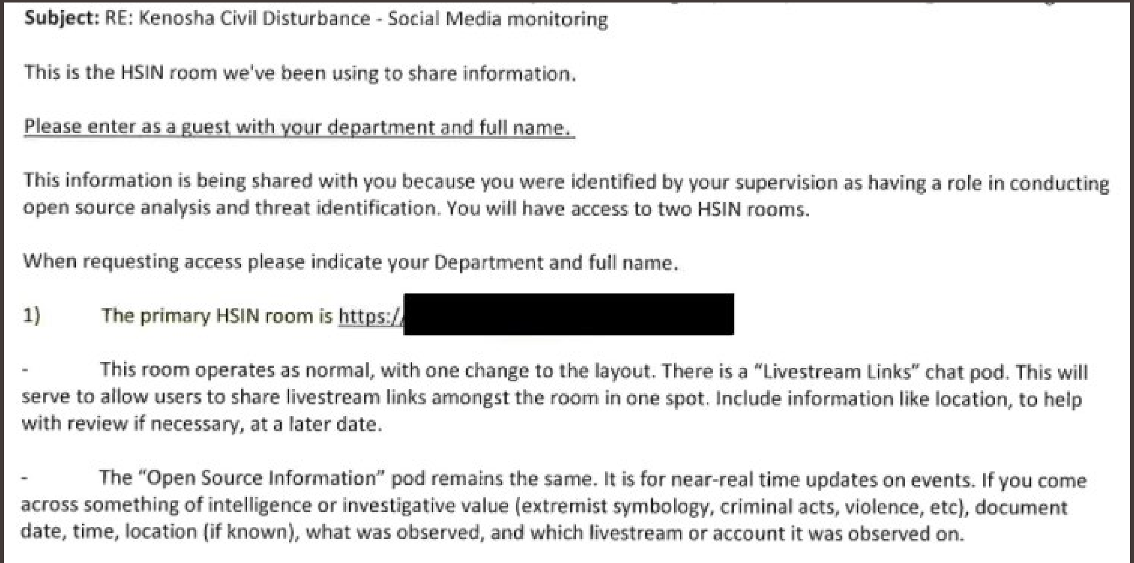
Technology Surveillance of Protesters

ACLU

How law enforcement uses our cellphones against us

- Electronic surveillance used in Kenosha and elsewhere in Wisconsin during 2020 protests:
  - Social media monitoring
  - Cellphone seizures
  - Geofencing warrants
- Other surveillance tactics that may have been used or could be used in the future:
  - Cell site simulators
  - Cell phone location tracking
  - Spyware

Our investigation showed that local and federal law enforcement agencies set up a social media monitoring site to surveil activities in Kenosha.



Subject: RE: Kenosha Civil Disturbance - Social Media monitoring

This is the HSIN room we've been using to share information.

Please enter as a guest with your department and full name.

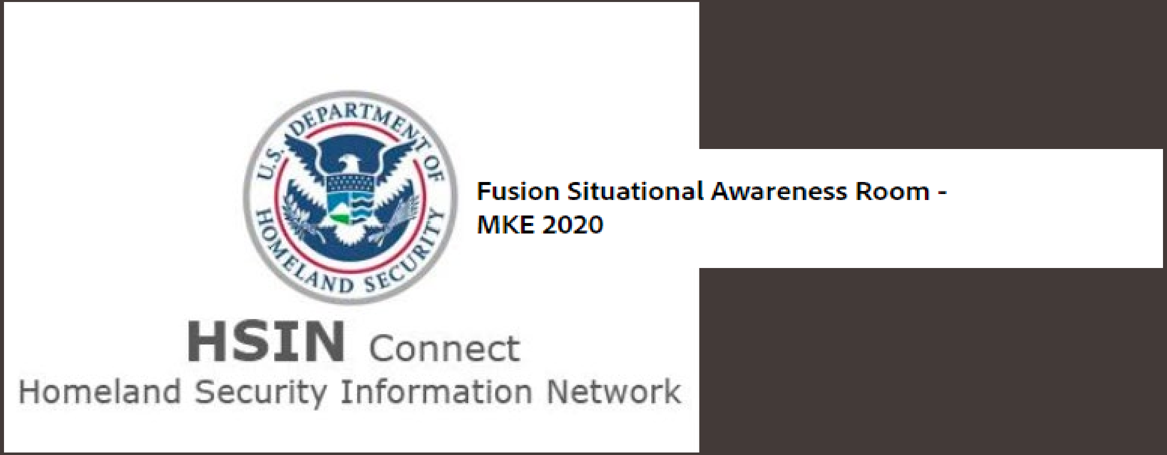
This information is being shared with you because you were identified by your supervision as having a role in conducting open source analysis and threat identification. You will have access to two HSIN rooms.

