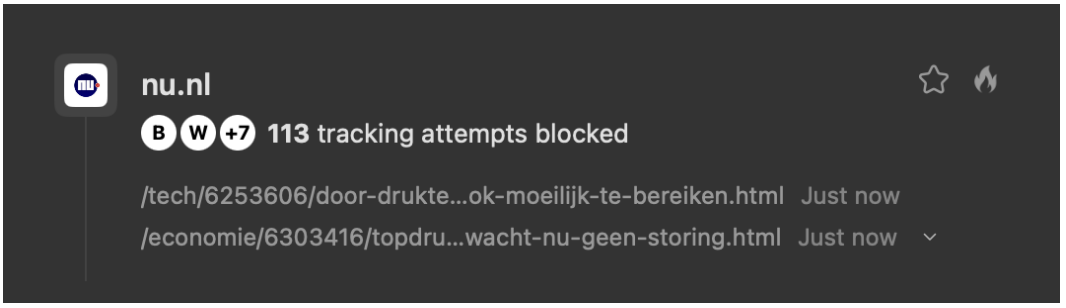
Data gebruik: privacy blijft in het geding

Denkerslab: Quinten Kok

Inhoud

We leven in een wereld waar digitale apparaten en applicaties ons overal omringen. Momenteel kunnen we het ons moeilijk meer voorstellen om zonder internetverbinding of mobiele telefoon te leven. Dat heeft allemaal voordelen. Ik heb te allen tijde een camera, rekenmachine, timer, klok, mp3- en mp4-speler, een interactieve gps, en nog veel meer bij de hand. Toch komt er bij het gebruik van deze onbegrijpelijke apparaten meer kijken dan alleen de positieve aspecten; zo levert een gebruiker ook een hele hoop in.

Veelal betalen gebruikers van 'gratis' applicaties of sites met hun data — en dus ook met hun privacy. Een simpel voorbeeld hiervan is www.nu.nl. Na een minuut klikken en rondkijken op de site zijn er 113 trackers gevonden (zie figuur 1).



Figuur 1: Nu.nl trackers na ~ 1 minuut gebruik (duckduckgo browser)

Deze trackers volgen een hele hoop verschillende informatie die mee wordt gegeven bij het betreden van een site. Websites (en applicaties) kunnen veel informatie uit het apparaat halen dat gebruikt wordt om de site of app te openen. Deze trackers worden veelal geregeld door externe partijen.

Lees 1: DuckDuckGo: Tracker radar

Privacy: privacy is niet meer hetzelfde

Sinds de explosie van het internet heeft het begrip van en privacy zelf een steeds kleinere rol gespeeld. In de van Dale en op de site van Van Dale is de betekenis van 'privacy' als volgt:

> pri·va·cy (de; v(m))
> 1. de mogelijkheid om in eigen omgeving helemaal zichzelf te zijn: iemands privacy schenden zich ongevraagd met zijn privéleven bemoeien

