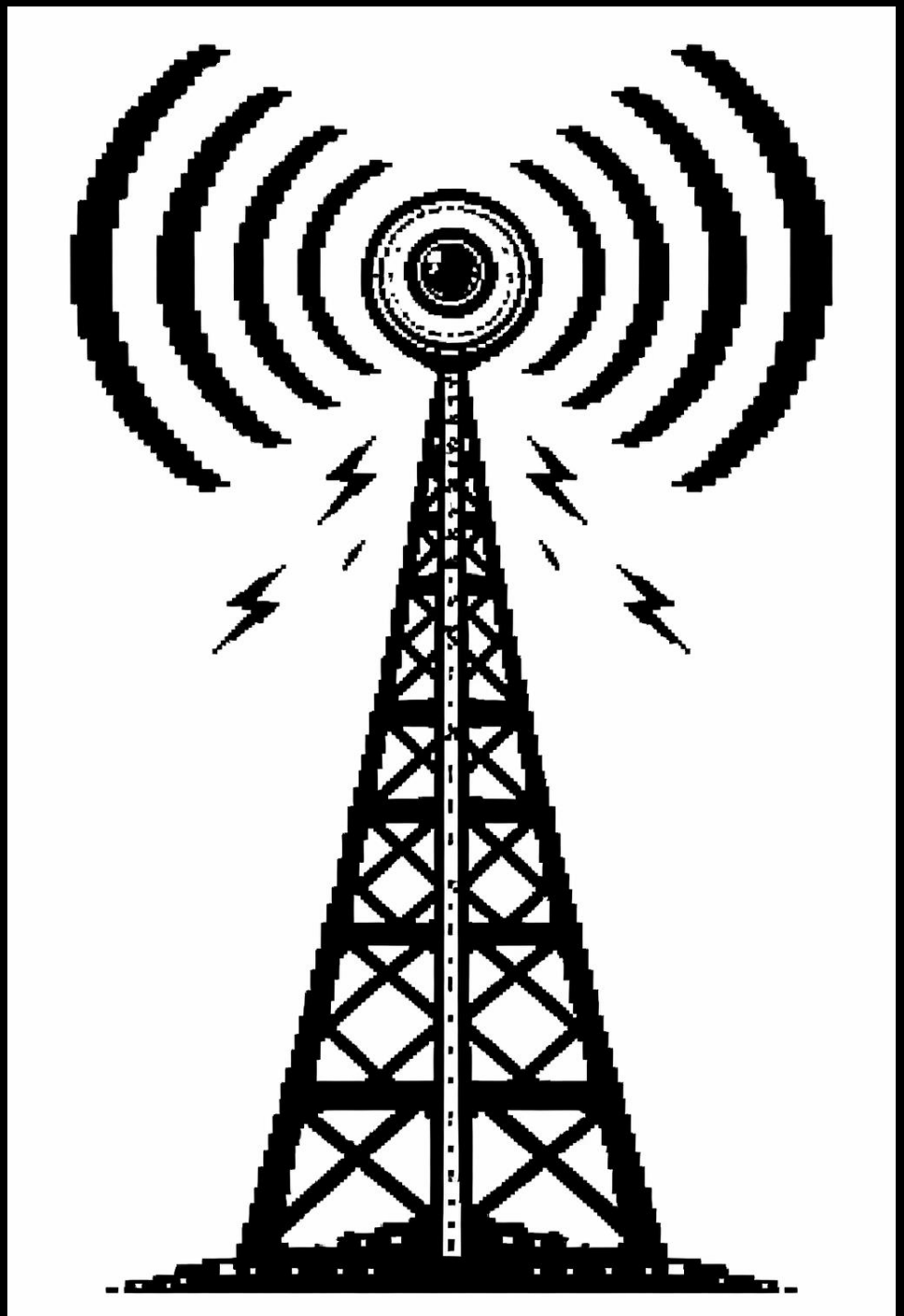
Cooper Quintin
*Senior Staff Technologist*

@oopsbagel
*Rayhunter Maintainer*

Rayhunter community


# Everyday SIGNINT;
# counter-surveillance with Rayhunter

IRL Orca hunting a stingray

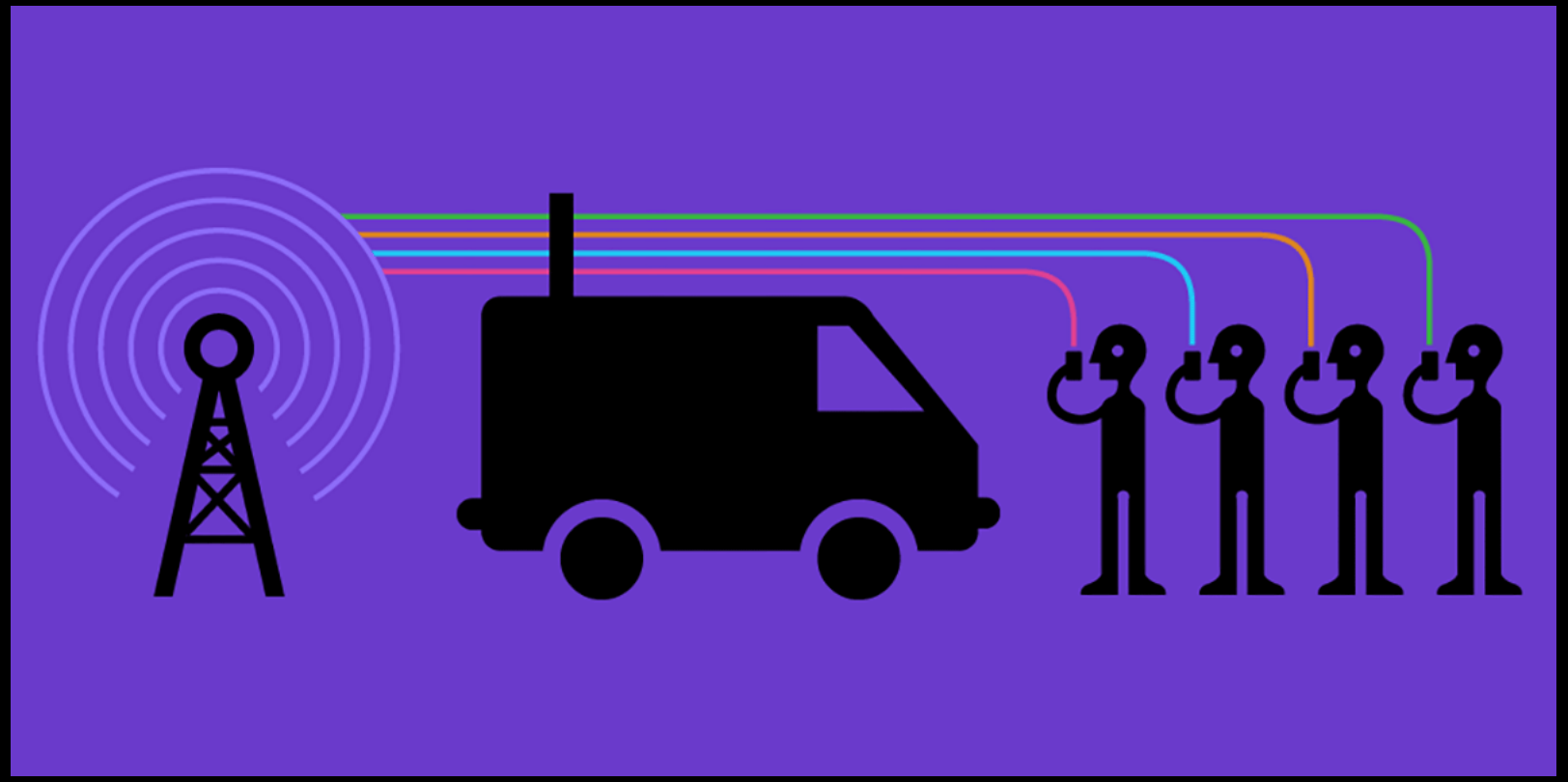


## Street Level Surveillance

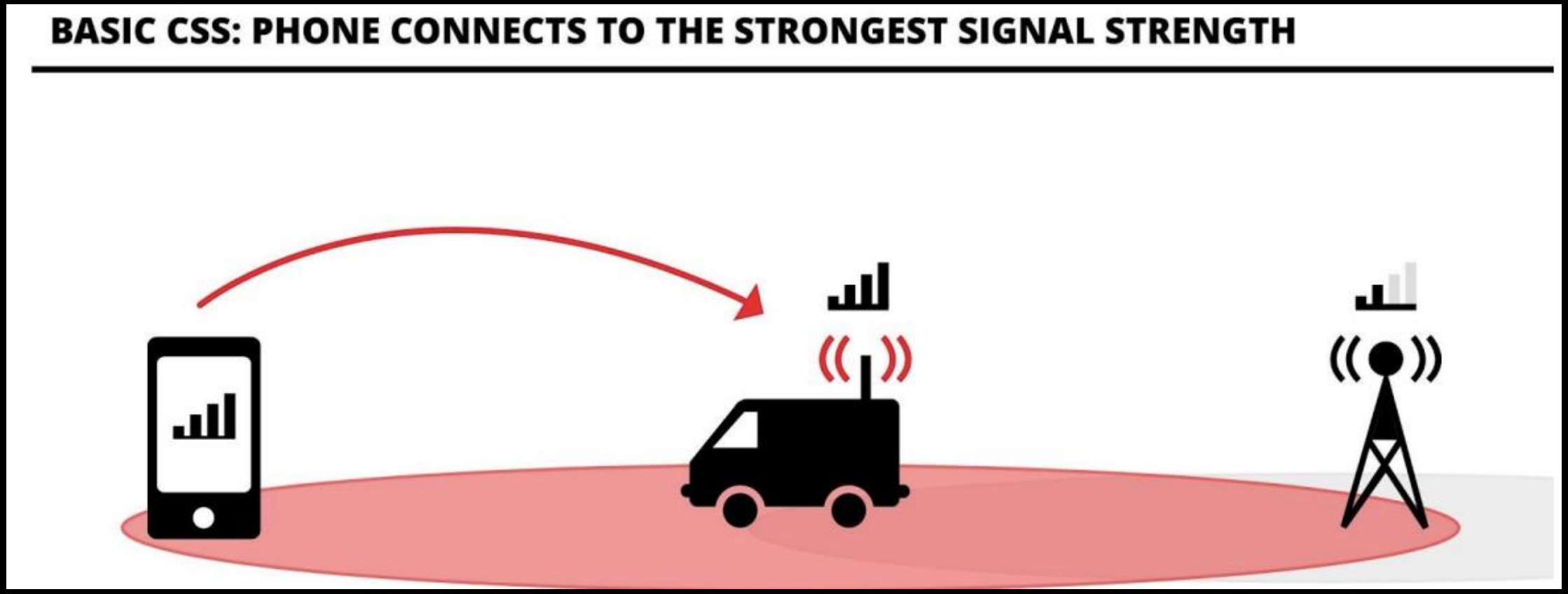
- Traffic Cameras
- ALPR cameras
- Shopping kiosks
- Facial Recognition software
- Stingrays