When requesting access please indicate your Department and full name.

1) The primary HSIN room is https:/[redacted]

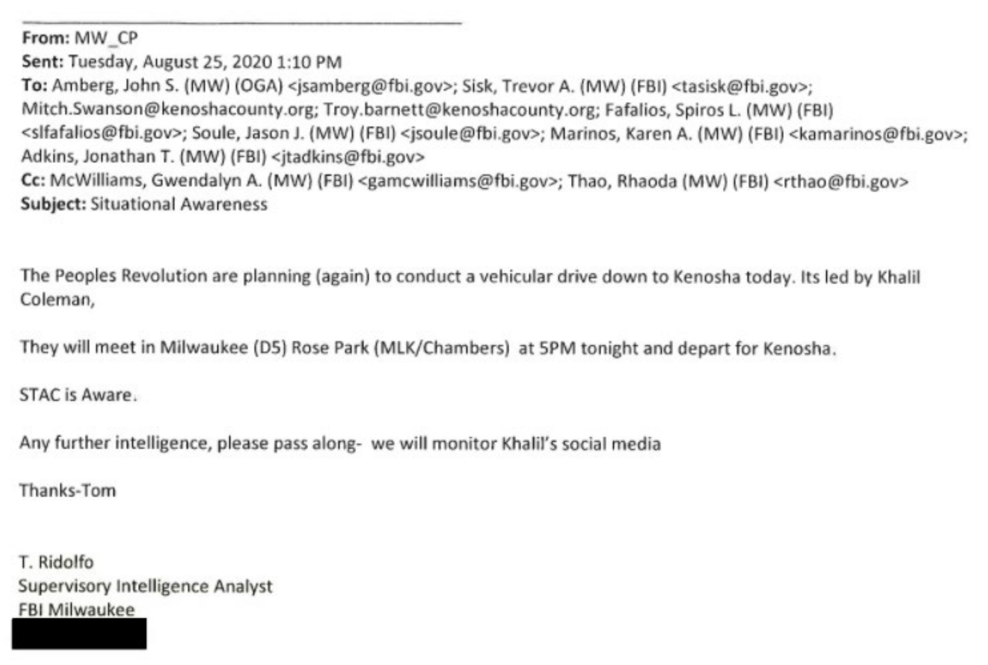
- This room operates as normal, with one change to the layout. There is a "Livestream Links" chat pod. This will serve to allow users to share livestream links amongst the room in one spot. Include information like location, to help with review if necessary, at a later date.

- The "Open Source Information" pod remains the same. It is for near-real time updates on events. If you come across something of intelligence or investigative value (extremist symbology, criminal acts, violence, etc), document date, time, location (if known), what was observed, and which livestream or account it was observed on.



Fusion Situational Awareness Room - MKE 2020

U.S. DEPARTMENT OF HOMELAND SECURITY
HSIN Connect
Homeland Security Information Network



From: MW_CP
Sent: Tuesday, August 25, 2020 1:10 PM
To: Amberg, John S. (MW) (OGA) <jsamberg@fbi.gov>; Sisk, Trevor A. (MW) (FBI) <tasisk@fbi.gov>; Mitch.Swanson@kenoshacounty.org; Troy.barnett@kenoshacounty.org; Fafalios, Spiros L. (MW) (FBI) <slfafalios@fbi.gov>; Soule, Jason J. (MW) (FBI) <jsoule@fbi.gov>; Marinos, Karen A. (MW) (FBI) <kamarinos@fbi.gov>; Adkins, Jonathan T. (MW) (FBI) <jtadkins@fbi.gov>
Cc: McWilliams, Gwendalyn A. (MW) (FBI) <gamcwilliams@fbi.gov>; Thao, Rhaoda (MW) (FBI) <rthao@fbi.gov>
Subject: Situational Awareness

The Peoples Revolution are planning (again) to conduct a vehicular drive down to Kenosha today. Its led by Khalil Coleman,

They will meet in Milwaukee (D5) Rose Park (MLK/Chambers) at 5PM tonight and depart for Kenosha.