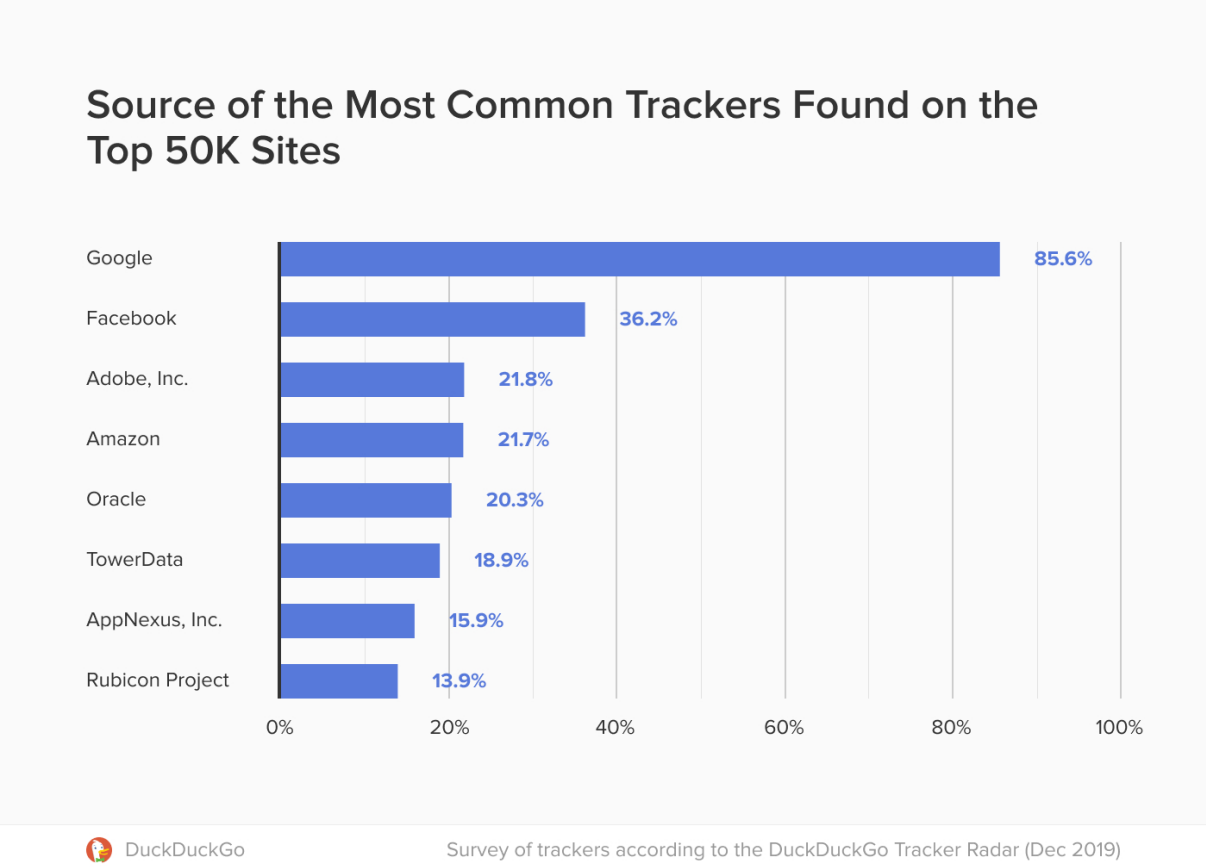
De wereld in de huidige staat is gevuld met digitale apparaten. Technologie is nu zo ver dat de Telegraaf nu eerder op de telefoon, tablet, of laptop gelezen wordt dan de papieren variant — met als gevolg dat trackers ook meelezen. Bij het lezen van de papieren krant zou het toch raar zijn als er iemand in de rug meekijkt en niet om mee te lezen, maar om te kijken naar welke reclame je kijkt, hoe lang je over een artikel doet, welke artikelen je leest, en nog heel wat meer. De privacy die de lezers van de Telegraaf in hun woonkamer hadden, is vertroebeld.

Modernisering zien we overal om ons heen, alles moet digitaler, sneller, slimmer, makkelijker, beter. Een thermostaat met touchscreen, een ‘slim’ auto besturingssysteem, digitale Ring-camera’s, etc. Maar de 'digitalisering' van privacy is nog ver te zoeken. Een nieuw idee van het begrip en de wetten die zich daaromheen bevinden, zou de gebruiker een veiligere digitale wereld kunnen bieden. Dit is iets waar de Europese Unie al mee bezig is, maar achter de feiten aan lijkt te lopen. Het proces om tot een nieuwe wet te komen duurt hiervoor te lang, naast het feit dat bedrijven — zoals Meta — snel om de wetten heen weten te werken.

Ethiek in digitale privacy

Het constant groter groeiende internet wordt door heel veel — meestal nerds, myself included — gezien als potentie. Concepten en applicaties die voorheen ondenkbaar waren, worden mogelijk en het gebruikersgemak kan steeds meer geoptimaliseerd worden. Zo zijn er alleen al voor webdevelopment elk jaar nieuwe toevoegingen die alles sneller, mooier, simpeler of praktischer maken (zie Interop 2024). Waar de potentie oneindig lijkt te zijn, zijn die potenties om onethisch om te gaan met de privacy van de eindgebruiker ook mogelijk oneindig. Hierbij is de valkuil ook dat veel developers en de opdrachtgevers

geen of weinig rekening hiermee (willen) houden. De makkelijkste voorbeelden zijn uiteraard Facebook (Meta) en Google. Deze giganten in de digitale wereld zijn de grootste boosdoeners is het vergaren van user data, en dus actief tegen de privacy van de gebruiker werken. In het rapport van DuckDuckGo, een bedrijf dat onder andere een privacy-gerichte browser heeft gemaakt, blijkt dat Google trackers teruggevonden zijn in 85.6 procent van de top 50.000 sites. Facebook komt tweede met 36.2% (Zie figuur 2).