# $Stingrays

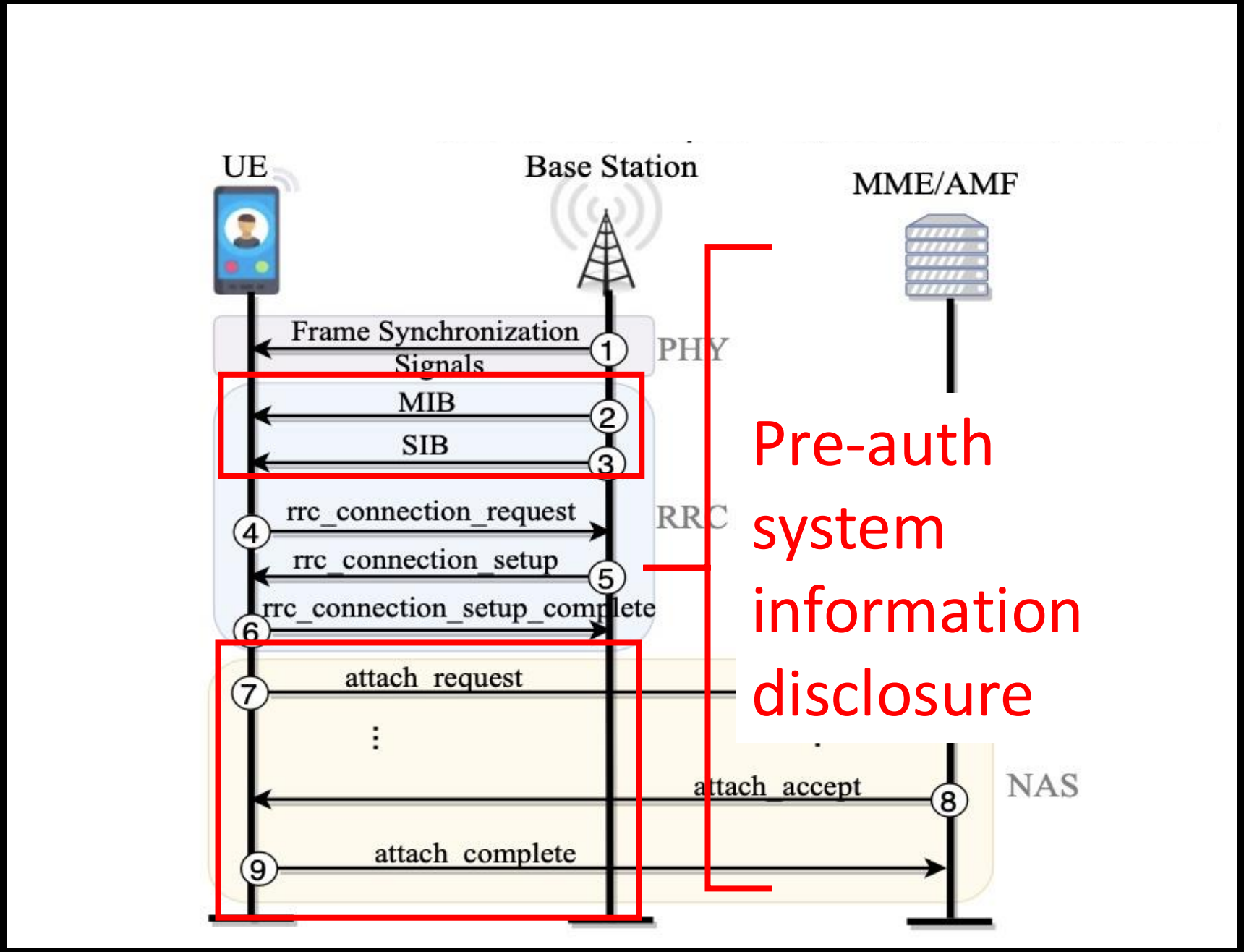
# Stingrays



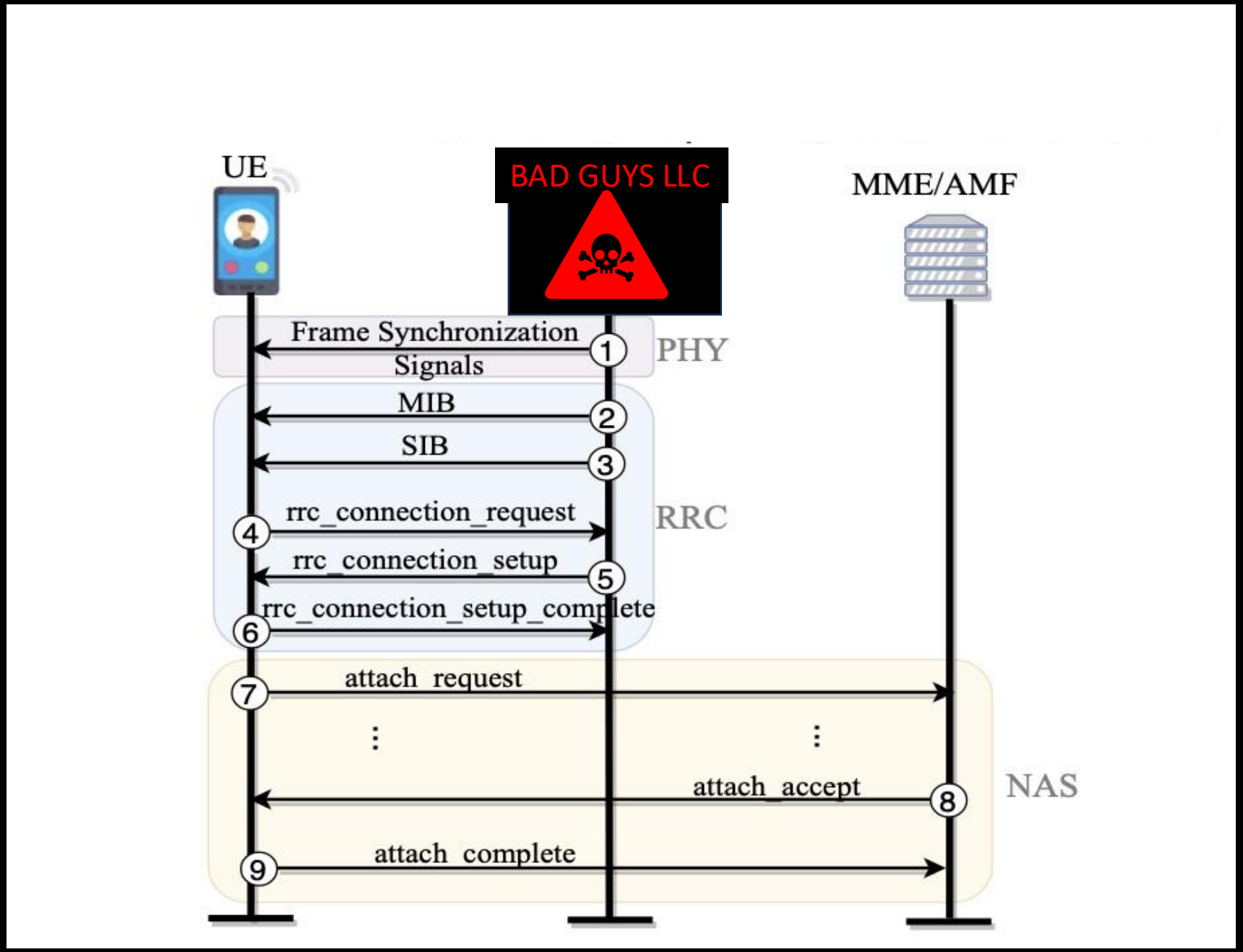
# Basic Mobile interception




https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf



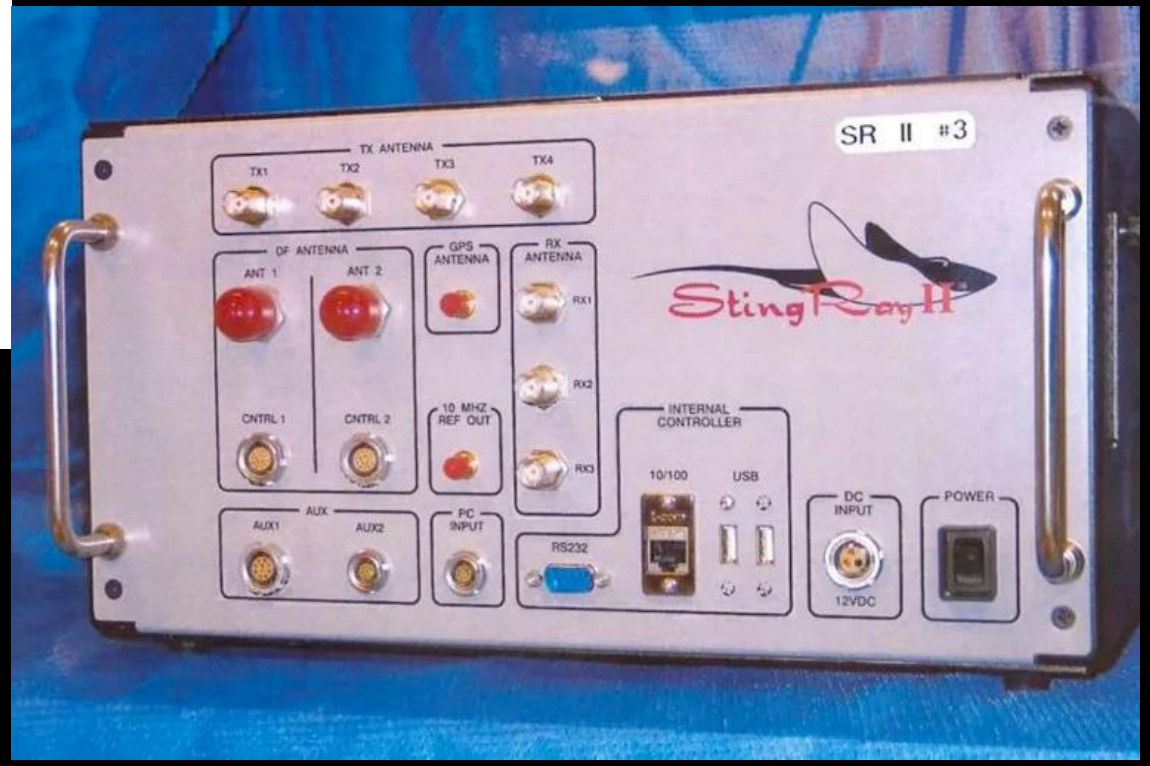

[Insecure Connection Bootstrapping in Cellular Networks:The Root of All Evil]




[Insecure Connection Bootstrapping in Cellular Networks:The Root of All Evil]

**Figure 4.** 5GNR Base Station NG

L3HARRIS®
FAST. FORWARD.




Jacobs
Challenging today.
Reinventing tomorrow.


https://www.muckrock.com/news/archives/2016/dec/07/rochester-police-release-unredacted-list-harris-co/

| KingFish Man-Portable System (Option 2): for CDMA.GSM/iDEN | | | | | | | |
|---|---|---|---|---|---|---|---|
| Registration, Dir Finding, Isolation & Collection Optional Dual-Mode enables KingFish to be used as a vehicular platform. Full-size laptop makes it easier to use in moving vehicle. 25 W PA and 2100 MHz Down Converter enable vehicular operations and capture of devices operating in the 2100 MHz range. AmberJack Direction-Finding device mounts in or on vehicle for DF functionality. Single radio transciever. Single XT and Single RX Oinly. | KINGFISH | KingFish System | $ | 27,800 | 1 | $ | 27,800 |
| | KF-CDMA-SW | CDMA controller software | $ | 18,100 | 1 | $ | 18,100 |
| | KF-GSM-SW | GSM controller software | $ | 18,100 | 1 | $ | 18,100 |
| | KF-iDEN-SW | iDEN controler software | $ | 18,100 | 1 | $ | 18,100 |
| | 2014069-101 | Rugged Mini Go Book PC | $ | 5,500 | 1 | $ | 5,500 |
| | | **Man-Portable Subtotal:** | | | | **$** | **87,600** |
| | **Dual-Mode Accessories** | | | | | | |
| | PA-KIT-25W-CONUS | High Power Filtered 25 W PA Kit - 800, 850,1900, 2100B4 MHz | $ | 11,500 | 1 | $ | 11,500 |
| | AJ-W | AmberJack-W (iDEN800/850/900/1800/1900/2100) | $ | 38,400 | 1 | $ | 38,400 |
| | Laptop PC (2009523-101) | Dell Latitude D630 Laptop PC Controller or equivalent spec | $ | 3,500 | | $ | - |
| | CONV-2100/1700-W/BP | StingRay 2100 MHz Band IV - AWS Down Converter | $ | 19,800 | 1 | $ | 19,800 |
| | **ADD TRAINING** | **Dual-Mode Accessories Subtotal:** | | | | **$** | **69,700** |
| | **ADD MAINTENANCE** | | **KingFish System Only** | | | **$** | **157,300** |

Option 2

# Kingfish package - $157,300

| Technology | Part Number | Description | Unit Price | Qty (ea.) | Total Price |
|---|---|---|---|---|---|
| **StingRay II Vehicular System CDMA/GSM/iDEN** | STINGRAY-II | StingRay II System Kit[1] | $ 148,000 | | $ - |
| Multi TX and RX. 4-radio transciever for Registration, Direction Finding, Isolation & Collection Multi-Transmit Capability. Each power amp is specific to an air interface (GSM, iDEN, CDMA). Systems may be ordered separately. | SRAY-II-CDMA-SW | CDMA Controller Software | $ 22,000 | | $ - |
| | SRAY-II-GSM-SW | GSM Controller Software | $ 22,000 | | $ - |
| | SRAY-II-iDEN-SW | iDEN Controller Software | $ 22,000 | | $ - |
| | Laptop PC (2009523-101) | Dell Latitude D630 Laptop PC Controller or equivalent spec | $ 3,500 | | $ - |
| | PA-KIT-30W iDEN 800 | Harpoon High Power Filtered 30W PA Kit - Single Band iDEN 800 | $ 16,400 | | $ - |
| | PA-KIT-30W Dual-Band CONUS | Harpoon High Power Filtered 30W PA Kit - Dual-Band 850/1900 | $ 20,200 | | $ - |
| | PA-KIT-30W 2100 | Harpoon High Power Filtered 30W PA Kit - Single Band 2100 | $ 18,550 | | $ - |
| | AJ-W | AmberJack-W (iDEN800/850/900/1800/1900/2100) | $ 38,400 | | $ - |
| | **ADD TRAINING** | | | | |
| | **ADD MAINTENANCE** | | **StingRay II System Only** | | **$ -** |

# Stingray package - $145,000


Jacobs
Challenging today.
Reinventing tomorrow.