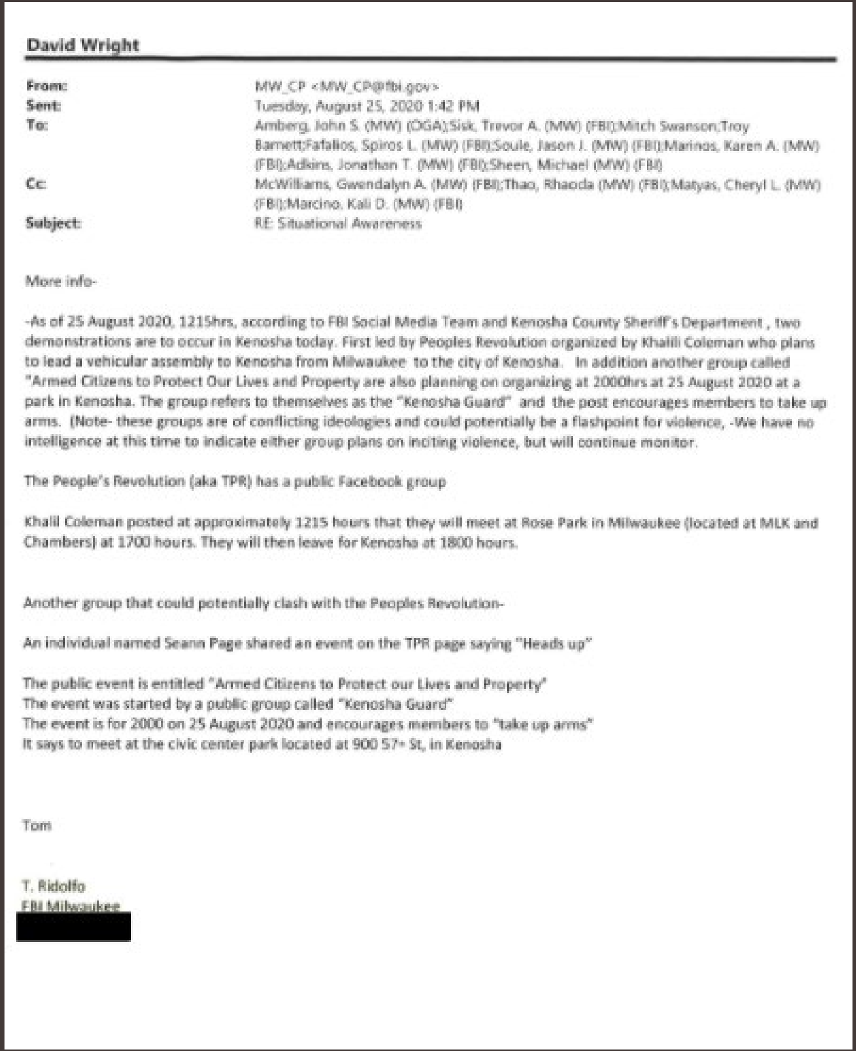
STAC is Aware.

Any further intelligence, please pass along- we will monitor Khalil's social media

Thanks-Tom

T. Ridolfo
Supervisory Intelligence Analyst
FBI Milwaukee
[redacted]

The Peoples Revolution appeared to be of particular interest to the FBI and Kenosha Sheriff



David Wright

From: MW_CP <MW_CP@fbi.gov>
Sent: Tuesday, August 25, 2020 1:42 PM
To: Amberg, John S. (MW) (OGA);Sisk, Trevor A. (MW) (FBI);Mitch Swanson;Troy Barnett;Fafalios, Spiros L. (MW) (FBI);Soule, Jason J. (MW) (FBI);Marinos, Karen A. (MW) (FBI);Adkins, Jonathan T. (MW) (FBI);Sheen, Michael (MW) (FBI)
Cc: McWilliams, Gwendalyn A. (MW) (FBI);Thao, Rhaoda (MW) (FBI);Matyas, Cheryl L. (MW) (FBI);Marcino, Kali D. (MW) (FBI)
Subject: RE: Situational Awareness

More info-

-As of 25 August 2020, 1215hrs, according to FBI Social Media Team and Kenosha County Sheriff's Department , two demonstrations are to occur in Kenosha today. First led by Peoples Revolution organized by Khalil Coleman who plans to lead a vehicular assembly to Kenosha from Milwaukee to the city of Kenosha. In addition another group called "Armed Citizens to Protect Our Lives and Property are also planning on organizing at 2000hrs at 25 August 2020 at a park in Kenosha. The group refers to themselves as the "Kenosha Guard" and the post encourages members to take up arms. (Note- these groups are of conflicting ideologies and could potentially be a flashpoint for violence, -We have no intelligence at this time to indicate either group plans on inciting violence, but will continue monitor.

