Wifi-tracking

Low Tech Canvas tegen High Tech Surveillance

Gebruik onze **draagbare gidsen** en word een digitale ontdekkingsreiziger in jouw stad. Door de kwesties rond gezichts-, stem-, en bewegingsherkenning, thermische camera's en wifitracking te verkennen, zal je jouw buurt in een heel ander licht zien.

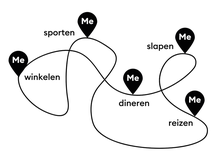
Een ontdekkingsreis is spannend, maar soms ook schokkend. Misschien leer je meer over de wereld dan je zou willen. Neem dit doek mee de straat op, wees nieuwsgierig, kijk, luister en speel! Experimenteer met onze tactieken en strategieën om het verzamelen van gegevens in de openbare ruimte tegen te gaan. Gebruik ze om zelf jouw buurt vorm te geven.

Verken de buurt

1. Wifitracking, hoe zit dat?

1. Wanneer een telefoon een wifinetwerk zoekt, stuurt deze onversleuteld een code mee – het 'MAC-adres'. Het MAC-adres is een uniek identificatienummer, elk apparaat dat verbonden is met internet heeft zo'n nummer.
2. Een voorbeeld van een MAC-adres: 60:AX:XX:XX:04.
3. De eigenaar van het wifinetwerk verwerkt het MAC-adres in combinatie met de signaalsterkte, de locatie van de telefoon en de datum en tijd.
4. In grotere ruimtes zoals vliegvelden, treinstations en winkelcentra wordt het internet aangeboden via verschillende toegangspunten. Hierdoor wordt je telefoon in zo'n ruimte gevolgd en dus ook jouw bewegingen. Dat geeft inzicht in hoe lang je je bijvoorbeeld ophoudt bij de koffiekiosk of bij de snackmuur.

Tip voor de pro: Jouw telefoon wil heel graag gezien worden en probeert continu verbinding te maken met de zendmasten en wifinetwerken in de buurt. Houd er rekening mee dat je telefoon kan worden gevolgd, zelfs als hij niet met een netwerk verbonden is.



2. Hoe uniek is jouw telefoon?

Ontdek je telefooninstellingen! Elke telefoon heeft een uniek 'media access control-adres' (MAC-adres). Volg de onderstaande instructies en vind die van jou:

Instructie:

iPhone: ga naar Instellingen > Algemeen > Info > vind het MAC-adres onder "Wifi-adres".

Android: ga naar Instellingen > Over de telefoon > Status > vind het MAC-adres onder "Wifi MAC adres".

Tip voor de pro: Het blijft een vreemd idee dat je geïdentificeerd kan worden door een serie willekeurige cijfers en letters. Om te weten aan wie het MAC-adres toebehoort, zijn er inderdaad ook andere gegevens nodig.

Maar in de praktijk maken we het bedrijven vaak veel te makkelijk door in te loggen met onze echte naam en e-mailadres op een gratis wifinetwerk – bijvoorbeeld op het vliegveld of station.

5. Het zichtbaar maken van 'onzichtbare' infrastructuren

Het vergroten van je privacy in de openbare ruimte begint met het ontdekken van welke technologie er wordt gebruikt en door wie. Richard Vijgen ontwikkelde de 'Architecture of Radio' app om het onzichtbare communicatielandschap van onze apparaten zichtbaar te maken.

Download de app in de (betaalde) appstore en ontdek het zelf.

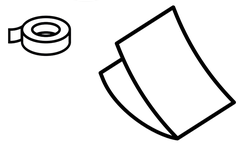
www.architectureofradio.com

8. Wees het systeem te slim af

Het werk 'Google Maps Hacks' van de Berlijnse kunstenaar Simon Weckert is een spannend voorbeeld van hoe je hightechsystemen kan 'hacken' met creatieve lowtechoplossingen.