**Figure 4.** 5GNR Base Station NG

**Figure 5.** 8MUX Amplifier

[Proposal Response for Cell-Site Simulator program for the Massachusetts State Police]


[Proposal Response for Cell-Site Simulator program for the Massachusetts State Police]

Proposal Response for CSS Program for the MSP
Solicitation #: SP24-Cell Site Simulator-X02

Jacobs

[Proposal Response for Cell-Site Simulator program for the Massachusetts State Police]

# $Legality

**Department of Justice Policy Guidance:**
**Use of Cell-Site Simulator Technology**

Purchase Order (PO) PIID 15M10318PA4100281

Awarding Agency

Department of J

CIENCE LLC

DEPOT CT SE STE 215
LEESBURG, VA 20175-3017
UNITED STATES

Congressional District: VA-10

public

); AND

TO BE CONTINUED...

Executive Order 14093 of March 27, 2023

**Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security**

# Graphite Caught

## First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted

# $Legality?


# $getResource

- Runs on a $20 hotspot
- Covert
- Easy to install
- User-friendly UI

# $projectGoals

- Real-time analysis to understand if free-speech activities are being monitored
- Expand to nationwide locales to get better data
- What exploits stingrays are using
- Give activists more threat-model data for safer operations

1337

h4xL0Rd


orbic
NO SERVICE
Retrieving data
usage info

SSID:RAYHUNTER
PW:FTP12345
192.168.1.1:8080

192.168.1.1:8080/index.html

Gemini

Not Secure 192.168.1.1:8080/index.html

rayhunter

Logs Report Issue Docs

## Current Recording

0 warnings

**ID: 1764983035**
38.49 KB

Start: 12/5/25, 8:03:55 PM EST
Last Message: 12/5/25, 8:16:40 PM EST

pcap qmdl zip Stop

## System Information

| | |
|---|---|
| **Rayhunter Version** | 0.8.0 |
| **Storage** | 16% used (34.6M used / 180.2M available) |
| **Memory (RAM)** | Free: 23.6M, Used: 136.3M |
| **Battery** |  |

## History

Filter for Warnings

| ID | Started | Last Message | Size | Download | Analysis |
|---|---|---|---|---|---|
| 1767702699 | 1/6/26, 7:31:39 AM EST | 1/7/26, 6:37:31 PM EST | 1.64 MB | pcap qmdl zip | 0 warnings |
| 1767562594 | 1/4/26, 4:36:34 PM EST | 1/4/26, 4:49:44 PM EST | 14.7 KB | pcap qmdl zip | 0 warnings |
| 1767561496 | 1/4/26, 4:18:16 PM EST | 1/4/26, 4:35:52 PM EST | 19 KB | pcap qmdl zip | 0 warnings |
| 1767391698 | 1/2/26, 5:08:18 PM EST | 1/4/26, 4:17:16 PM EST | 2.6 MB | pcap qmdl zip | 0 warnings |
| 1767381729 | 1/2/26, 2:22:09 PM EST | 1/2/26, 5:07:54 PM EST | 91.81 KB | pcap qmdl zip | 0 warnings |
| 1766608492 | 12/24/25, 3:34:52 PM | 12/27/25, 11:51:23 AM | | | |

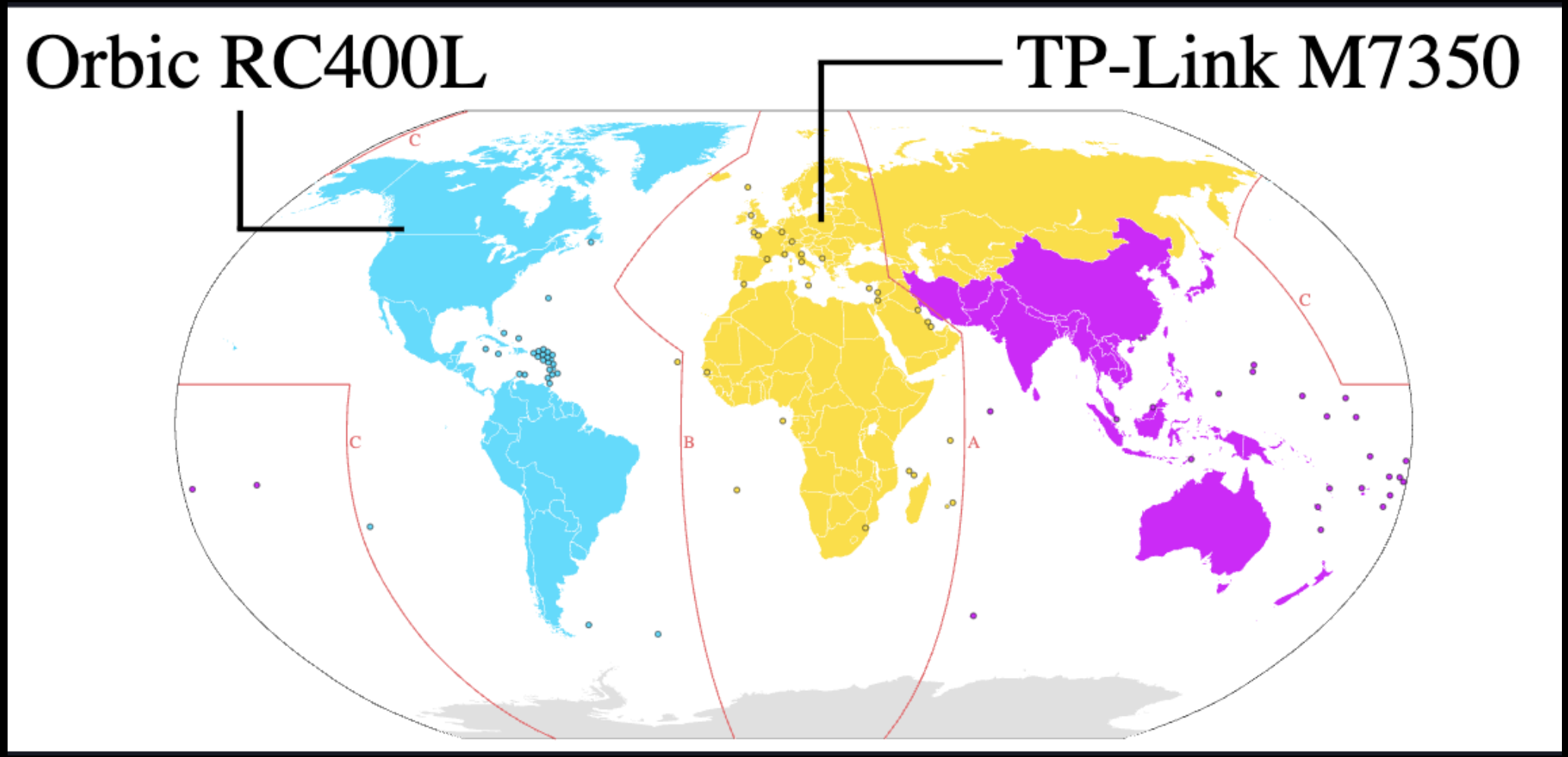
# $undrTehH00d

- Rayhunter reads qualcomm diag data to ingest logs
  - Rooted to access the debug layer
- Captures comm. data between device and base station
- Stores files locally
- Analyzes for anomalies
- Outputs results to the webui w/pcaps for further analysis

# $initRayhunter

- Rayhunter runs on just about any hotspot with a qualcomm modem

# $initRayhunter



# $initRayhunter

| Device | Recommended region |
| --- | --- |
| Wingtech CT2MHS01 | Americas |
| Tmobile TMOHS1 | Americas |
| TP-Link M7310 | Africa, Europe, Middle East |
| PinePhone and PinePhone Pro | Global |
| FY UZ801 | Asia, Europe |
| Moxee hotspot | Americas |

# $Heuristics

# $heuristics

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1764944009 | 12/5/25, 9:13:29 AM EST | 12/6/25, 7:57:48 AM EST | 424.4 KB | pcap | qmdl | zip | 0 warnings |

Re-analyze

No warnings to display!

Metadata

Analysis by Rayhunter version 0.8.0

Analyzers

**Identity (IMSI or IMEI) requested in suspicious manner:** Tests whether the ME sends an Identity Request NAS message without either an associated attach request or auth accept message

**Connection Release/Redirected Carrier 2G Downgrade:** Tests if a cell releases our connection and redirects us to a 2G cell.

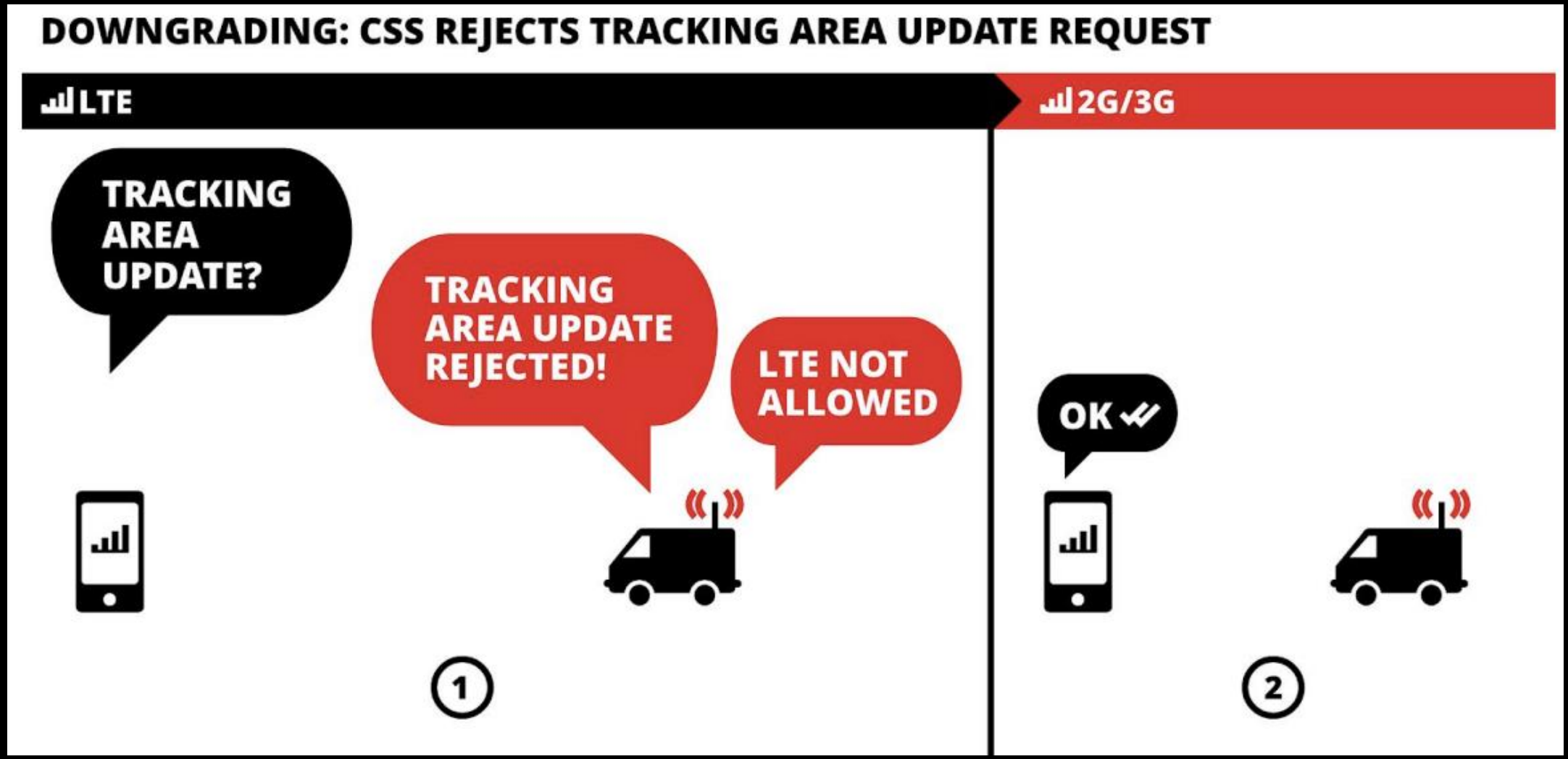
**LTE SIB 6/7 Downgrade:** Tests for LTE cells broadcasting a SIB type 6 and 7 which include 2G/3G frequencies with higher priorities.

