Surveillance, Data, and Privacy in Cellular Networks

Robert Liu ’20, November 15th 2021

Disclaimer

- These are strictly my personal views and not those of any employer, past, present, or future

What does surveillance look like?

Twin Cities man found guilty in hit-and-run crash that killed 2 men nearly 8 years ago

The men were struck while fighting in a road in western Wisconsin, authorities said.

By Paul Walsh Star Tribune | NOVEMBER 12, 2021 — 7:34AM

A Twin Cities man has been found guilty in a hit-and-run crash that killed two men nearly eight years ago in western Wisconsin.

Andrew M. Endres, 33, of Randolph, pleaded no contest this week in Polk County Circuit Court to two counts of hit and run resulting in death in connection with the crash on Jan. 11, 2014, that killed Richard L. Cobenais Jr., 41, who lived near Luck, Wis., and Benjamin R. Juarez, 28, of Frederic, Wis.

Endres, who was a longtime firefighter in his community, remains free on bond ahead of sentencing scheduled for Jan. 18.

Cobenais and Juarez were struck by a pickup truck and killed shortly before 6:30 p.m. along County Road E, northeast of Balsam Lake. The two had been at a home and got into a fight that spilled into the road, where they were struck, according to the Sheriff's Office.

[redacted]

On Sept. 28, 2020, a man called the Sheriff's Office and said his estranged wife heard Endres say he ran over the two men and was drunk at the time, the charges against him read. A law enforcement search of Endres' cellphone revealed that he was in the area less than five hours before the collision and until late the next morning before heading back to Minnesota, the charges continued.

About two weeks later, the pickup was located in Crow Wing County under new ownership and seized by law enforcement.

Paul Walsh • 612-673-4482

[redacted]

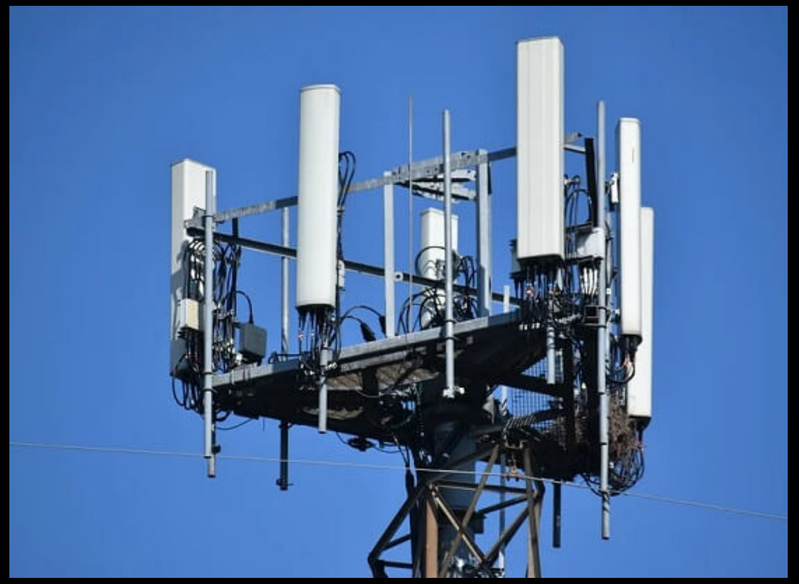
UNCLASSIFIED//LES

Provider Retention Periods

(As of March 2019)