The People's Revolution (aka TPR) has a public Facebook group

Khalil Coleman posted at approximately 1215 hours that they will meet at Rose Park in Milwaukee (located at MLK and Chambers) at 1700 hours. They will then leave for Kenosha at 1800 hours.

Another group that could potentially clash with the Peoples Revolution-

An individual named Seann Page shared an event on the TPR page saying "Heads up"

The public event is entitled "Armed Citizens to Protect our Lives and Property"
The event was started by a public group called "Kenosha Guard"
The event is for 2000 on 25 August 2020 and encourages members to "take up arms"
It says to meet at the civic center park located at 900 57th St, in Kenosha

Tom

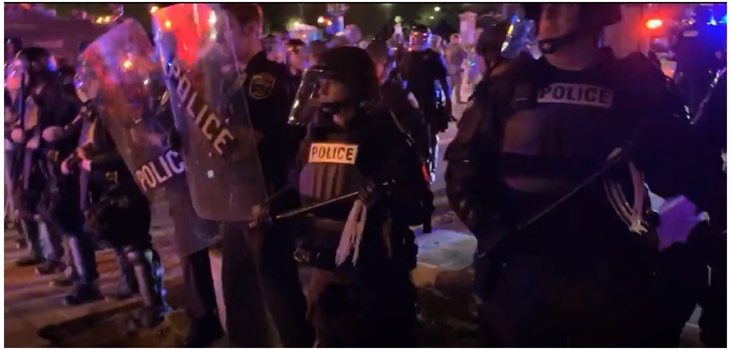
T. Ridolfo
FBI Milwaukee
[redacted]

Cellphone Seizures

- Cellphones were confiscated during the George Floyd protests in Milwaukee, protests in Wauwatosa, and the Kenosha.
- Protesters arrested during protests regularly reported that their cell phones were not immediately returned to them after their release.
- Police need a warrant to search your cellphone. You should not consent.
- Companies like Cellbrite and Greysmith sell law enforcement tools to crack encryption on cellphones to extract data.

Police took and kept cellphones of arrested protesters.

Ryan Clancy, Milwaukee County Supervisor and ACLU of Wisconsin Legal Observer, describes how police persuaded him to give up the contents of his cell phone after his arrest during a George Floyd protests in Milwaukee. He also says there were unexplained disruptions to cellphone apps during the protests.

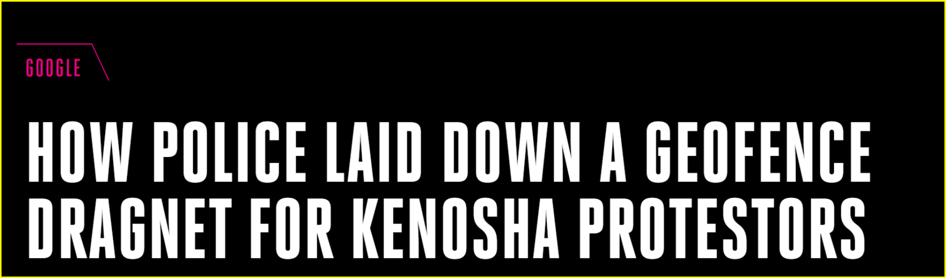


https://youtu.be/n5iGkdoNfBU

Reporting at The Verge has revealed that law enforcement used geofencing warrants sent to Google as part of investigations into 2020 events in Kenosha.