**Null Cipher:** Tests whether the cell suggests using a null cipher (EEA0)

**NAS Null Cipher Requested:** Tests whether the MME requests to use a null cipher in the NAS security mode command

**Incomplete SIB:** Tests whether a SIB1 message contains a full chain of followup sibs

# $downgrade attacks



# $downgrade attacks

- 2G Downgrade
  - Crimeware
  - Content injection
  - Outside of the US

# $downgrade attacks

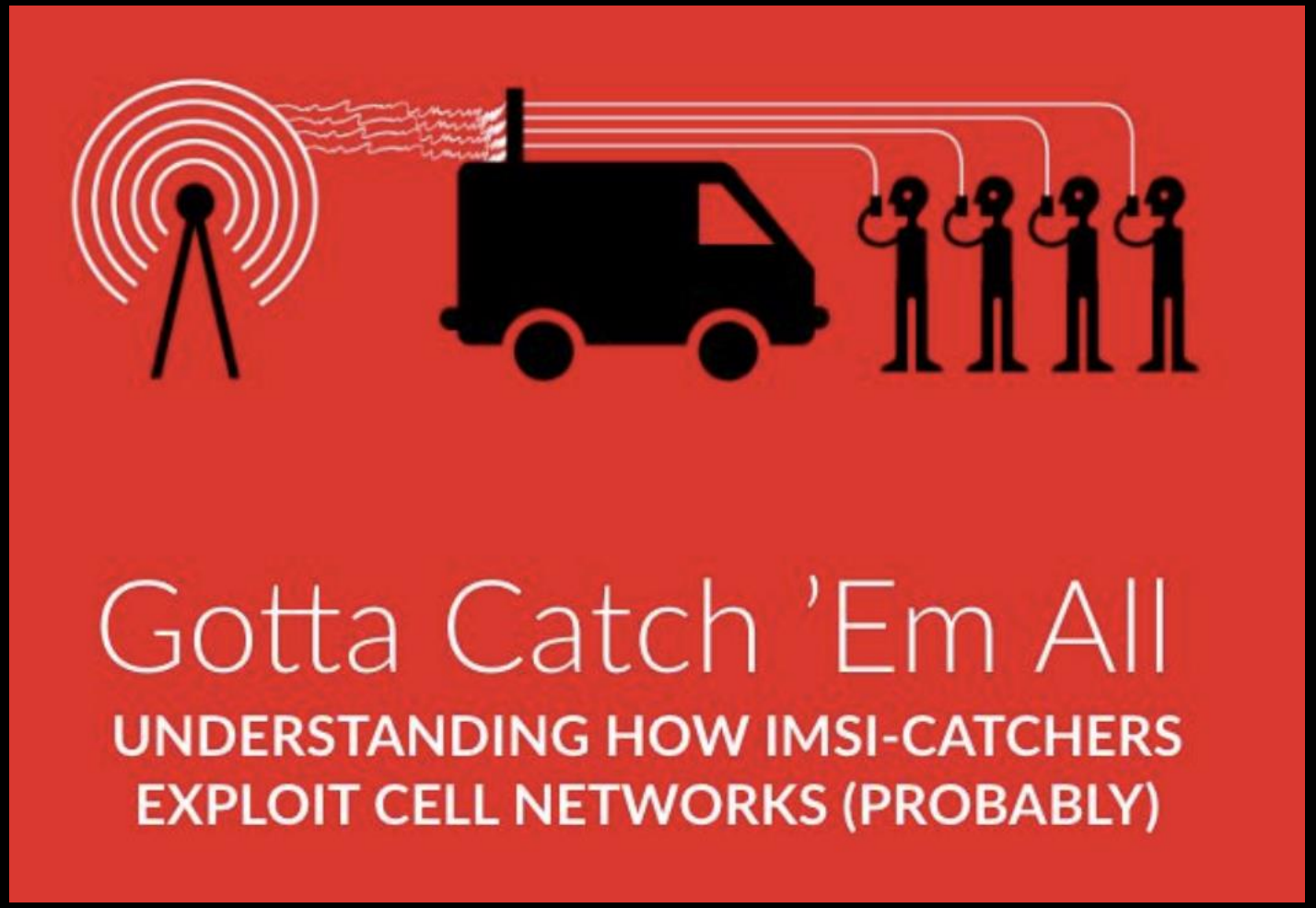
# Suspected Paris Bomb Was Actually an IMSI-Catcher

By **Eric Priezkalns** 3 Jan 2023 Privacy & Intellectual Property

# $Null cipher attacks

- Null Cipher
  - Checks to see if the base station suggests null ciphers
  - Removes encryption
  - Great for content interception
  - Legitimate use for 911 calls with no service

# $further reading




https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf

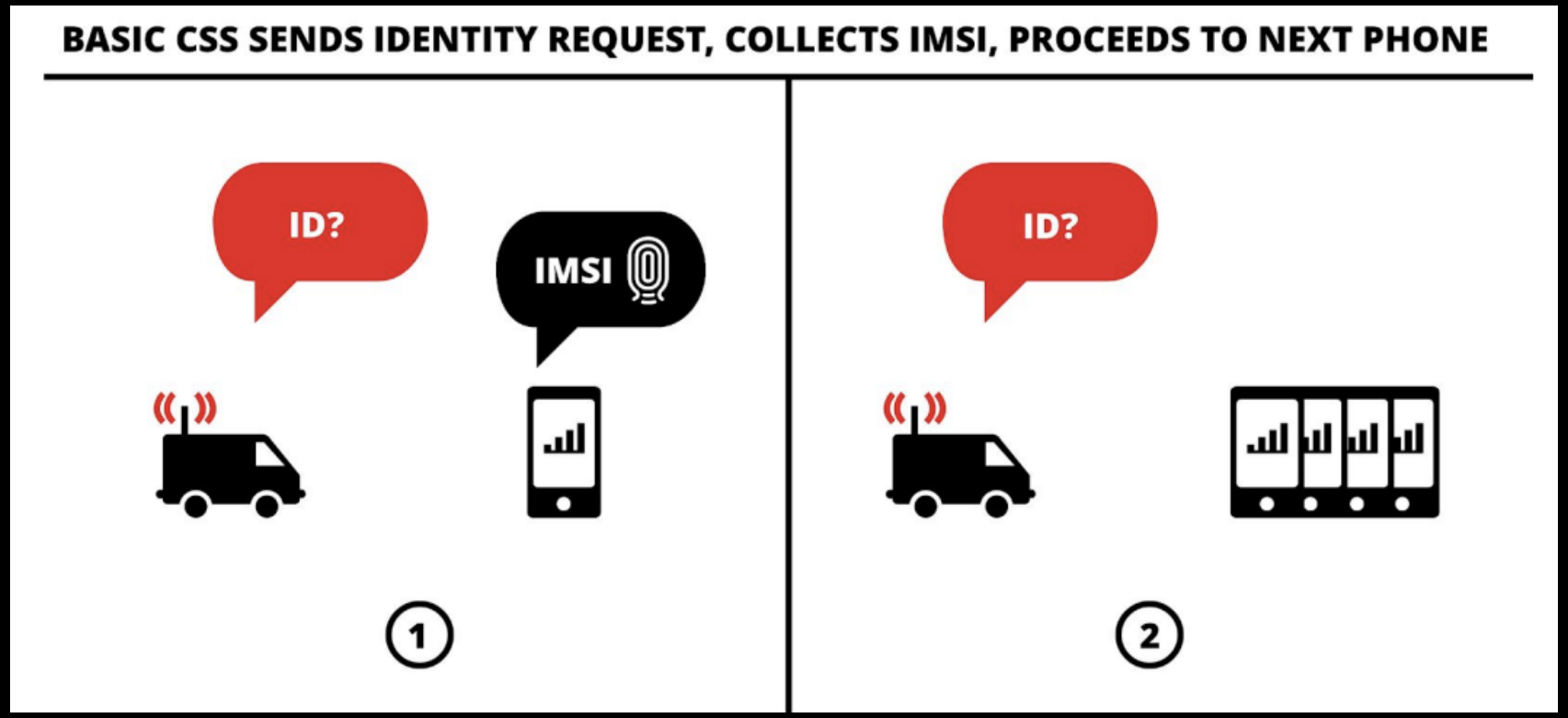
# $Incomplete SIB Chains

- Incomplete SIB chains
  - Legitimate towers will frontload clients with SIBs
  - CSS will send only NECESSARY SIB messages

# $Identity requests

- Device IMSI Requested
  - IMSI/IMEI is requested without authentication
  - Toughest requests to parse
  - Legitimate requests are common
  - But stingrays use this as a vector

# $Identity requests



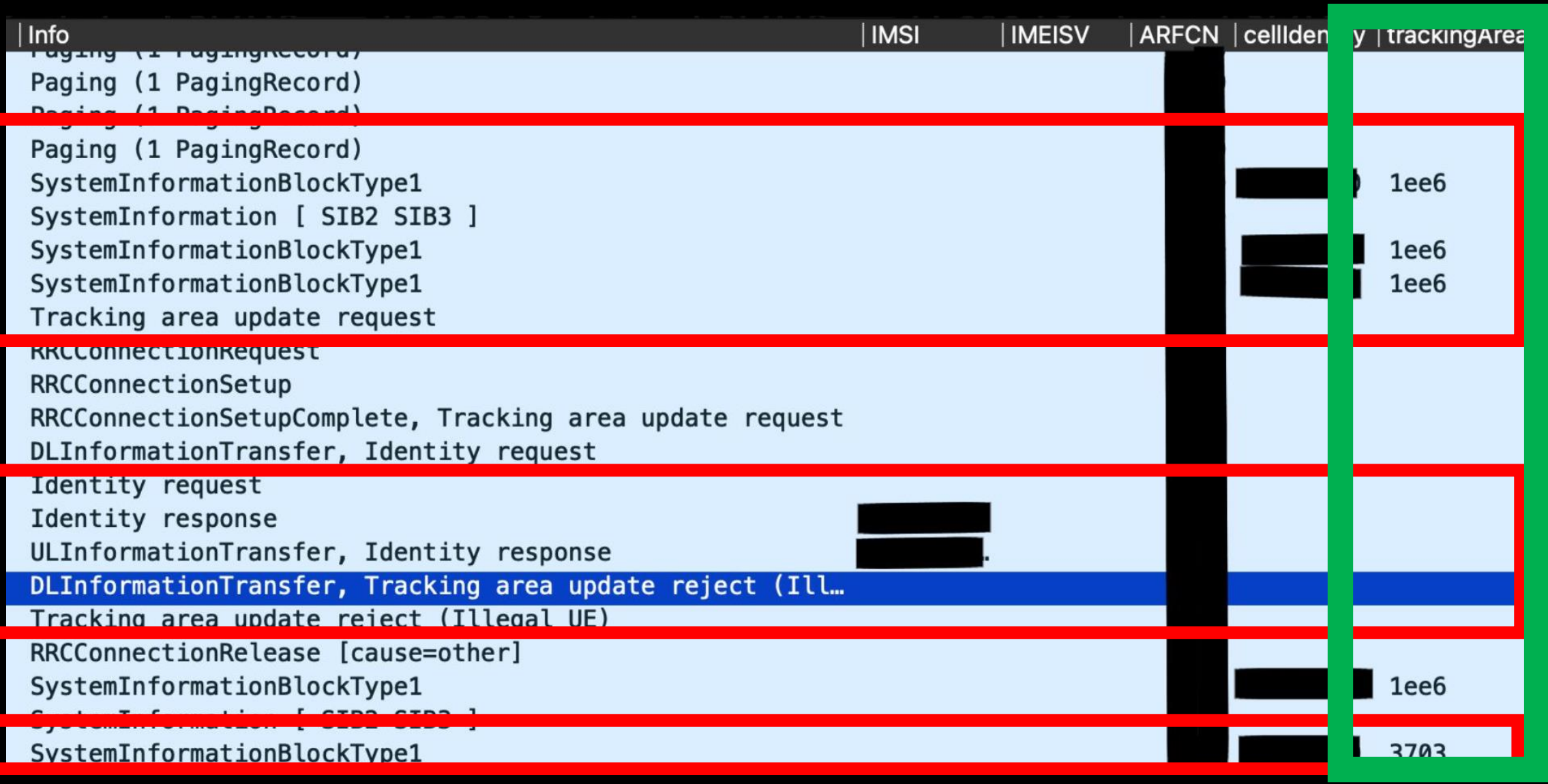

Basic IMSI request

# $Identity requests

Tell-Tale Stingray flow:

- IMSI Request ->No Auth -> Detach
  - Sus

# $inTheWild




Commercial CSS Identification PCAP – CAPE – EFF

# $inTheWild

# $inTheWild

```
→  pcaps rayhunter-check -p 2_diff_tac_cause_3.pcap
INFO  [rayhunter_check] Analyzers:
INFO  [rayhunter_check]     - Identity (IMSI or IMEI) requested in suspicious manner (v2): Tests whether the ME sends an Identity Request NAS message without either an
 accept message
INFO  [rayhunter_check]     - Connection Release/Redirected Carrier 2G Downgrade (v1): Tests if a cell releases our connection and redirects us to a 2G cell.
INFO  [rayhunter_check]     - LTE SIB 6/7 Downgrade (v1): Tests for LTE cells broadcasting a SIB type 6 and 7 which include 2G/3G frequencies with higher priorities.
INFO  [rayhunter_check]     - Null Cipher (v1): Tests whether the cell suggests using a null cipher (EEA0)
INFO  [rayhunter_check]     - NAS Null Cipher Requested (v1): Tests whether the MME requests to use a null cipher in the NAS security mode command
INFO  [rayhunter_check]     - Incomplete SIB (v1): Tests whether a SIB1 message contains a full chain of followup sibs
INFO  [rayhunter_check] **** Beginning analysis of 2_diff_tac_cause_3.pcap
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.182570 +00:00 SIB1 scheduling info list was malformed (packet 108)
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.182688 +00:00 SIB1 scheduling info list was malformed (packet 110)
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.182688 +00:00 SIB1 scheduling info list was malformed (packet 111)
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.183072 +00:00 Disconnected after Identity Request without Auth Accept (f
WARN  [rayhunter_check] 2_diff_tac_cause_3.pcap: WARNING (Severity: High) - 1980-01-26 05:46:22.183411 +00:00 SIB1 scheduling info list was malformed (packet 123)
INFO  [rayhunter_check] 2_diff_tac_cause_3.pcap: 350 messages analyzed, 5 warnings, 1 messages skipped
```

CAPE PCAP Rayhunter analysis – CAPE – EFF -$ref12

# $inTheWild

```
+00:00 SIB1 scheduling info list was malformed (packet 108)
+00:00 SIB1 scheduling info list was malformed (packet 110)
+00:00 SIB1 scheduling info list was malformed (packet 111)
+00:00 Disconnected after Identity Request without Auth Accept (f
+00:00 SIB1 scheduling info list was malformed (packet 123)
```

CAPE PCAP Rayhunter analysis – CAPE – EFF -$ref12

# $inTheWild

```
-goodsim.qmdl: INFO - 2025-06-07 21:22:06.117 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: INFO - 2025-06-08 00:22:28.411 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 08:46:57.462 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-08 08:46:58.206 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 09:22:13.650 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-08 09:22:14.536 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 12:20:30.716 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-08 12:20:31.448 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 21:22:34.877 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-08 21:22:35.574 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-08 23:46:24.430 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-08 23:46:25.220 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-09 09:22:42.106 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-09 09:22:42.787 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-09 10:43:39.567 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-09 10:43:40.258 +00:00 Disconnected after Identity Request without Auth Accept
-goodsim.qmdl: WARNING (Severity: High) - 2025-06-09 23:49:13.069 +00:00 Identity requested without Attach Request
-goodsim.qmdl: INFO - 2025-06-09 23:49:13.802 +00:00 Disconnected after Identity Request without Auth Accept
```

Caribbean Cruise – ZeroChaos via EFF -$ref12

# $inTheWild

```
WARNING (Severity: High) - 2025-06-10 14:21:55.975 +00:00 NAS Security mode command requested null cipher(packet 166851)
WARNING (Severity: High) - 2025-06-10 14:22:06.562 +00:00 NAS Security mode command requested null cipher(packet 166877)
WARNING (Severity: High) - 2025-06-10 14:44:15.245 +00:00 NAS Security mode command requested null cipher(packet 167483)
WARNING (Severity: High) - 2025-06-10 14:45:05.109 +00:00 NAS Security mode command requested null cipher(packet 167591)
WARNING (Severity: High) - 2025-06-10 14:45:15.717 +00:00 NAS Security mode command requested null cipher(packet 167612)
WARNING (Severity: High) - 2025-06-10 14:45:26.340 +00:00 NAS Security mode command requested null cipher(packet 167633)
WARNING (Severity: High) - 2025-06-10 14:45:36.852 +00:00 NAS Security mode command requested null cipher(packet 167654)
WARNING (Severity: High) - 2025-06-10 14:45:47.430 +00:00 NAS Security mode command requested null cipher(packet 167675)
WARNING (Severity: High) - 2025-06-10 15:42:52.250 +00:00 NAS Security mode command requested null cipher(packet 170505)
WARNING (Severity: High) - 2025-06-10 15:43:02.816 +00:00 NAS Security mode command requested null cipher(packet 170526)
WARNING (Severity: High) - 2025-06-10 15:43:13.335 +00:00 NAS Security mode command requested null cipher(packet 170547)
WARNING (Severity: High) - 2025-06-10 15:43:24.007 +00:00 NAS Security mode command requested null cipher(packet 170568)
WARNING (Severity: High) - 2025-06-10 15:43:34.513 +00:00 NAS Security mode command requested null cipher(packet 170589)
WARNING (Severity: High) - 2025-06-10 15:56:28.342 +00:00 NAS Security mode command requested null cipher(packet 171416)
WARNING (Severity: High) - 2025-06-10 15:56:38.885 +00:00 NAS Security mode command requested null cipher(packet 171442)
WARNING (Severity: High) - 2025-06-10 15:56:49.612 +00:00 NAS Security mode command requested null cipher(packet 171463)
WARNING (Severity: High) - 2025-06-10 15:57:03.956 +00:00 NAS Security mode command requested null cipher(packet 171484)
WARNING (Severity: High) - 2025-06-10 15:57:14.478 +00:00 NAS Security mode command requested null cipher(packet 171505)
WARNING (Severity: High) - 2025-06-10 16:10:07.127 +00:00 NAS Security mode command requested null cipher(packet 172263)
WARNING (Severity: High) - 2025-06-10 16:10:18.090 +00:00 NAS Security mode command requested null cipher(packet 172289)
```

Port of Turks & Caicos – ZeroChaos via EFF -$ref12

# $inTheWild

```
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:15:02.598 +00:00 Disconnected after Identity Request without Auth Accept (frame 1036)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:15:39.066 +00:00 Disconnected after Identity Request without Auth Accept (frame 1056)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:16:21.876 +00:00 Disconnected after Identity Request without Auth Accept (frame 1078)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:16:47.325 +00:00 Disconnected after Identity Request without Auth Accept (frame 1100)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:17:05.607 +00:00 Disconnected after Identity Request without Auth Accept (frame 1121)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:17:31.074 +00:00 Disconnected after Identity Request without Auth Accept (frame 1141)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:17:45.371 +00:00 Disconnected after Identity Request without Auth Accept (frame 1159)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:18:04.609 +00:00 Disconnected after Identity Request without Auth Accept (frame 1179)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:19:00.843 +00:00 Disconnected after Identity Request without Auth Accept (frame 1204)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:19:58.452 +00:00 Disconnected after Identity Request without Auth Accept (frame 1224)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:21:02.466 +00:00 Disconnected after Identity Request without Auth Accept (frame 1250)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:22:00.123 +00:00 Disconnected after Identity Request without Auth Accept (frame 1275)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:23:06.593 +00:00 Disconnected after Identity Request without Auth Accept (frame 1303)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:24:00.435 +00:00 Disconnected after Identity Request without Auth Accept (frame 1327)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:25:04.431 +00:00 Disconnected after Identity Request without Auth Accept (frame 1352)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:26:02.012 +00:00 Disconnected after Identity Request without Auth Accept (frame 1373)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:28:02.370 +00:00 Disconnected after Identity Request without Auth Accept (frame 1397)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:30:02.705 +00:00 Disconnected after Identity Request without Auth Accept (frame 1425)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:37:51.056 +00:00 Disconnected after Identity Request without Auth Accept (frame 1464)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:38:09.060 +00:00 Disconnected after Identity Request without Auth Accept (frame 1482)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:41:41.630 +00:00 Disconnected after Identity Request without Auth Accept (frame 1518)
WARN [rayhunter_check] 1746544340.qmdl: WARNING (Severity: High) - 2025-05-06 17:42:32.237 +00:00 Disconnected after Identity Request without Auth Accept (frame 1542)
```

Chicago – Rayhunter community – via EFF -$ref12

# $inTheWild

```
INFO  [rayhunter_check] **** Beginning analysis of 1746553345-2.qmdl
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:46:07.027 +00:00 Disconnected after Identity Request without Auth Accept (frame 13411)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:50:57.546 +00:00 Disconnected after Identity Request without Auth Accept (frame 13572)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:51:02.685 +00:00 Disconnected after Identity Request without Auth Accept (frame 13601)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:52:43.567 +00:00 Disconnected after Identity Request without Auth Accept (frame 13743)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:53:06.714 +00:00 Disconnected after Identity Request without Auth Accept (frame 13760)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 22:53:57.111 +00:00 Disconnected after Identity Request without Auth Accept (frame 13797)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:13:23.503 +00:00 Disconnected after Identity Request without Auth Accept (frame 14530)
INFO  [rayhunter_check] 1746553345-2.qmdl: INFO - 2025-05-07 23:14:47.870 +00:00 Identity request happened without auth request followup (frame 14646)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:14:54.907 +00:00 Disconnected after Identity Request without Auth Accept (frame 14650)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:19:25.402 +00:00 Disconnected after Identity Request without Auth Accept (frame 14830)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:21:46.438 +00:00 Disconnected after Identity Request without Auth Accept (frame 14972)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:28:29.688 +00:00 Disconnected after Identity Request without Auth Accept (frame 15218)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:28:51.864 +00:00 Disconnected after Identity Request without Auth Accept (frame 15235)
WARN  [rayhunter_check] 1746553345-2.qmdl: WARNING (Severity: High) - 2025-05-07 23:29:31.928 +00:00 Disconnected after Identity Request without Auth Accept (frame 15279)
```

Penn Station NYC – Alliraine– via EFF -$ref12

NO WARS
NO KINGS

$inTheWild

NO ICE


# LOOKS LIKE CHICAGO PD HAD A STINGRAY OUT AT THE ERIC GARNER PROTEST LAST NIGHT

12/08/2014


Villita - Chicago – 11.8.25


Villita - Chicago – 11.8.25

# LOOKS LIKE CHICAGO PD HAD A STINGRAY OUT AT THE ERIC GARNER PROTEST LAST NIGHT

12/08/2014

Dispatch: “CPIC [Chicago police's spy 'fusion' center] on the air for a mobile”
Officer 1: “Go ahead”
Officer 2: “Yeah one of the girls, an organizer here, she’s been on her phone a lot. You guys picking up any information, uh, where they’re going, possibly?”
Officer 1: “Yeah we’ll keep an eye on it, we’ll let you know if we hear anything.”
Officer 2: “10-4. They’re compliant, and they’re, they’re doing ok now but she’s spending a lot of time on the phone.”
Officer 1: “10-4”

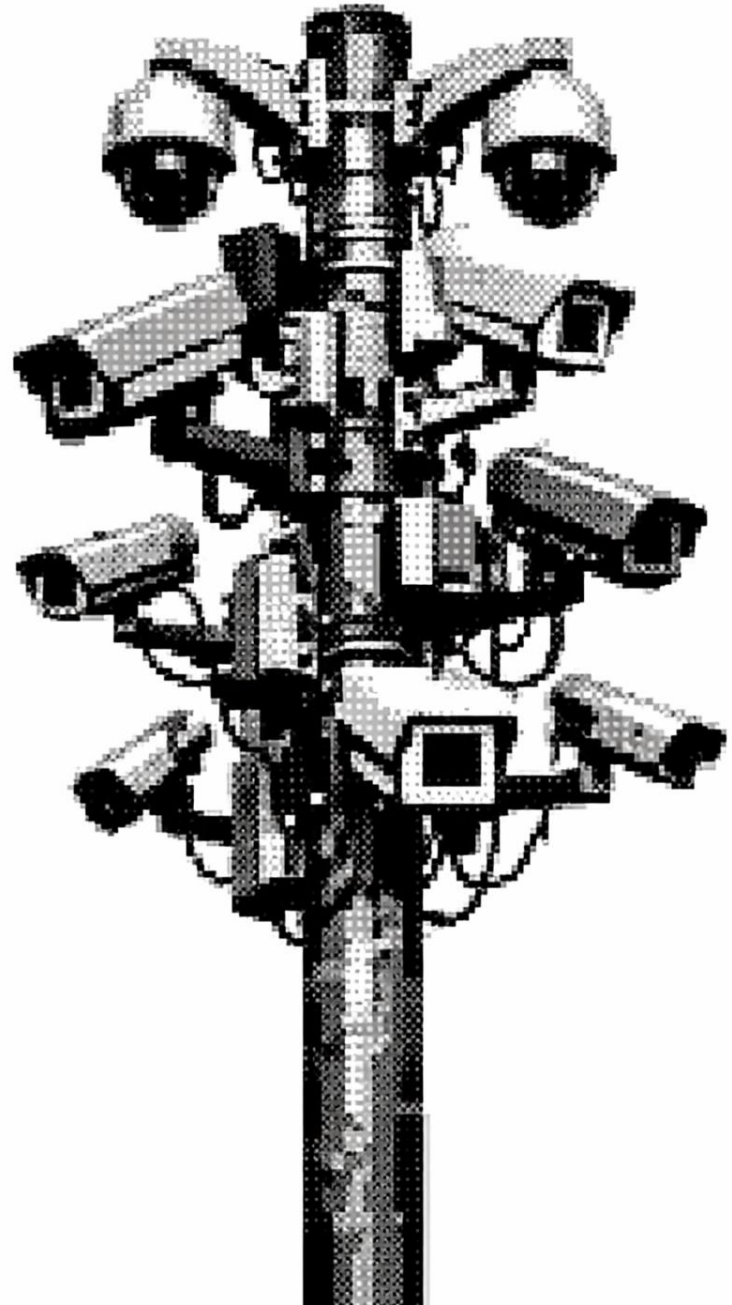
# Chicago alderperson says federal agents handcuffed her at Humboldt Park medical facility