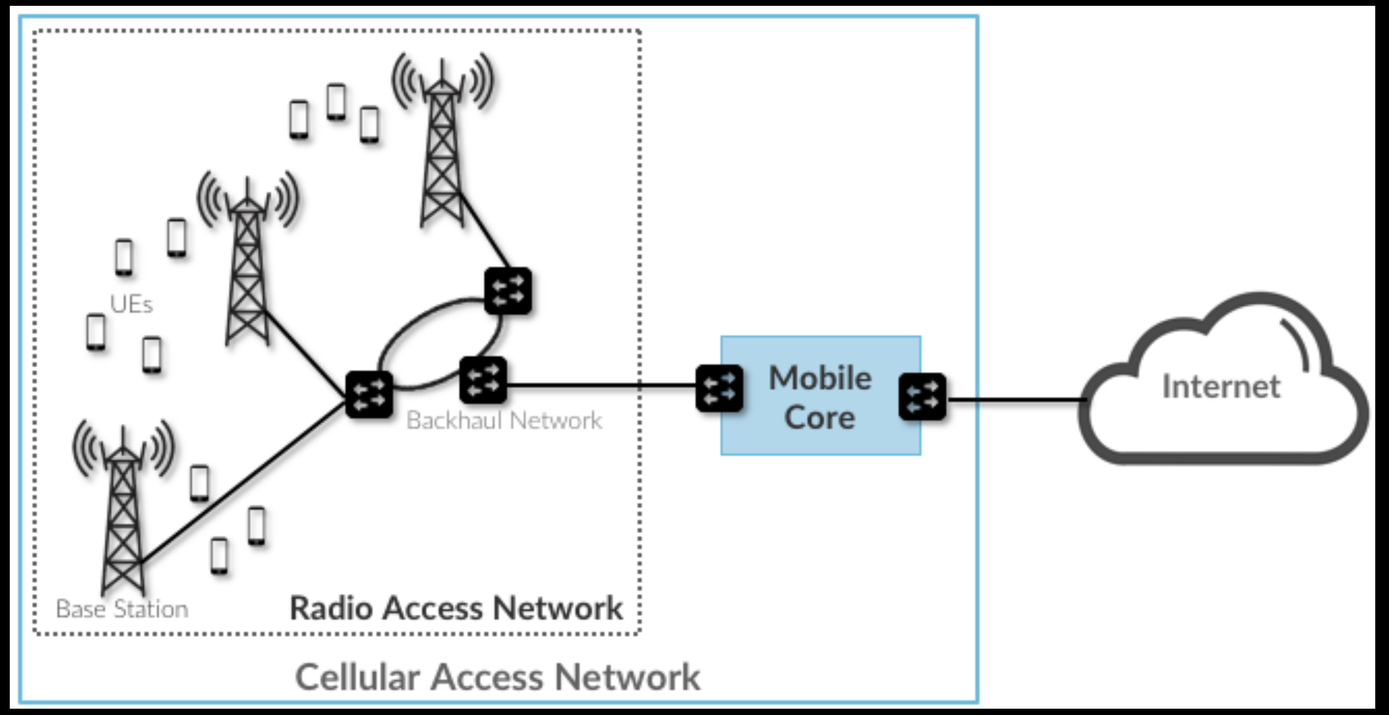
Provider	AT&T	Cricket (AT&T)	T-Mobile	MetroPCS (T-mobile)	Sprint	Verizon	US Cellular
Subscriber	7 years	12/20/2015-present	2 years prepaid; since account opened with postpaid	2 years	10 years	3-5 years	7 years
Call Detail Records	7 years	12/20/2015-present	2 years prepaid; since account opened with postpaid	2 years	18 months; backup tapes available 2005 to present	1 year	1 year
Cell Site (Voice)	7 years	12/20/2015-present	2 years	2 years	18 months	1 year	1 year
SMS tolls	7 years	12/20/2015-present	2 years	2 years	18 months	1 year	1 year
Cell Site (SMS)	7 years	12/20/2015-present	2 years	2 years	No CDR, Yes Reveal (PCMD) for 90 days	No CDR, Yes RTT (PCMD) 8-30 days	No
SMS content	No (AT&T msg app 90 days; ~10%)	No	No	No	Only on T-III	7 days	3-5 days
Cell Site (Data)	7 years	12/20/2015-present	No	No	90 days (if request IPDR Report)	1 year	No
Tower Dumps	7 years	12/20/2015-present	2 years	2 years	18 months	1 year	1 year
Prospective	Mobile Locate (Triangulation / AGPS)	Mobile Locate (Triangulation / AGPS)	E911 (Triangulation)	No	GPS "Ping" (device dependent)	Yes	No, but force "no ring" call
PCMD/RTT (Historic)	No, but NELOS (90 days)	No, but NELOS (90 days)	No	No	PCMD (~90 days SMS & voice; 2 weeks data)	RTT 8 days	PCMD (30 days)
WiFi Calling	Pending	Pending	App / Open WiFi	No	18 months	On VoLTE report only	No
VoLTE	Yes	Yes	Yes since account opened	No	Yes 90 days	Yes 1 year	Yes 1 year
Store Video	Yes	Yes	15-45 days (sbp)	15-45 days (sbp)	2-3 months (sbp)	30 days (sbp)	30-60 days (sbp)
Voicemail	Yes- all stored VMs	Yes- all stored VMs	14 days	14 days	20 days	No	No
Cloud Storage	AMS	AMS				Via Synchronoss	
Internet/Web Browsing	1 year	1 year	No	No	No	187 days	No