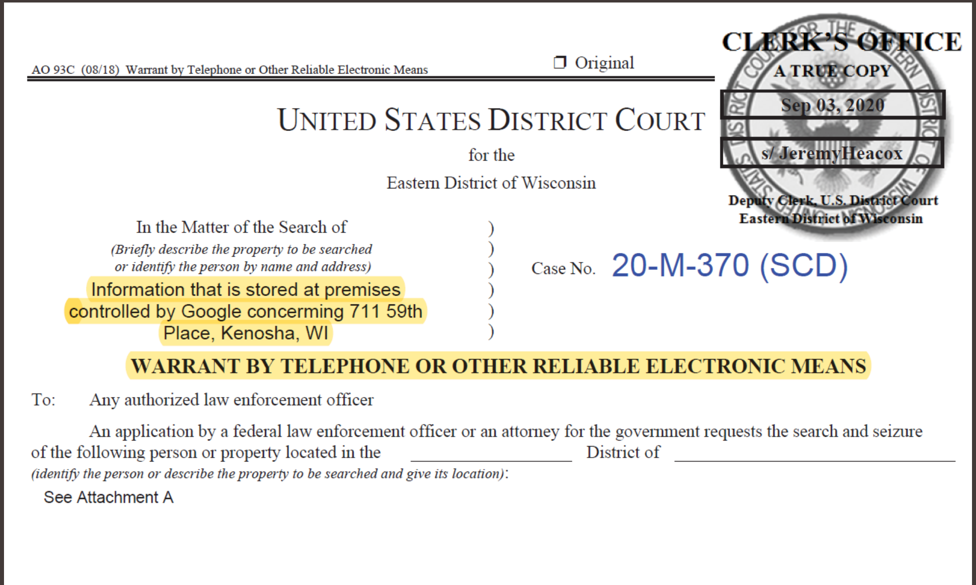
A geofencing warrant asks Google to identify all devices that were within a specific geographic space during a specified time period, such as when a fire broke out.

In one warrant "police set a two-hour window and a geofence covering the middle third of the downtown's largest public park space. It was a significant span of time on the busiest night of the protest in an area that provided a natural meeting place for anyone who had taken to the streets that night."



GOOGLE

HOW POLICE LAID DOWN A GEOFENCE DRAGNET FOR KENOSHA PROTESTORS



AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original

CLERK'S OFFICE
A TRUE COPY
Sep 03, 2020
s/ JeremyHeacox
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Information that is stored at premises)
controlled by Google concerning 711 59th)
Place, Kenosha, WI)

Case No. 20-M-370 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

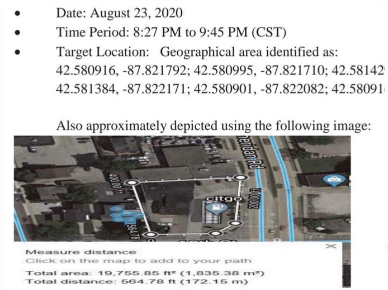
An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the ____________ District of ____________________
(identify the person or describe the property to be searched and give its location):

See Attachment A

https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake

Where did law enforcement use geofence warrants in Kenosha in 2020?

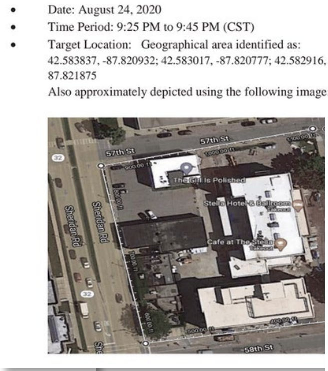
- Multiple geofence warrants for areas near protests, including the Dinosaur Museum, Library Park, and businesses along Sheridan Road.



- Date: August 23, 2020
- Time Period: 8:27 PM to 9:45 PM (CST)
- Target Location: Geographical area identified as: 42.580916, -87.821792; 42.580995, -87.821710; 42.58142 42.581384, -87.822171; 42.580901, -87.822082; 42.58091

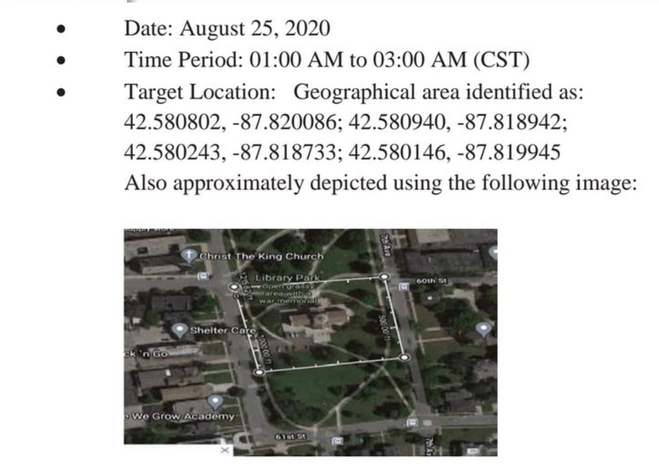
Also approximately depicted using the following image:

Measure distance
Click on the map to add to your path
Total area: 19,755.85 ft² (1,835.38 m²)
Total distance: 564.78 ft (172.15 m)



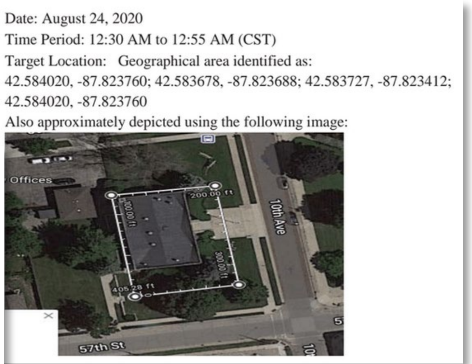
- Date: August 24, 2020
- Time Period: 9:25 PM to 9:45 PM (CST)
- Target Location: Geographical area identified as: 42.583837, -87.820932; 42.583017, -87.820777; 42.582916, -87.821706; 42.583713, -87.821875

Also approximately depicted using the following image:



- Date: August 25, 2020
- Time Period: 01:00 AM to 03:00 AM (CST)
- Target Location: Geographical area identified as: 42.580802, -87.820086; 42.580940, -87.818942; 42.580243, -87.818733; 42.580146, -87.819945

Also approximately depicted using the following image:



- Date: August 24, 2020
- Time Period: 12:30 AM to 12:55 AM (CST)
- Target Location: Geographical area identified as: 42.584020, -87.823760; 42.583678, -87.823688; 42.583727, -87.823412; 42.584020, -87.823760

Also approximately depicted using the following image:

Stingrays – Cell Site Simulators

- Cell phone signals typically go through a tower operated by your cellphone company, but with a cell site simulator, signals go through a "stingray" operated by law enforcement.
- Federal and Wisconsin law enforcement have and use these systems.
- With a stingray, law enforcement can track the location of a cellphone, listen to unencrypted conversation, read unencrypted text messages, and more.

