Wi-Fi tracking

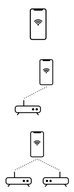
Low Tech Canvas Against High Tech Surveillance

Use our **wearable** guides to become a digital explorer of your city. See your neighborhood in a new light while exploring issues around facial recognition, voice identification, gait recognition, thermal imaging, and Wi-Fi tracking.

Be careful: becoming an explorer is exciting but at times jarring. You might learn more about your world than you want. Now take this canvas to the streets, bring your curiosity, watch, listen, and play. Try out some of our tactics and strategies to resist data collection in public space and co-design your neighborhood.

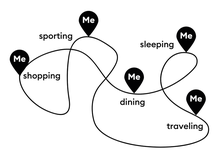
Getting a lay of the land

1. How to track people using Wi-Fi



1. Your phone is broadcasting a unique number to connect to Wi-Fi.
2. It tries to connect to Wi-Fi using a unique number called a Mac Address: 60:AX:XX:XX:04
3. The receiver processes the MAC address in combination with signal strength, the location of the phone and the date and time.
4. This can be used to track you in a specific location.

Pro spotter tip: your phone wants to be visible at all times. It continuously broadcasts, and tries to connect to surrounding Wi-Fi networks. Note that your phone can be tracked even if it is not connected to the network.



2. How unique is your phone?

Each phone has a unique number, a MAC (media access control address) address. Find yours:

Instructions

iPhone: go to Settings > General > About > find the MAC address under the "Wi-Fi Address"

Android: go to Settings > About Device > Status > find the MAC address under the "WiFi MAC address"

Pro spotter tip: From a random number to a person. It might feel strange that you can be identified by this weird looking number. In theory, if a company collects data about this number over time and combines it with other data, a person could be identified.

In practice, public Wi-Fi offered at airports and stations might ask for your email or phone number. This allows them to map your every movement to your identity.

3. Are you being tracked in your neighborhood?

Wi-Fi tracking is mostly invisible, but maybe we can find some traces of it. Let's explore; go to the following location and see if you can find any traces of Wi-Fi tracking.

4. Targeted advertising goes offline

With Wi-Fi tracking popping up from stations to shopping malls, the question is how comfortable are you with Wi-Fi tracking? Check out the use cases below and indicate how comfortable you are with the use of this technology. Listen to your gut, and write on this canvas how comfortable you are from not at all to very.

5. Making 'invisible' infrastructures visible

The first step in navigating privacy in public spaces is knowing what is going on. Richard Vijgen developed the Architecture of Radio app to reveal the invisible technological landscape our devices interact with.

Download his app in the app store and explore for yourself (note: it is a paid app)

www.architectureofradio.com

8. Tricking the system

Berlin based artist Simon Weckert's Google Maps Hacks is an exciting example of how one can hack high tech systems with creative low tech solutions.

Walking across a bridge with 99 second-hand phones in a small cart he fooled Google into thinking there was a traffic jam.

simonweckert.com/googlemapshacks.html

Navigating privacy in public spaces

6. Protecting your identity

Explore your phone settings! An easy way to minimize Wi-Fi tracking is to turn off your Wi-Fi when you leave your house.

Android instructions:
Swipe down and turn of Wi-Fi

Go to Settings > Privacy > Advanced > Ads and turn on "Opt out of Ads Personalization"

iPhone instructions:
Swipe up and turn of Wi-Fi

Go to Settings > Privacy > Advertising > Turn on "Limit Ad Tracking" and click on "Reset Advertising Identifier". Go to Settings > Privacy > Location Services > System Services > turn off Location-based Apple-advertenties.

7. Create your own protective bag

Preventing being tracked in a building by blocking your phone from broadcasting. One way to do this is to build a protective shield, also known as a Faraday bag.

Materials:

- Scissors
- Tick paper
- Aluminium foil
- Tape

Instructions:

Step 1 Make a paper pouch
Measure the width, height, and depth of your phone (+ case, if you have one).