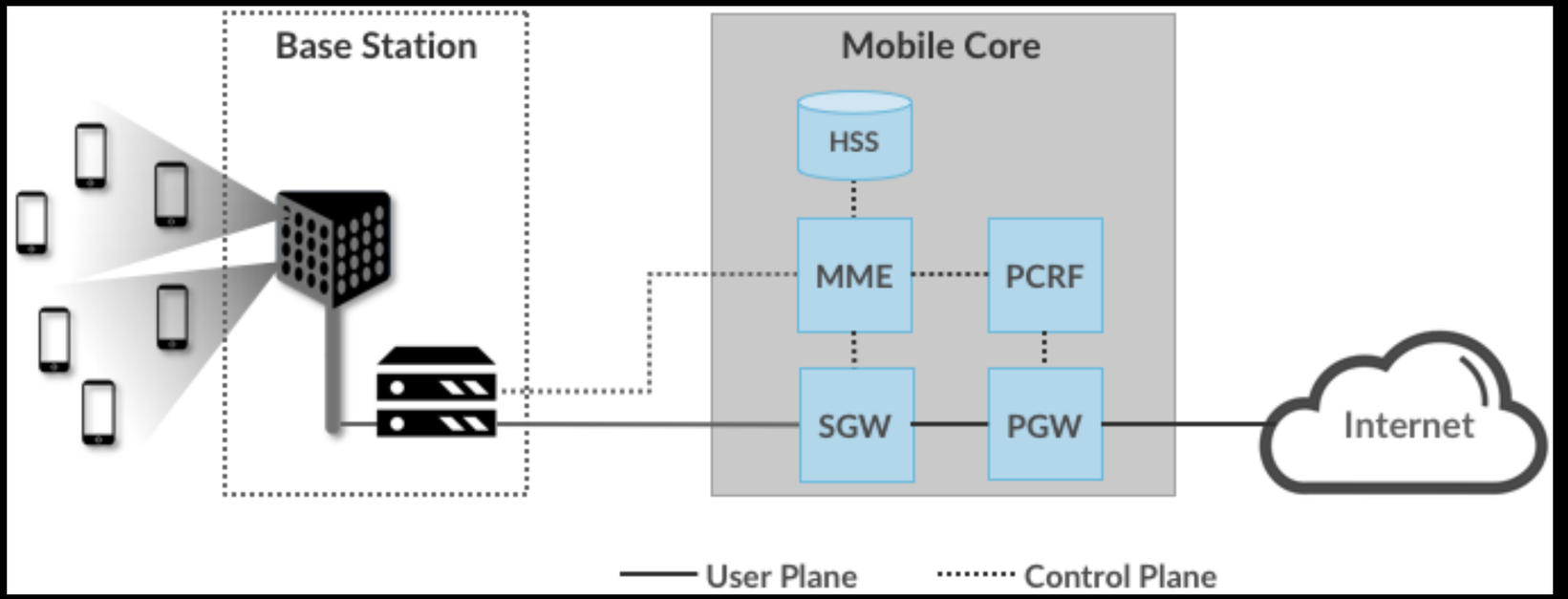
UNCLASSIFIED//LES



Telco Evolutions

- Manual -> electronic switching
- Switched network -> packet-based network
- Static phones -> mobile devices
- 1G to 5G: Analog to digital and packet-only standards
- 5G: More towers, better throughput


UEs
Backhaul Network
Mobile Core
Internet
Base Station
Radio Access Network
Cellular Access Network


