Surveillance, Data, and Privacy in Cellular Networks
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.

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
### Provider Retention Periods

(As of March 2019)

<table>
<thead>
<tr>
<th>Provider</th>
<th>AT&amp;T</th>
<th>Cricket (AT&amp;T)</th>
<th>T-Mobile</th>
<th>MetroPCS (T-mobile)</th>
<th>Sprint</th>
<th>Verizon</th>
<th>US Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber</td>
<td>7 years</td>
<td>2 years prepaid; since account opened with postpaid</td>
<td>2 years</td>
<td>10 years</td>
<td>3-5 years</td>
<td>7 years</td>
<td></td>
</tr>
<tr>
<td>Call Detail</td>
<td>7 years</td>
<td>2 years prepaid; since account opened with postpaid</td>
<td>2 years</td>
<td>18 months; backup tapes available 2005 to present</td>
<td>1 year</td>
<td>1 year</td>
<td></td>
</tr>
<tr>
<td>Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Site (Voice)</td>
<td>7 years</td>
<td>2 years</td>
<td>2 years</td>
<td>1 months (PCMD)</td>
<td>1 year</td>
<td>1 year</td>
<td></td>
</tr>
<tr>
<td>(Voice)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS tolls</td>
<td>7 years</td>
<td>2 years</td>
<td>2 years</td>
<td>18 months</td>
<td>1 year</td>
<td>1 year</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Site (SMS)</td>
<td>7 years</td>
<td>2 years</td>
<td>No CDR, Yes Revealed (PCMD) for 90 days</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Data)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS content</td>
<td>7 years</td>
<td>2 years</td>
<td>No</td>
<td>No</td>
<td>Only on T-III</td>
<td>7 days</td>
<td>3-5 days</td>
</tr>
<tr>
<td>No (AT&amp;T msg app 90 days, -10%)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tower Dumps</td>
<td>7 years</td>
<td>2 years</td>
<td>2 years</td>
<td>18 months</td>
<td>1 year</td>
<td>1 year</td>
<td></td>
</tr>
<tr>
<td>Prospective</td>
<td>7 years</td>
<td>2 years</td>
<td>2 years</td>
<td>18 months</td>
<td>1 year</td>
<td>1 year</td>
<td></td>
</tr>
<tr>
<td>Mobile Locate</td>
<td>Mobile Locate (Triangulation / AGPS)</td>
<td>Mobile Locate (Triangulation / AGPS)</td>
<td>E911 (Triangulation)</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiFi Calling</td>
<td>Pending</td>
<td>Pending</td>
<td>App / Open WiFi</td>
<td>No</td>
<td>No</td>
<td>PCMD (90 days)</td>
<td></td>
</tr>
<tr>
<td>PCMD/RTT (Historic)</td>
<td>No, but NELOS (90 days)</td>
<td>No, but NELOS (90 days)</td>
<td>No</td>
<td>No</td>
<td>PCMD (8 days)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoLTE</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Volte</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Store Video</td>
<td>Yes</td>
<td>15-45 days (slp)</td>
<td>15-45 days (slp)</td>
<td>2-3 months (slp)</td>
<td>30 days (slp)</td>
<td>30-60 days (slp)</td>
<td>Via Synchronous</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Yes all stored VMs</td>
<td>Yes all stored VMs</td>
<td>14 days</td>
<td>14 days</td>
<td>20 days</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cloud Storage</td>
<td>AMS</td>
<td>AMS</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Internet/Web</td>
<td>1 year</td>
<td>1 year</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>187 days</td>
</tr>
</tbody>
</table>
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
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.
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

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
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 shown 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?
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.


Sources (2)


• Schneier, Bruce. (11 February 2014). Everything We Know About How the NSA Tracks People's Physical Location. The Atlantic.
Sources (3)