Add 2,5 cm to your phone width measurement and 5 cm to your phone height measurement.

Leave 5 cm above the phone so the top can be folded over like an envelope.

Step 2 Aluminyze
Make a pouch of aluminium foil that fits around your paper pouch.

Step 3 outer layer
Make your second paper pouch and make sure it fits around the first paper and the aluminium pouch.

As this is the outer layer, experiment with colors and prints!

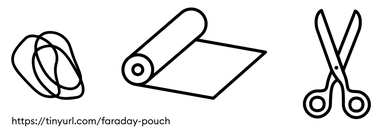
Step 4 Combining now
Shove the aluminium layer around the first paper layer. Put these in your outer paper pouch layer.

Step 5. Closing off
Add a flap of paper fitted with aluminium foil.

Put your phone in your newly made faraday pouch and close the flap with a rubber band.

Step 6: Test your protective bag by having someone call you while your phone is inside.

Pro spotter tip: when your phone is in your faraday bag it has gone off the grid, this will protect you from being tracked but remember you will not be able to receive any calls or text messages.



https://tinyurl.com/faraday-pouch

9. Exercise your rights

The European data protection bill has given us more control over what happens to our data. For example, you now have the right to access your data held by a third party, correct it if it's inaccurate, ask for it to be removed, or even move it to another platform. Let's try how this works in a public space.

Step 1: Find a location where they are using Wi-Fi tracking, think of shopping malls, train stations, and a subways station. Look for this icon or a notice board through which the company announces Wi-Fi tracking.

Step 2: In case you turned-off your Wi-Fi signal, turn it on again.

Step 3: Note down the exact location (any characteristics), time and date.

Step 4: Find out who is responsible for the Wi-Fi tracking by reading the information sign or finding out who is responsible for the space.

Step 5: Approach the entity responsible for the Wi-Fi tracking (this can often be done over email) and ask them to remove your unique Mac address from their database. Include the location, time and date in the request.

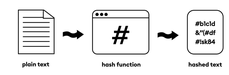
Step 6: Still uncomfortable with your personal data being collected and stored for Wi-Fi tracking? File a complaint with your local data protection agency or write a letter to your Alderman.

Pro spotter tip: They might answer that they can not find your Mac Address as they have used 'hashing' to pseudonymised it. Say what? Find out more below.

Tip: Look for signs, stickers and the small print.

On the canvas we have used a pseudonymised Mac address. Can you find it?

10. Hashing



Hashing: replaces 'personal data' with a random string of numbers so that you cannot be identified in the dataset.

Pseudonymization: is a practice that allows a company or research institute to use personal data without tying it to a specific person. Take the example of using Wi-Fi tracking on a station to analyze how many people buy coffee or food at a certain shop to determine the rent. They need to use your Mac address to track your movement across a station, but as it is directed towards the businesses in the station, the Wi-Fi tracker does not need to know who you are, just where you are.

Tip: Pseudonymization does not offer a 100% anonymity as the process can be reversed.

11. Join a community

The use of WiFi-tracking is a complex issue. Don't go at it alone, find a community!

Pro spotter tip: Find your local digital rights group or crypto party and join their mailing list or meet ups. Unsure where to find them? Search for 'human rights and WiFi-tracking' 'NGO + digital rights + your country'

You'll probably find groups like Bits of Freedom, EDRi, Liberty, Ada Lovelace Institute, AI Now, Article 19, La Quadrature du Net, and Data and Society.

Support those fighting for your rights.
Donate to your local digital rights or human rights group.

Colophon

Version Sept 2021 ENG V.04

Produced by

Fieke Jansen, Data Justice Lab in collaboration with designcollective idiotēs with support from Designlab Digital City, Amsterdam.

datawear.
www.datawear.it

Supported by

mozilla · City of Amsterdam · Hivos people unlimited · oba · idiotēs