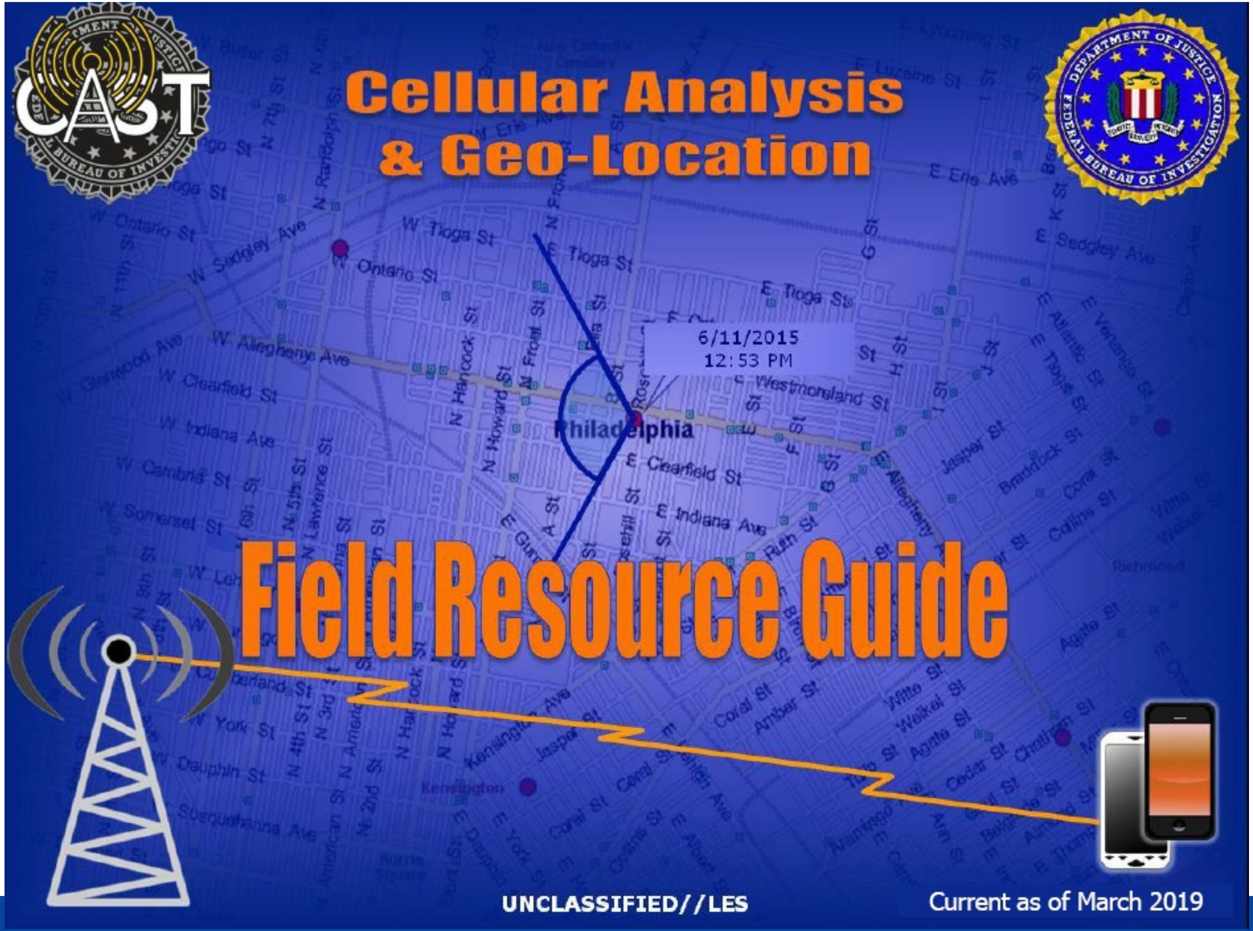
Stingrays – Cell Site Simulators

- The actual capabilities of current cell site simulators are a closely held secret by law enforcement and manufacturers, and vary depending on phone technology, the cell carrier, and type of simulator.
- Cell site simulators can potentially intercept real time unencrypted phone calls, text messages, instant messages, web browsing, video chat and more.
- For more information see www.eff.org/pages/cell-site-simulatorsimsi-catchers

Use of surveillance technology:

I. Federal and state law enforcement should not use the types of data gathering and surveillance techniques to track:
   A. the locations of protesters' cell phones
   B. Highly sensitive and personal conversations
   C. Text messages
   D. Metadata

The FBI conducts regular training for law enforcement about cell phone systems.