Base Station
Mobile Core
HSS
MME
PCRF
SGW
PGW
Internet
User Plane
Control Plane

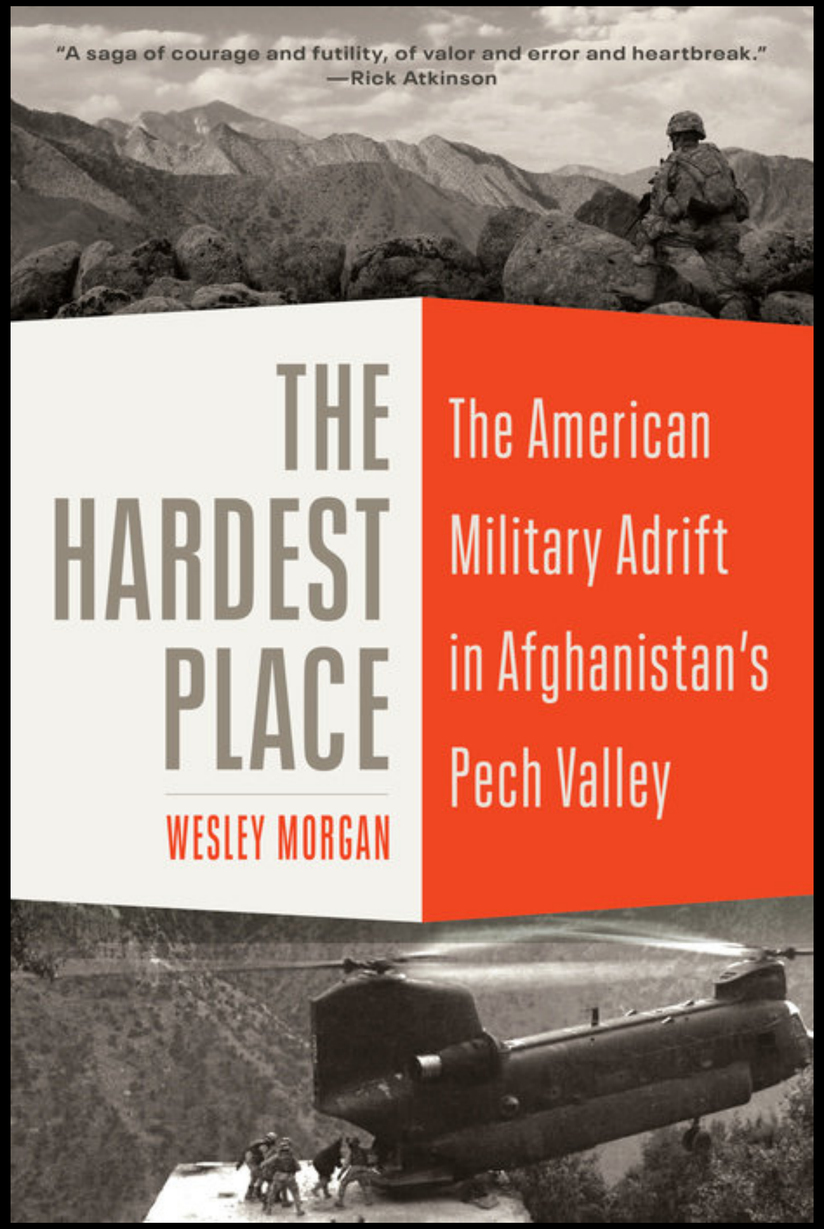
You’re already pwned

- Govs require telcos to implement lawful intercept capability for calls and data
- Identity: All cellular devices are traceable through providers’ subscriber DBs
- Those DBs contain your IMSI, name, address, and billing info
- Location: IP geolocation, WiFi fingerprinting, cell site simulation, telco data collection
- Relationships: network analysis on telco location data, social media, etc.

Who’s doing the surveilling?

Foreign Surveillance

- Satellite and cell phone surveillance, Kunar Province, Afghanistan
- Operation Haymaker: JSOC drone campaign in Kunar
- Lawful Intercept Section, National Directorate of Security, Afghanistan



