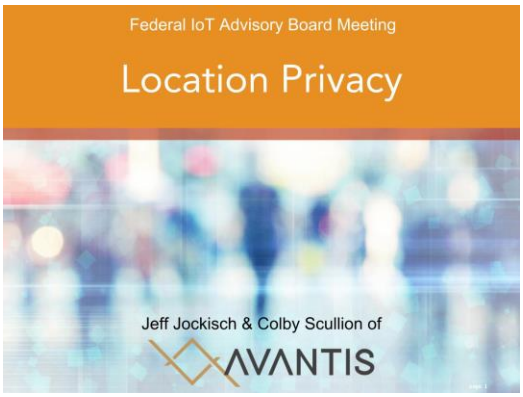
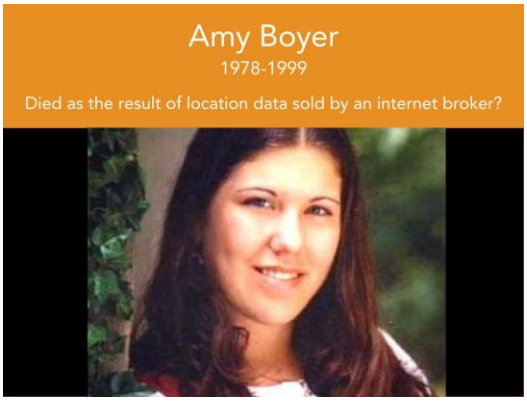
Federal IoT Advisory Board Meeting, 5/17/2023



Thank you for the invitation to be here today at this Federal IoT Advisory Board Meeting.

I'm Jeff Jockisch, Chief Privacy Officer of Avantis Privacy. My primary role is as data privacy researcher investigating data brokers.

I'm here with Colby Scullion, the CEO of Avantis. Well be tag-teaming this quick presentation on location privacy. Let's roll with the presentation.



Do you know who this is?
Amy Boyer died in 1999.

She is perhaps the first person to have died as the result of location data sold by an internet data broker.

A stalker Amy Boyer never met contacted Docusearch and requested info including the location of her employment. Docusearch charged him $109. A couple months later, he drove to Amy's workplace and fatally shot her as she left. https://archive.epic.org/privacy/boyer/

Our location problem hasn't gotten better since 1999. It's gotten worse.

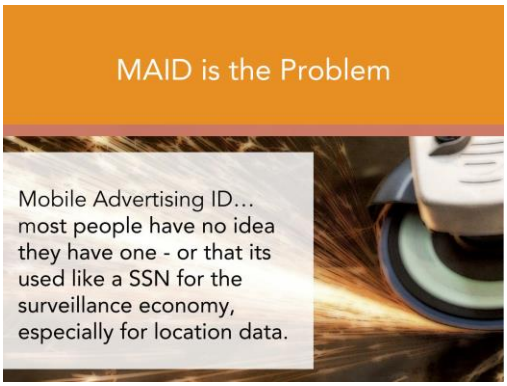
A 2019 investigation by Motherboard found that “AT&T, T-Mobile, Sprint, and Verizon were selling their customers' location data to data brokers, who would in turn provide it to bounty hunters with little oversight.” https://www.vice.com/en/article/8xwngb/t-mobile-put-my-life-in-danger-says-victim-of-black-market-location-data

Your phone leaks location data. Some of this leakage is based on the many technologies used to improve accuracy and triangulate your location. Many phones improve location accuracy by combining GPS, with Wi-Fi, and Bluetooth Low Energy technology.

A lot of this but not all, feeds into the advertising ecosystem.

Of course it's not simply your phone that leaks your location. Your car can do that as well, from onboard GPS, onboard wifi, and even your license plate. Automatic license plate readers are scooping up this info across the nation.

While there are many ways you can leak location data, the ones that most easily tie back to you are connected to your Mobile Advertising ID.



Most of the location leakage is tied to your MAID - Your Mobile Advertising ID. It's like a SSN you didn’t know you had.

Your SSN is linked to your credit history, so new creditors can use it to understand your financial profile.

Advertisers link everything possible to your Mobile Advertising ID, in part to serve you more and better ads.

But also to collect and sell that data to people who may have other purposes: people that want to
screen you,
influence you,
cheat you,
even harm you.

Mobile Advertising IDs track you
through Apps,
though Websites,
through Advertisements.

Every time you see an ad on your phone,
about 20 business received your location information
...because they bid on that ad space.

They see your data even if they don't win the bid. Isn't that strange?
An org might sit in the background bidding penny's and knowing they will lose, but sucking up information they can build into profiles...

Believe it or not, you can delete your Mobile Advertising ID.

Research indicates very few users have deleted their Mobile Advertising ID (MAID).
Just over 2% of Android users have disabled their MAID.
https://www.singular.net/blog/google-limit-ad-tracking/

On the Apple platform the numbers are better.
25+% have their MAID enabled so that they can give data to their favorite apps.
https://www.statista.com/statistics/1234634/app-tracking-transparency-opt-in-rate-worldwide/

**** LOCATION BROKERS:**

There are a lot of location brokers. We've identified 124 with independent research.
They aggregate location data - almost exclusively based on MAID.
And they do this based upon your indirect consent via apps and other services.

**** RE-IDENTIFICATION:**

Location brokers like to tell you their data is anonymous. Don't believe that.
You can be identified from a few sets of lat long coordinates.
Four sets will uniquely ID 95% of Americans. https://www.nature.com/articles/srep01376

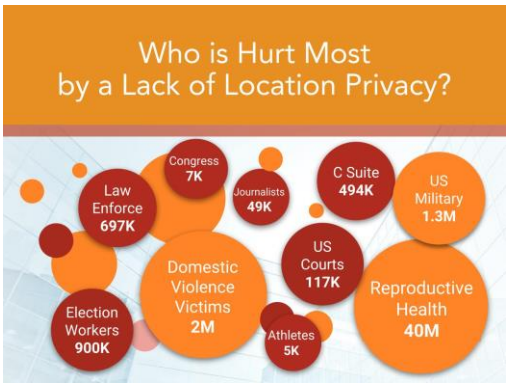
Worse yet, data brokers like BigDMB advertise they have already matched your 'anonymous' MAID to your personal data. Just insert a credit card.
https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii

All … in the name of …. Advertising?
Really?

It's **invasive**. It's **dangerous**.

When we talk about location privacy its not simply privacy we are worried about but physical safety.

Who is hurt the most?



The people most hurt by the lack of location privacy are diverse:

* People concerned with Reproductive Health in the wake of the Dobbs decision
* Domestic Violence victims: trying to stay a step ahead of pursuers
* The US Military: not wanting to reveal the location of soldiers and operations
* Law Enforcement
* The US Court System
* Company Executives

And many more.

We'll leave you with this rhetorical question:
Should location data about these people be for sale?
Should location data about anyone be for sale?

Are marginally better ads worth risk to physical safety?