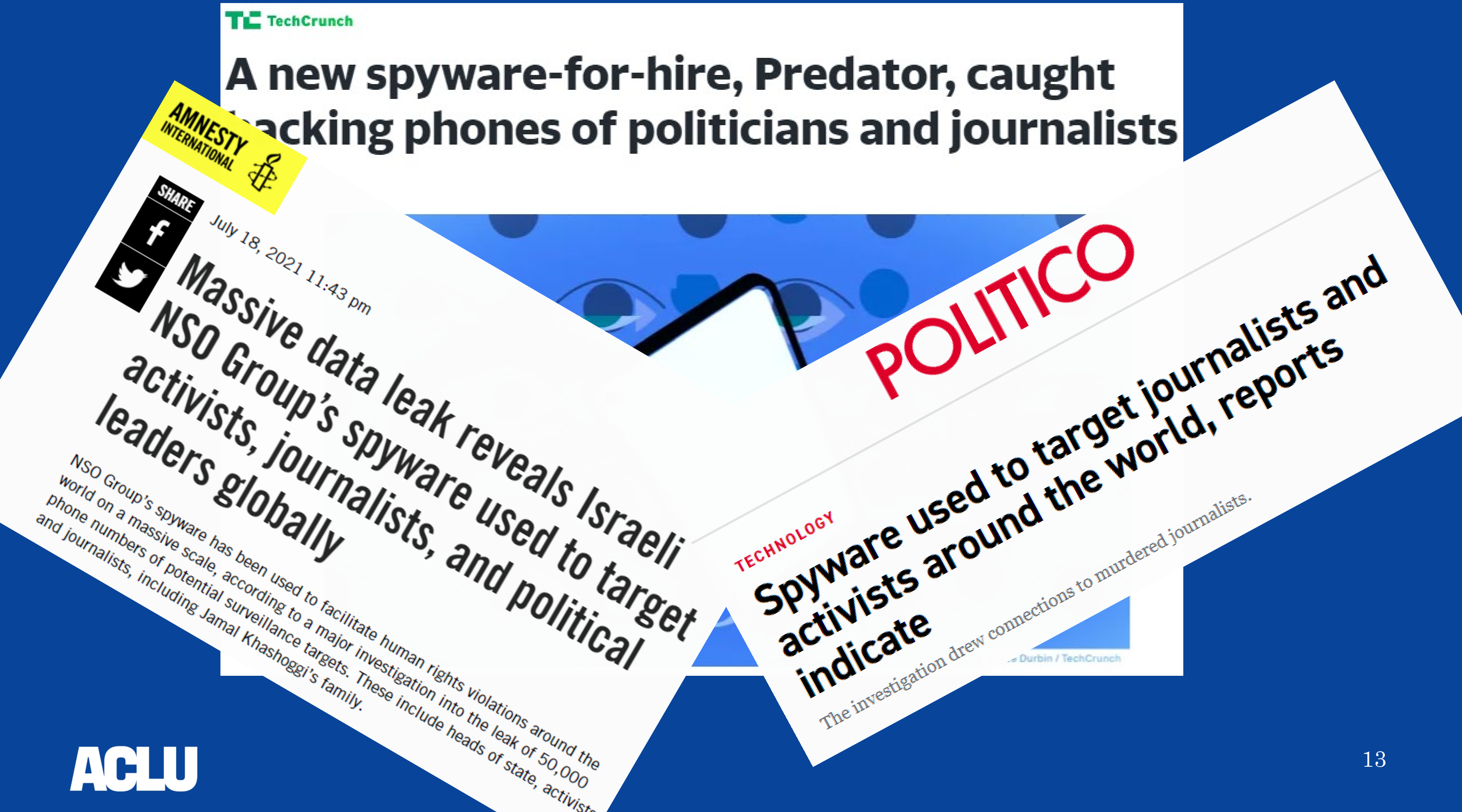


Cellular Analysis & Geo-Location

Field Resource Guide

UNCLASSIFIED//LES

Current as of March 2019



TechCrunch

A new spyware-for-hire, Predator, caught hacking phones of politicians and journalists

AMNESTY INTERNATIONAL

July 18, 2021 11:43 pm

Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally

NSO Group's spyware has been used to facilitate human rights violations around the world on a massive scale, according to a major investigation into the leak of 50,000 phone numbers of potential surveillance targets. These include heads of state, activists and journalists, including Jamal Khashoggi's family.

POLITICO

TECHNOLOGY

Spyware used to target journalists and activists around the world, reports indicate

The investigation drew connections to murdered journalists.

a Durbin / TechCrunch

Before attending a protest:

- Consider not taking your phone.
- Make sure your phone is encrypted and password protected with the latest updates to operating system.
- Use a numerical PIN and turn off facial recognition and thumb print.
- Use encrypted communication apps like Signal or Telegram for calls or texts.
- Turn off location services and Wi-Fi when not in use.
- Use a VPN when using public Wi-Fi.

At a protest:

- Be conscious of your privacy settings for streaming, photo posting, or sharing what you are doing.
- Remember if you are livestreaming to a public social media account (i.e. Facebook or Instagram), you are providing information to enforcement who may monitor your stream.
- Consider recording to your device rather than livestreaming.
- If you do decide to stream, use the ACLU Mobile Justice app.
- Avoid taking photos of protester's faces without their consent.

If police take your phone:

- Cell phones can only be searched with a warrant, or your consent, but there is evidence that police attempt to view the contents of phones without warrants.
- If asked, never consent to have your phone reviewed.
- If your phone is kept after arrest and release, immediately send written demand that it be returned, including another statement that you object to the search of your phone.

Avoiding spyware:

- Never click on links from people you don’t know.
- Never click on unexpected links from people you do know.
- Most spyware comes through attachments – to an instant message or a WhatsApp or Facebook chat. Don’t open if you are uncertain of the source.
- Power phone all the way off and restart on a regular basis. This can remove some types of spyware from the phone’s memory.

ACLU

WE THE PEOPLE