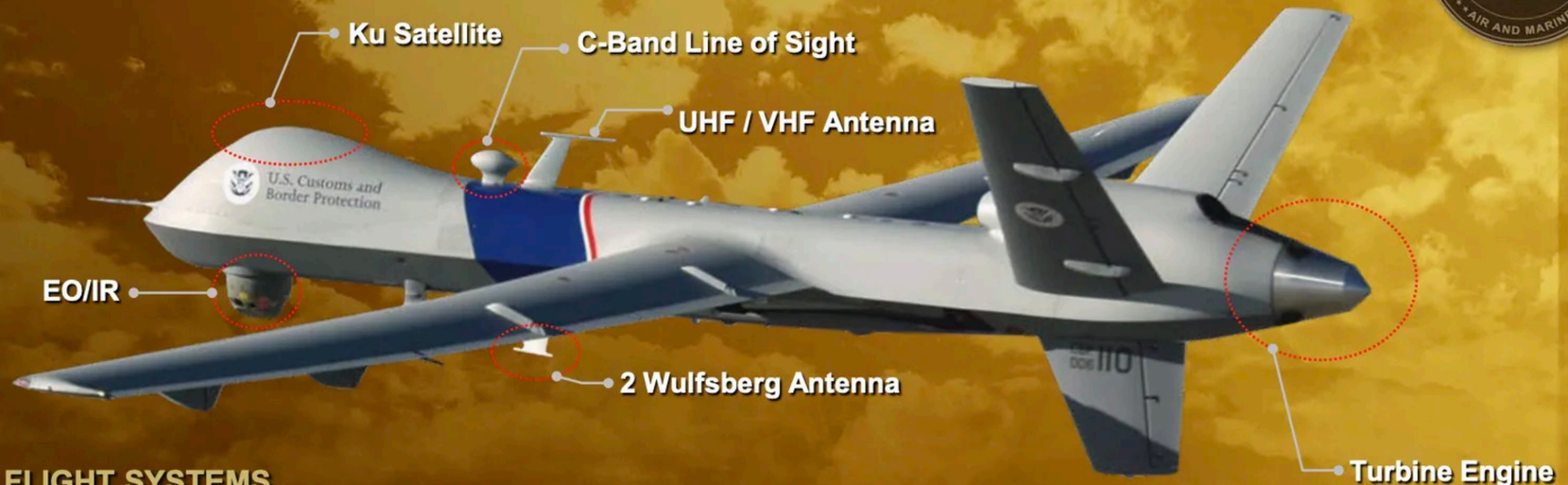
What goes around, comes around.

Domestic Surveillance

- George Floyd riots, Minneapolis, May 2020.
- Capitol riot, January 6 2021.


U.S. Customs and
Border Protection

Air and Marine Predator B



PROVEN FLIGHT SYSTEMS

- Predator family of aircraft flown by USAF more than 18 years and 2,000,000 hours