Met slechts 99 tweedehands telefoons in een klein karretje hield hij Google voor de gek: het systeem dacht dat er een verkeersopstopping was.

simonweckert.com/googlemapshacks.html



Bescherm je privacy op straat

3. Word jij in jouw buurt gevolgd?

Wifitracking is grotendeels onzichtbaar, maar misschien kunnen we een aantal dingen ontdekken. We gaan op verkenningstocht: ga naar de volgende locaties en kijk of je sporen van wifitracking kunt vinden.

Treinstation | Metrostation | Winkelcentrum | Google Street View

4. Wie vertrouw jij met wifitracking?

Nu wifitracking opduikt op stations en in winkelcentra is de vraag hoe jij je voelt over het gebruik van deze technologie. Vind jij het oké dat de technologie voor deze doeleinden wordt gebruikt?

	Niet	Heel erg
Stations tellen het aantal mensen dat een winkel binnenkomt om zo de huurprijs van winkels te bepalen		
De spoorwegen controleren de drukte in de trein en helpt je een lege stoel vinden		
De gemeente monitort de drukte op een station voor de brandveiligheid		
Winkels analyseren de beweging van klanten om hun koopgedrag te kunnen voorspellen		
De gemeente houdt drukte op bepaalde locaties bij om gebieden op tijd af te zetten		
Vliegvelden analyseren bewegingen van reizigers om gerichte reclame op je telefoon aan te bieden		
Metro analyseert drukte op de stations voor het verbeteren van hun dienstverlening		
Google street view verwerkt wifitoegangspunten om hun locatievoorzieningen te optimaliseren		

6. Bescherm je identiteit

Een eenvoudige manier om wifitracking tegen te gaan is om wifi uit te schakelen wanneer je je huis verlaat. Volg de instructies hieronder om wifi uit te zetten en reclametracking op je mobiel te verminderen.

Android instructies:
Swipe naar beneden en zet wifi uit

Ga naar Instellingen > Privacy > Geavanceerd > Advertenties en zet "Opt out of Ads Personalization" aan.

iPhone instructies:
Swipe naar boven en zet wifi uit

Ga naar Instellingen > Privacy > Reclame > Zet "Beperk reclametracking" aan en klik op "Stel reclame ID opnieuw in".

Ga naar Instellingen > Privacy > Locatievoorzieningen > Systeem > en zet "Locatiegebonden Apple Advertenties" uit.

Op het doek gebruiken we een gepseudonimiseerd MAC-adres, kan jij het vinden?

7. Maak een privacybeschermend tasje

Voorkom dat je telefoon contact kan maken met wifitrackers door een privacybeschermend tasje, ook wel bekend als een Faradaytas, te maken.

Benodigdheden:

- Schaar
- Dik papier
- Alumniumfolie
- Tape

Instructie:

Stap 1 Papieren tasje
Maak een papieren zakje dat je telefoon goed omsluit.

Tip: leg je telefoon op het papier, maak een omtrek van je telefoon, voeg aan de zijkanten 2,5 cm toe, aan de onderkant 10 cm en aan de bovenkant 5 cm.

Knip deze omtrek uit het papier en vouw hem om je telefoon door de onderkant naar boven te klappen en plak deze aan de zijflappen vast met tape. Het papier dat aan de bovenkant uitsteekt dient als sluitflap.

Stap 2 Aluminiseer
Maak op dezelfde manier een tasje van aluminiumfolie dat om je papieren zakje past.

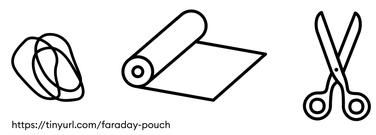
Stap 3 Buitenlaag
Maak nu een tweede papieren zakje, dit moet om het eerste papieren zakje en het aluminiumfolie passen.
Dit is de buitenkant, probeer verschillende kleuren en prints!

Stap 4 Combineer
Schuif de aluminium laag over het eerste papieren tasje.
Schuif hier het buitenste papieren tasje omheen.

Stap 5 Maak het af
Voeg een papieren flap voorzien van aluminiumfolie toe.
Stop je telefoon in je gloednieuwe Faradaytasje en maak het dicht met een elastiekje.

Stap 6 Test
Werkt jouw Faradayzakje? Test het. Vraag of iemand je belt terwijl je telefoon erin zit.