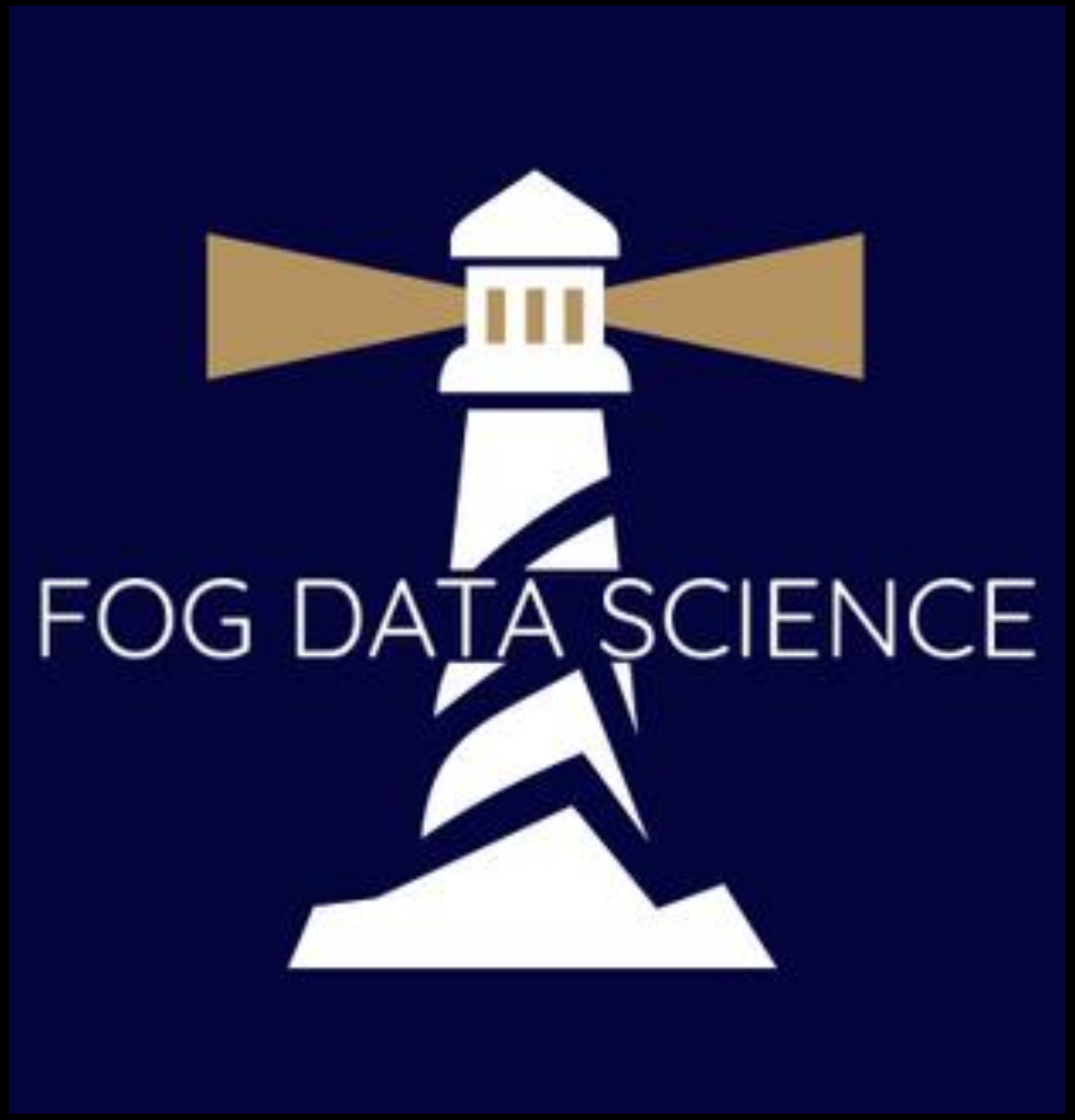
Video shows tear gas deployed across Chicago; Gov. Pritzker calls for investigation into South Shore raid

By Jasmine Minor and Tre Ward

Saturday, October 4, 2025


ICE
POLICE






## $FogDataScience

- Stealth data broker
- Proprietary application
- Used by law enforcement

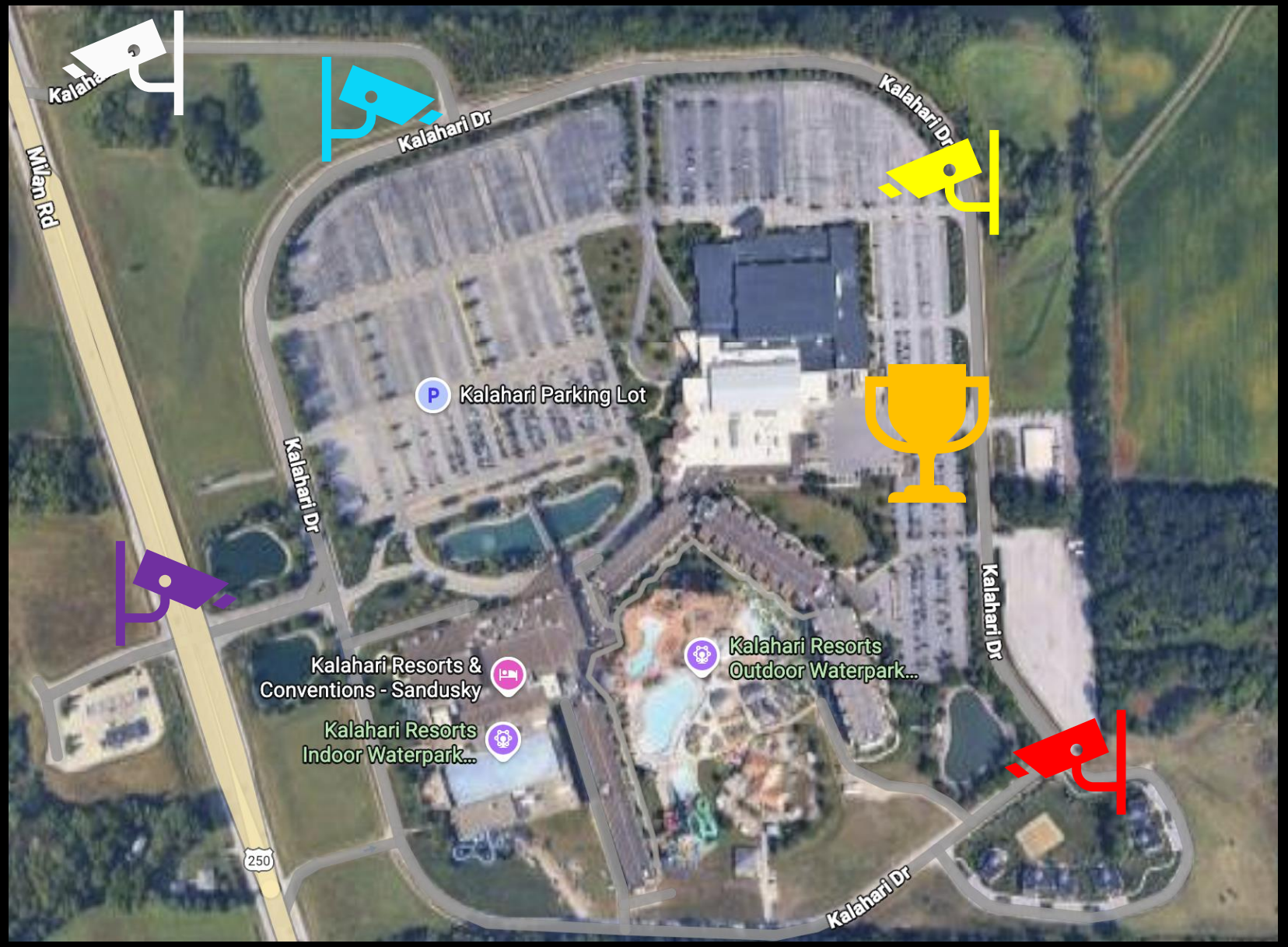

Phone #4- Probably Neighbor
Date/Time
10/06 04:00 - 01/02 04:59
Eastern Daylight Time
Devices/Signals
1 Device (7339 Signals)
Show Timeline
New Query
FOG SCIENCE PRA
Date: 11/30/21 By: M. Ogilby, 2574
760
65
4
4
5th Ave

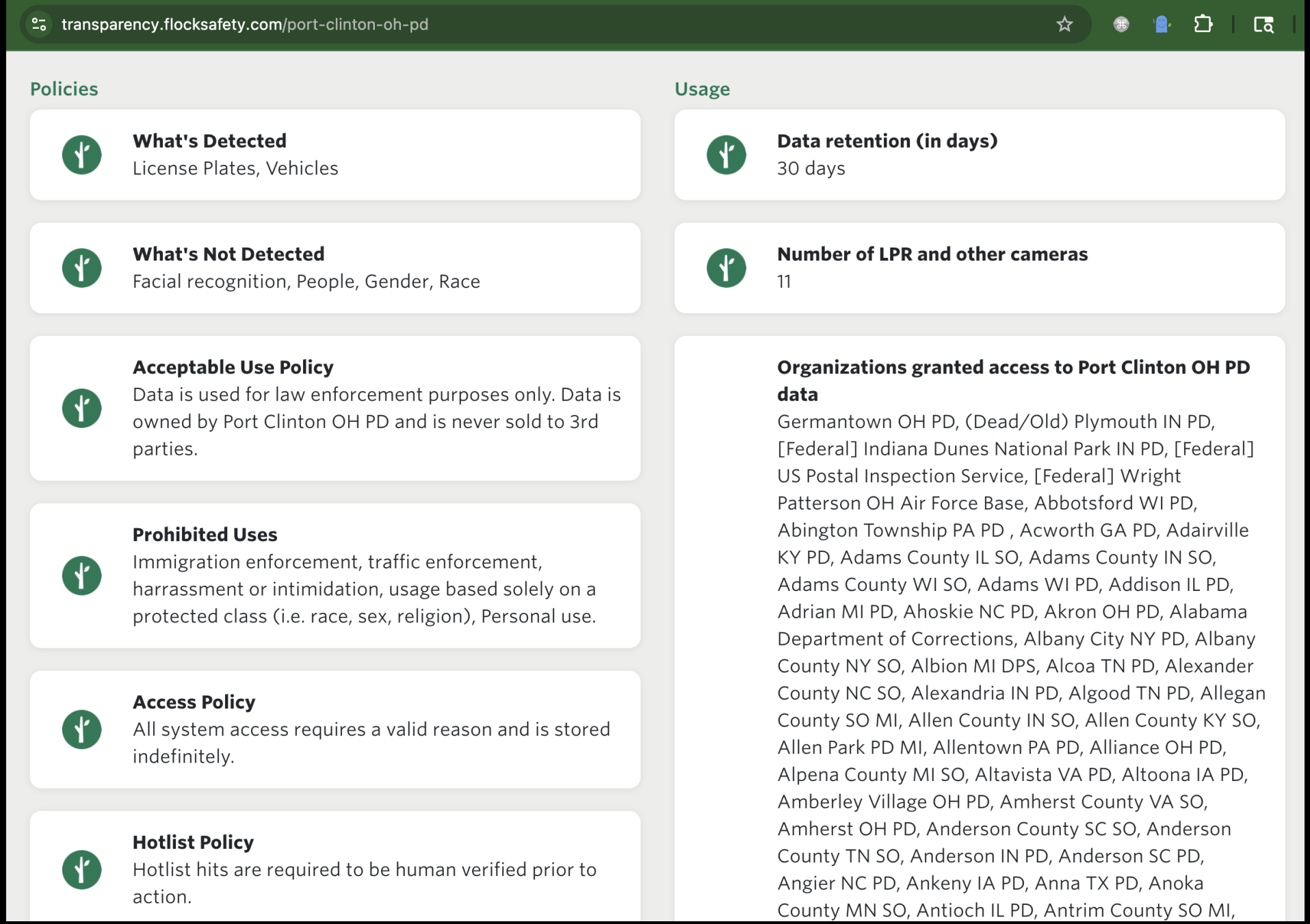
## $getFlocked

- ALPR camera network
- Vehicle identification
- First responder drones
- Shodan-famous

# $getFlocked

- Plate Recognition
- Vehicle identifier
- Location databases
- Hotlists


Kalahari Dr
Kalahari Dr
Milan Rd
Kalahari Parking Lot
Kalahari Dr
Kalahari Dr
Kalahari Resorts &
Conventions - Sandusky
Kalahari Resorts
Outdoor Waterpark...
Kalahari Resorts
Indoor Waterpark...
250
Kalahari Dr




https://transparency.flocksafety.com/port-clinton-oh-pd

# Root from the Coop – Device 3: Root Shell on Flock Safety's Bravo Compute Box

gainsec September 19, 2025

# Fly-By – Device 2: The Falcon/Sparrow – Gated Wireless RCE, Camera Feed, DoS, Information Disclosure and More

gainsec September 27, 2025

# Flock Exposed Its AI-Powered Cameras to the Internet. We Tracked Ourselves

JASON KOEBLER · DEC 22, 2025 AT 11:05 AM

Flock left at least 60 of its people-tracking Condor PTZ cameras live streaming and exposed to the open internet.