- More than 10,000 hours in border Security / Homeland Security role

MTS-B EO/IR IMAGE

LYNX SAR IMAGE

PREDATOR

- Wing Span: 66 ft
- Length: 36 ft
- Max Takeoff Weight: 10,500 lb

PERFORMANCE

- Range: Up to 3200 nm
- Max Demonstrated Endurance: 21 hrs
- Air Speed Max / Transit / Loiter: 240+ / 180 / 110 kts

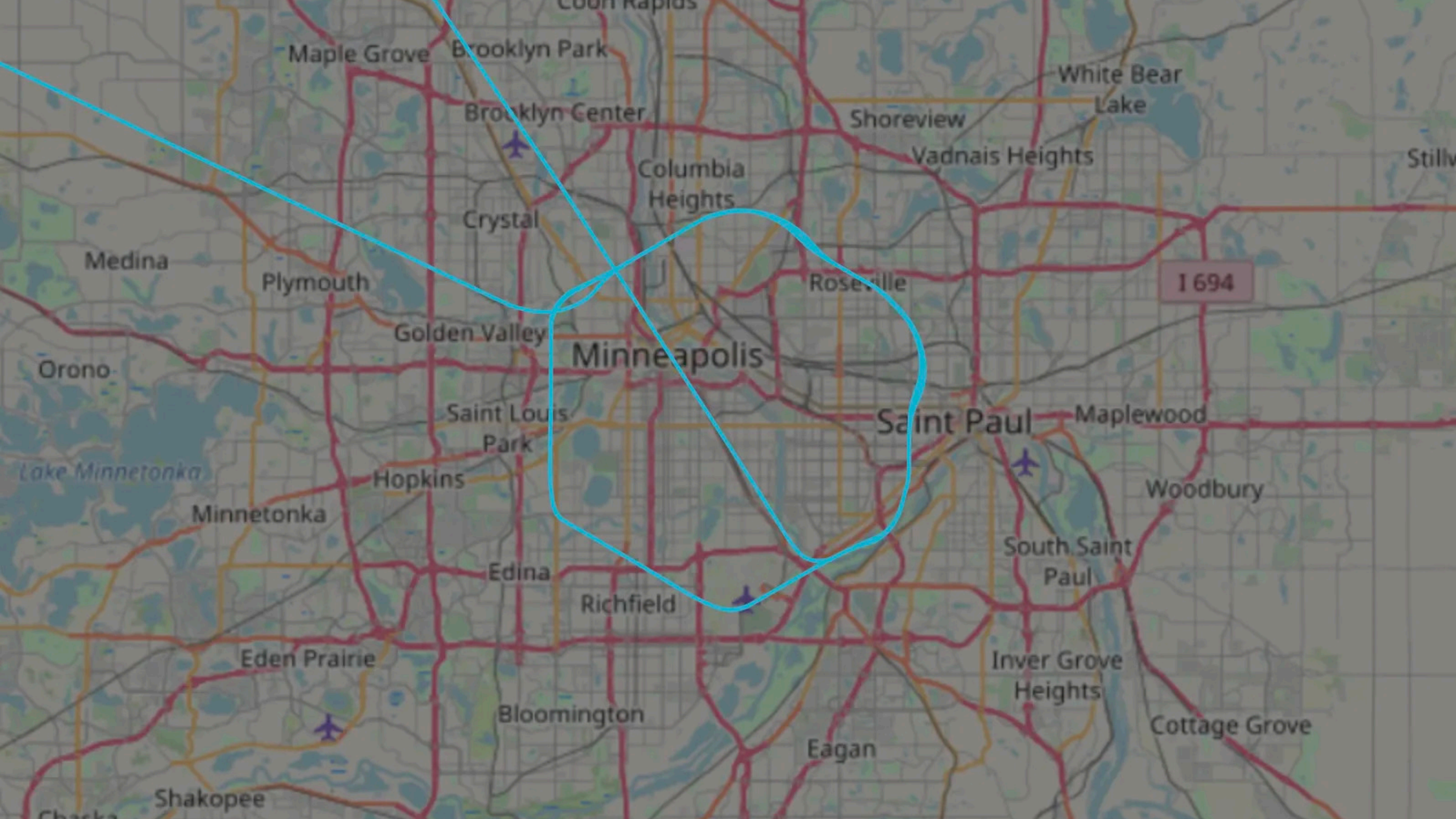
PAYLOADS:

- Multi-Spectral Targeting System (MTS-B) EO/IR
- Lynx Synthetic Aperture Radar (SAR)
- Law enforcement and civilian communications (UHF/VHF)
- Ku-band / Iridium satellite communications links

OPERATIONAL AIRCRAFT

- CBP 104, CBP 108, CBP 110, CBP 119, CBP 125

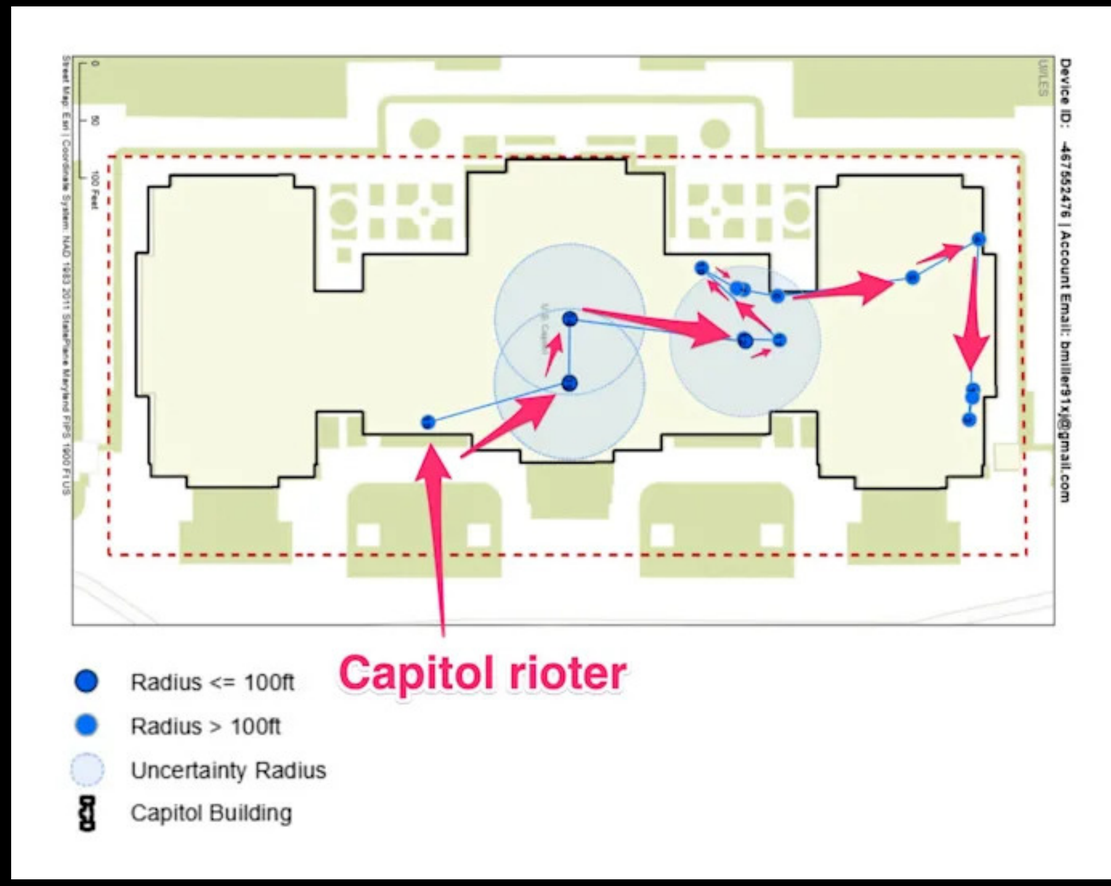
U.S. Customs and Border Protection


Maple Grove
Brooklyn Park
Brooklyn Center
White Bear Lake
Shoreview
Vadnais Heights
Columbia Heights
Crystal
Medina
Plymouth
Roseville
I 694
Golden Valley
Minneapolis
Orono
Saint Louis Park
Saint Paul
Maplewood
Lake Minnetonka
Hopkins
Minnetonka
Woodbury
South Saint Paul
Edina
Richfield
Eden Prairie
Inver Grove Heights
Bloomington
Cottage Grove
Eagan
Shakopee

According to records obtained through a search warrant which was served on Google, a mobile device associated with bmiller91xj@gmail.com was present at the U.S. Capitol on January 6, 2021. Google estimates device location using sources including GPS data and information about nearby Wi-Fi access points and Bluetooth beacons. This location data varies in its accuracy, depending on the source(s) of the data. As a result, Google assigns a "maps display radius" for each location data point. Thus, where Google estimates that its location data is accurate to within 10 meters, Google assigns a "maps display radius" of 10 meters to the location data point. Finally, Google reports that its "maps display radius" reflects the actual location of the covered device approximately 68% of the time. In this case, Google location data shows that a device associated with bmiller91xj@gmail.com was within the U.S. Capitol at the locations show in the map below, with the "maps display radius" reflected on the accompanying chart.

On or about February 6, 2021, AT&T provided access to records responsive to legal process regarding phone numbers (***) ***-5898 and (***) ***-6025. The numbers were subscribed to Stephanie Nisonger at their address in Bradford, Ohio and email address snisonger.1012@gmail.com.

According to records obtained through a search warrant which was served on AT&T on January 6, 2021, in and around the time of the incident at the U.S. Capitol Building, the cellphones associated with phone numbers (***) ***-5898 and (***) ***-6025 were identified as having utilized a cell site consistent with providing service to a geographic area that included the interior of the U.S. Capitol Building.



Is there a solution?

A Private and Secure Telco

- Own your own infrastructure: HW, SW, and data links
- Keep as little data as possible
- Avoid prosecution from all Earthly gov’ts
- ???
- Profit!

The Prime Suspect?


STARLINK

Questions?

Sources

- Cox, Joseph. (2021, October 25). *Here's the FBI's Internal Guide for Getting Data from AT&T, T-Mobile, Verizon.* Motherboard.
- Hall, Madison. (2021, March 24). *The DOJ is creating maps from subpoenaed cell phone data to identify rioters involved with the Capitol insurrection.* Business Insider.
- Morgan, Wesley. (2021). Haymaker: 2011-2013. In *The Hardest Place: The American Military Adrift in Afghanistan's Pech Valley.*
- Scahill, Jeremy and Glenn Greenwald. (2014, February 10). *The NSA's secret role in the U.S. assassination program.* The Intercept.

Sources (2)

- Walsh, Paul. (12 November 2021). *Twin Cities man found guilty in hit-and-run crash that killed 2 men nearly 8 years ago*. StarTribune.com.
- DrydenWire.com. (22 October 2020). *Charges Filed in Double-Fatal Hit-and-Run Cold Case.*
- BBC News. (13 October 2021). *Afghanistan: British trained intelligence unit officers ‘abandoned’ - BBC Newsnight*. YouTube.com.
- Schneier, Bruce. (11 February 2014). *Everything We Know About How the NSA Tracks People's Physical Location*. The Atlantic.

Sources (3)

- Heilweil, Rebecca. (10 June 2020). *Members of Congress want to know more about law enforcement's surveillance of protesters.* Vox.