Tip voor de pro: Zit je mobiel in je Faradaytas? Dan is die niet meer zichtbaar voor het netwerk. Let op: je zal ook geen oproepen of sms'jes meer ontvangen.



https://tinyurl.com/faraday-pouch

9. Maak gebruik van je rechten

De AVG, onze privacywet, geeft je meer rechten en controle over wat er met je gegevens gebeurt. Zo heb je nu het recht op toegang tot jouw persoonlijke data die in het bezit zijn van een derde partij, om ze te corrigeren als ze niet correct zijn en om ze te verwijderen. Probeer nu hoe dit werkt in de publieke ruimte.

Stap 1: Zoek een locatie waar gebruik wordt gemaakt van wifitracking, denk aan winkelcentra, treinstations en metrostations. Zoek naar het pictogram of een informatiebord waarmee wifitracking op de locatie wordt aangekondigd.

Stap 2: Als je bij een eerdere opdracht je wifisignaal hebt uitgeschakeld, zet dit dan eerst weer aan.

Stap 3: Noteer de exacte locatie met eventuele kenmerken, datum en tijd.

Stap 4: Zoek uit wie verantwoordelijk is voor wifi-tracking. Kijk op informatieborden of je daarop ziet staan wie er verantwoordelijk is voor de ruimte.

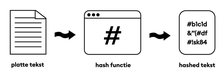
Stap 5: Benader de partij die verantwoordelijk is voor de wifitracking, dit kan vaak via e-mail, en vraag ze om je unieke MAC-adres te verwijderen uit hun database. Noem de locatie, datum en tijd in het verzoek.

Stap 6: Voel je je er nog steeds ongemakkelijk bij dat je in publieke ruimtes wordt gevolgd door wifitrackers, dien dan een klacht in bij de Autoriteit Persoonsbescherming of schrijf een brief naar de wethouder.

Tip voor de pro: Het kan zijn dat de wifitrackers je MAC-adres niet kunnen vinden, omdat ze een techniek gebruiken die 'hashing' wordt genoemd, waarmee ze je MAC-adres pseudonimiseren. Eehhh – hashing...? Pseudonimiseren?

Tip: Let op informatieborden, stickers en op kleine lettertjes

10. Hashing



Hashing: 'persoonlijke data' worden vervangen door een willekeurige reeks getallen, zodat jij niet meer geïdentificeerd kan worden in de dataset.

Pseudonimisering: hiermee kan een bedrijf of onderzoeksinstelling persoonlijke gegevens gebruiken zonder dat deze aan een specifiek persoon gekoppeld zijn.

Op stations wordt bijvoorbeeld vaak gekeken naar het aantal mensen dat bepaalde routes loopt of winkels in gaat, om zo de huurprijs te bepalen. Hierbij wordt niet gekeken naar wie daar loopt, wel naar hoeveel mensen waar lopen. Je MAC-adres maakt het mogelijk om te analyseren waar je bent en hoe lang je in een winkel staat.

Let op: Het klinkt mooi, maar pseudonimisering biedt geen 100% anonimiteit, omdat de gegevens vrij makkelijk weer aan jou gekoppeld kunnen worden.

11. Sluit je aan!

Het gebruik van wifitracking is een ingewikkelde zaak. Samen sta je sterker, sluit je aan bij organisaties bij jou in de buurt om op de hoogte te blijven.

Tip voor de pro: Spot je lokale digitale rechtengroep of cryptofeest, abonneer je op een mailinglijst of ga naar meet-ups van groepen die zich hiermee bezighouden. Zoek bijvoorbeeld online naar 'mensenrechten en wifitracking' en de naam van je stad, of 'NGO + digitale rechten'.

Voorbeelden van groepen zijn: Bits of Freedom, Amnesty International, PILP NJCM, EDRi, Ada Lovelace Institute, Article 19, en La Quadrature du Net.

Steun degenen die voor je rechten vechten. Doneer aan lokale organisaties die zich inzetten voor digitale rechten en mensenrechten.

Colophon

Versie: Sept 2021 NL V.03

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