## Flock Admin

75.243.117.153
153.sub-75-243-117.myvzw.com
Verizon Business
United States, Acworth

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Tue, 9 Dec 2025 01:03:42 GMT
Connection: keep-alive
Content-Length: 27881
```

## Flock Admin

75.235.242.132
132.sub-75-235-242.myvzw.com
Verizon Business
United States, Alexandria

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Mon, 8 Dec 2025 06:04:16 GMT
Connection: keep-alive
Content-Length: 27881
```

## Flock Admin

72.111.133.26
26.sub-72-111-133.myvzw.com
Verizon Business
United States, Denver

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Mon, 8 Dec 2025 01:40:19 GMT
Connection: keep-alive
Content-Length: 27881
```


https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet-we-tracked-ourselves/

Let's call this what it is: Flock, and the law enforcement agencies we partner with, are under coordinated attack.

The attacks aren't new. You've been dealing with this for forever, and we've been dealing with this since our founding, from the same activist groups who want to defund the police, weaken public safety, and normalize lawlessness. Now, they're producing YouTube videos with misleading headlines. They're also trying to turn a public records process into a weapon against you and against us.

**Make no mistake, we're fighting this fight for you, and, I hope, *with* you.** I remain committed to building world-class technology to help you keep your communities safe. And doing so in a transparent, secure, and privacy centric way.

Please be on the lookout for more information from our Customer Success and Product teams.

Garrett

As far as your assertion that we are currently under attack, I do not believe that this is so. I have dedicated the last 41 years of my life to serving the citizens of the City of Staunton as a police officer, the last 22 as the police chief. What we are seeing here is a group of local citizens who are raising concerns that we could be potentially surveilling private citizens, residents and visitors and using the data for nefarious purposes These citizens have been exercising their rights to receive answers from me, my staff, and city officials, to include our elected leaders. In short, it is democracy in action.

Chief Jim Williams

# City to Terminate Contract with Flock Safety for License Plate Readers

Dec. 19, 2025 –Staunton Police Chief Jim Williams, in consultation with the City Manager and City Council, will move forward to cancel the city's contract with Flock Safety, ending the use of the stationary automated license plate readers that have been installed in the city.

# Congressman Krishnamoorthi, Senator Wyden Urge FTC to Investigate Surveillance Tech Companies to Protect Americans' Personal Data

November 3, 2025 Press Release

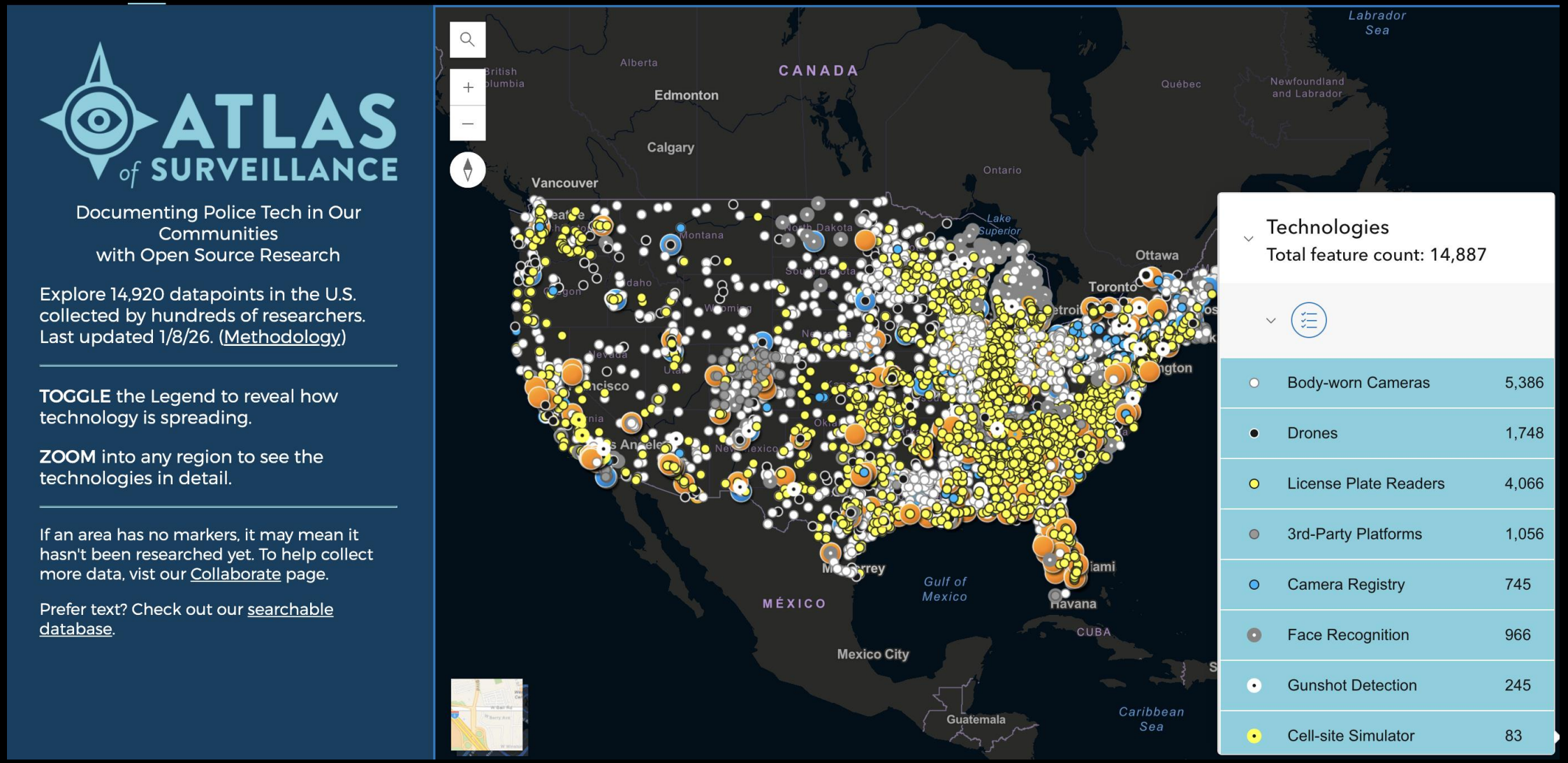
WASHINGTON - Congressman Raja Krishnamoorthi (D-IL) and Senator Ron Wyden (D-OR) today called for an investigation into Flock Safety, a surveillance technology company, for failing to implement cybersecurity protections, allowing Americans' personal data to be exposed for hackers, criminals, and spies to steal.

"Flock has received vast sums of taxpayer money to build a national surveillance network," Congressman Krishnamoorthi and Senator Wyden wrote in their letter to Federal Trade Commission (FTC) Chair Andrew Ferguson. "But Flock's cavalier attitude towards cybersecurity needlessly exposes Americans to the threat of hackers and foreign spies tapping this data. Accordingly, we urge the FTC to hold Flock accountable for its negligent cybersecurity practices."

# $Surveillance Self Defense

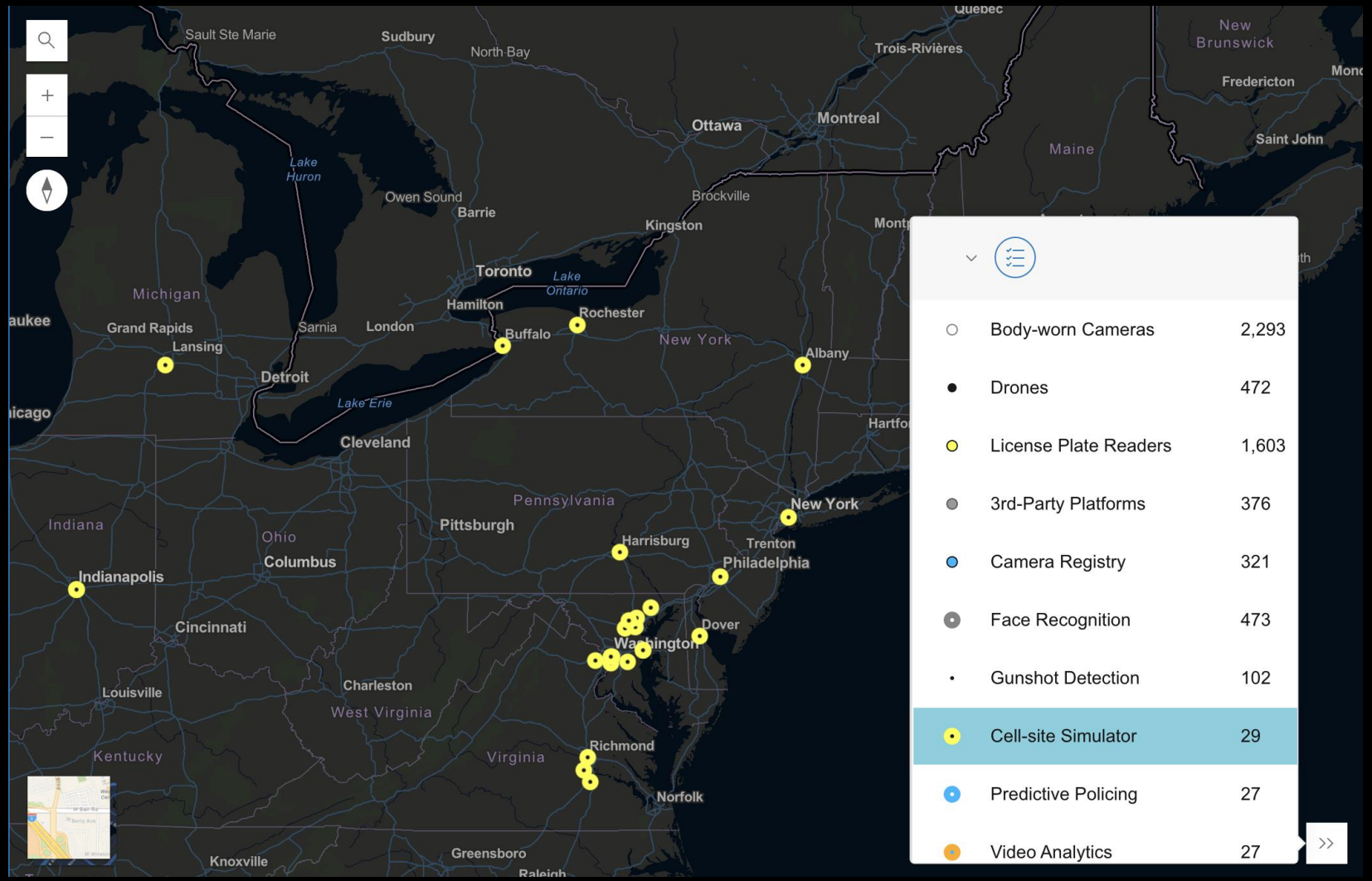

https://www.atlasofsurveillance.org/

# $Surveillance Self Defense




https://www.atlasofsurveillance.org/

# $Surveillance Self Defense

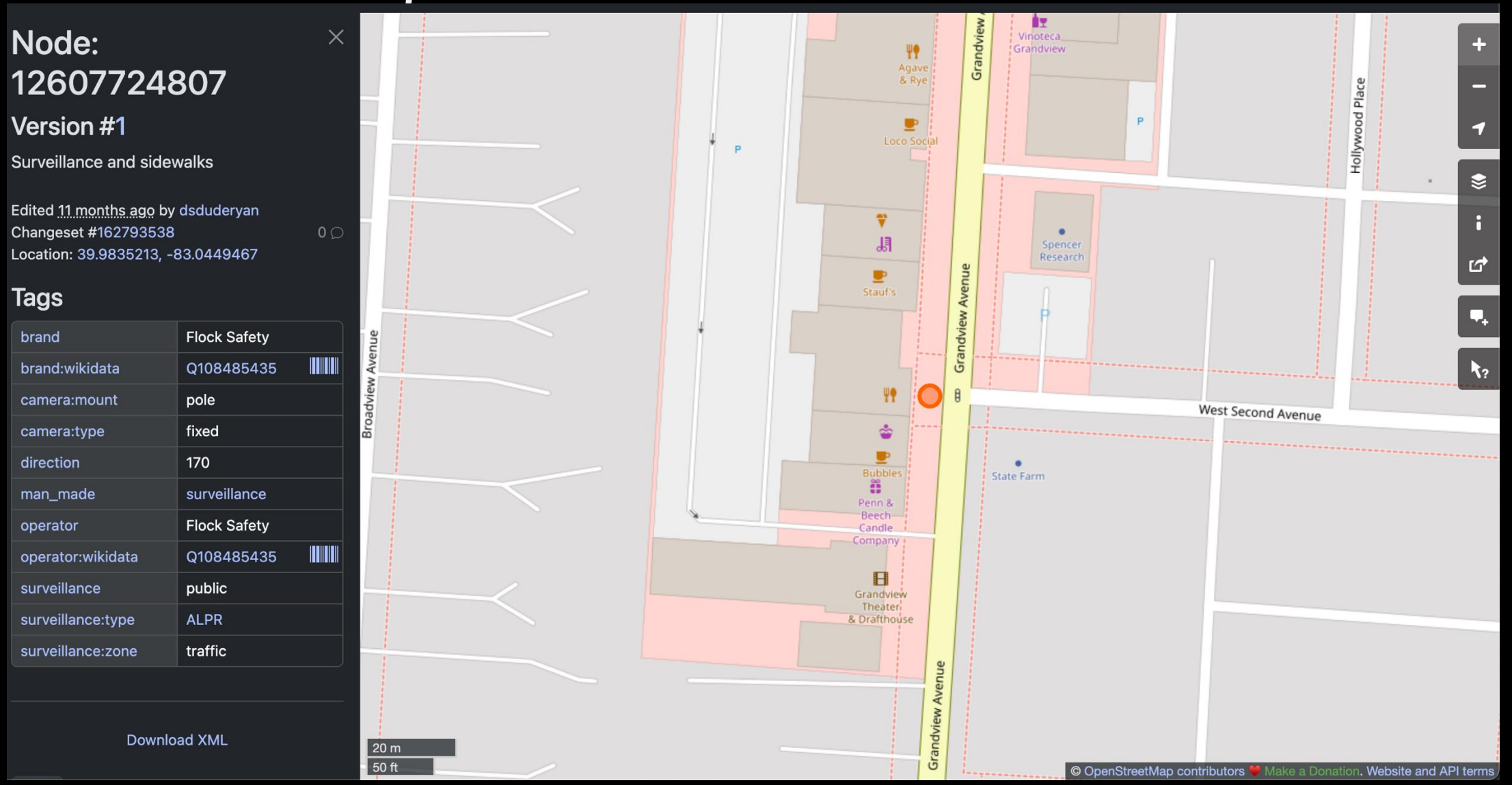



https://www.atlasofsurveillance.org/

# $Surveillance Self Defense


https://deflock.me

# $Surveillance Self Defense




https://www.openstreetmap.org/node/12607724807#map=19/39.983521/-83.044947

# $Surveillance Self Defense


https://ssd.eff.org/

# $Surveillance Self Defense

- Encrypting your Iphone
- Managing digital footprints
- How to Use Signal
- How to Use Tor
- Choosing a VPN
- WTEW: Attending a protest
- Data Destruction

https://ssd.eff.org/

# $Community

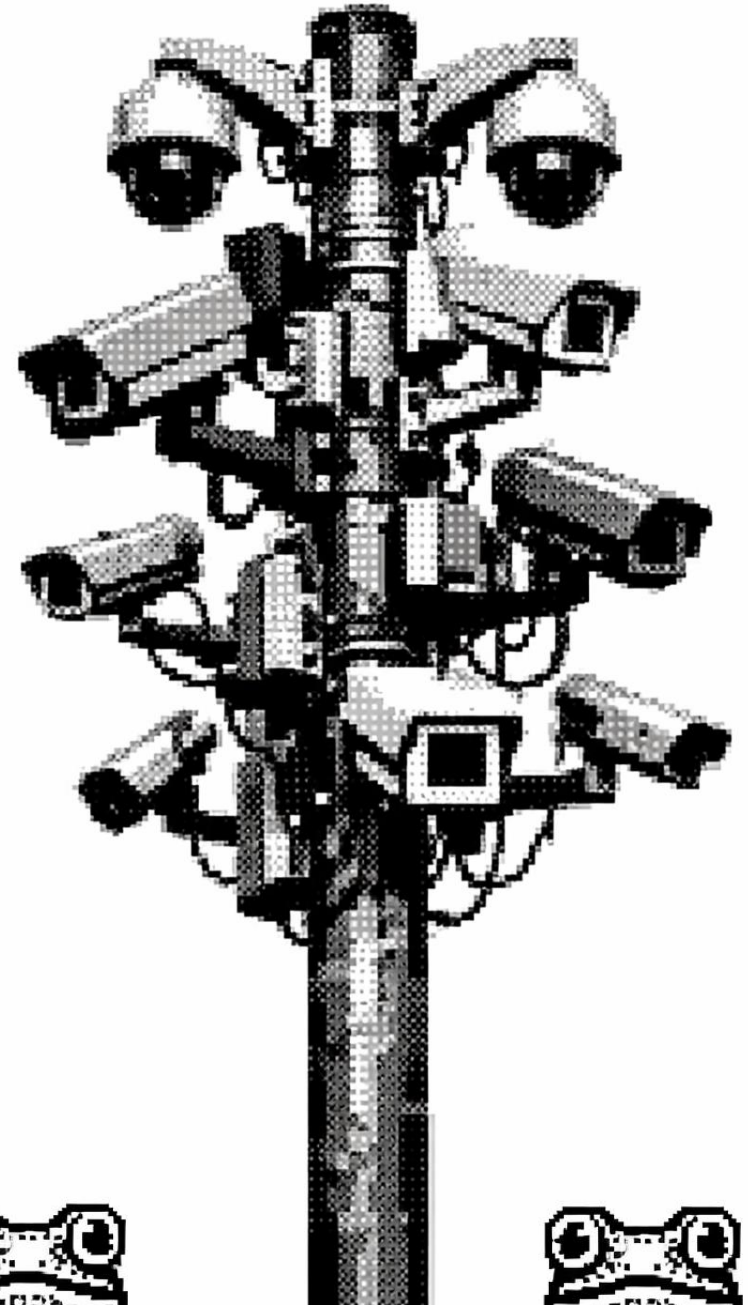
https://www.lucyparsonslabs.com/

https://citizenlab.ca/

https://www.pilsendefenseaccess.com/

https://www.cape.co/

https://efforg.github.io/rayhunter/



CRIMINAL JUSTICE, LAW ENFORCEMENT, LOCAL LAW ENFORCEMENT, MILITARIZATION OF POLICE, SURVEILLANCE AND PRIVACY

# Chicago and Los Angeles have used 'dirt box' surveillance for a decade

part of the largest police department in the United States. During a recent panel, New York City Police Commissioner William Bratton declared that predictive policing "is the wave of the future," and that "the 'Minority Report' of 2002 is the reality of today."

New York police are "data mining huge amounts of information and developing algorithms that will effectively mine that data in many ways the human brain cannot," said Bratton, referring to the department's trawling of social media and crime data, as

https://revealnews.org/article/chicago-and-los-angeles-have-used-dirt-box-surveillance-for-a-decade/

# $why

*..”what does it take for people to recognize a dystopia.. I kinda feel like it backfired”*

*-Jaron Lanier*

*2019 NYT interview*

*‘Jaron Lanier Fixes The Internet’*

Jaron Lanier Fixes the Internet

# Aurora police settle with Colorado woman for $1.9M after video of her and kids held at gunpoint went viral

By Austen Erblat

Updated on: February 5, 2024 /

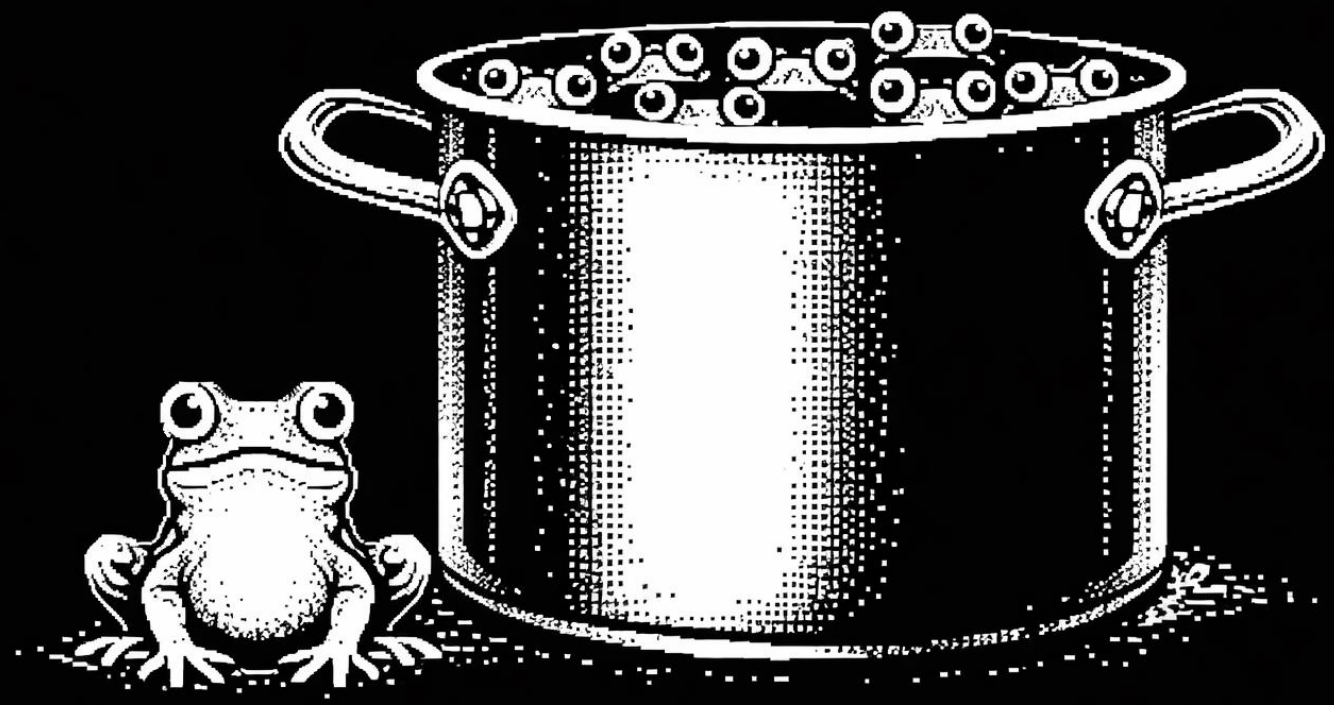
BY LUCAS ROPEK PUBLISHED OCTOBE

“It was like eight cop cars t

they were going until they

‘Get on the ground,’ and I w

Updated August 17, 2024 12:30 PM



# $Thank you

dreadloc__

# $Ref

1. Phone stats
2. DOJ use of CSS
3. DOJ FDS Contract
4. Gerogetown Facial Study
5. ICE PARAGON Contract
6. Graphite Jounalists
7. Cellular Bootstrapping
8. Gotta Catch’em All
9. Rayhunter Devices
10. Jacobs Bid for Mass State PD
9. Upenn Mobile Security
10. Rochester PD CSS financials
11. CAPE work on CSS
12. EFF pcaps slds 33-37
13. Garner Protest Surveillance
14. FDS Chino PD Pitch
15. Bratton – Minority Report
16. Gainsec – Root Shell
17. Gainsec – Feed intercept
18. 404 media on flock PTZs

# $Ref(cont'd)

18. Benn Jordan - Flock PTZ
19. Staunton Va - Cancels flock contract
20. Police Chief Flock Stalker
21. Kansas PD Officer Stalking
22. Menasha Stalker
23. Flock Healthcare search
24. Misidentified Aurora Vehicle
25. Baltimore School Ai Incident