Figuur 2: DuckDuckGo trackers in de top 50.000 sites

Privacy in het geding zonder trackers

Trackers zijn niet de enige boosdoeners — maar wel een grote, lees daarvoor verder — ook applicaties zonder trackers kunnen veel data van een gebruiker verkrijgen. Applicaties zoals Instagram, Facebook, LinkedIn, etc. krijgen al veel data van de gebruiker zelf! De gebruiker vult alles over zich in, van geboortedatum tot adres, telefoonnummer enzovoorts. Hierdoor kunnen bedrijven al makkelijker informatie van specifieke gebruikers vinden en toepassen. Hier geldt ook dat het in principe niet een slecht ding hoeft te zijn, toch zien we het tegendeel in de praktijk. Facebook heeft een hele hoop

uitschieters gehad, deze zijn veel in het nieuws gekomen, datalekken, verkopen van data of zelfs het gratis weggeven van gebruikersdata of gehele gesprekken van gebruikers in hun sms-service. [Lees 2: Facebook shares messages between mother and daugher] De gebruikers die slachtoffer zijn van deze praktijken zijn er vaak niet over geïnformeerd, en moeten het zelf uit de privacy statement halen. Hierin kan je die gebruiker ook niet kwalijk nemen dat ze geen (of niet alle) privacy-statements van techbedrijven wil of kan lezen, in een onderzoek (enigszins verouderd) bleek dat het op jaarbasis naar schatting 244 uur per jaar kost om alle privacy policy te lezen van één gebruiker.

[Lees 3: Reading policy cost]

App- en webtrackers: de blackbox

Niet alleen websites gebruiken trackers, ook veel apps op mobiele telefoons en tablets maken gebruik van trackers. [Lees 4: NYT location data privacy]. Hiervoor geven veel gebruikers zelf toestemming. Bij het eerste gebruik van een applicatie kan bijvoorbeeld de vraag om locatietoestemming naar voren komen. Toch wordt bij het geven van die toestemming vaak niet goed gedacht over het gebruik van die app en waarom ze die data nodig hebben. De apps die toegang krijgen van de gebruiker maken vervolgens gebruik van externe trackers om zo de locatie van het apparaat te volgen — dat is op zichzelf niet iets slechts, sterker nog, het kan best nuttig zijn. Echter, als het bedrijf volledig vrij is om te doen met die data wat ze willen, dan kan het heel snel een verkeerde kant op gaan. In het artikel hierboven van de New York Times is de data van een vrouw genaamd Lisa Magrin gebruikt om haar te volgen, zonder dat ze dat initieel wist. De data die daarbij gebruikt was door de NYT was anoniem, maar zonder al te veel moeite zijn ze erachter gekomen wie ze was. Zo was de privacy van mevrouw Magrin volledig uit de deur en nergens meer te bekennen.

Anonimiteit bestaat niet meer

Het onderzoeksteam van de NYT is niet de enige die makkelijk gebruikers kunnen herkennen in anonieme data, MIT-onderzoekers zijn nog een stapje verder gegaan. In januari 2015 is er een onderzoek gedaan naar creditcarddata en daaruit unieke gebruikers vinden. [Lees 5: Credit Card MIT]. Hierin is geconstateerd dat er met “just four fairly vague pieces of information — the dates and location of four purchases” genoeg informatie is om 90 procent van

de mensen in de dataset te identificeren — een dataset van creditcardtransacties van 1.1 miljoen gebruikers over 3 maanden.

Consequenties en gevaren

Een gebruiker kan vrijwel niet onopgemerkt het digitale landschap betreden, ze worden direct gevolgd door trackers of geven zelf veel informatie weg. Voorafgaand aan dit artikel is er bij een groep van 30 studenten gevraagd hoe ze zich voelen over deze informatie. Daarbij was het herhalende antwoord: "Ik heb niets te verbergen, dus waarom zou het uitmaken?". Op deze stelling is lastig een antwoord te geven, hierbij een poging om dat toch te doen.

De gebruikers en hun probleem

Voorafgaand aan de voorbeelden, moeten we kijken waarom gebruikers zo makkelijk hun privacy en data opgeven. Ook in het onderzoek zijn er platformen gebruikt waarvan bekend is dat ze data opslaan en er gebruik van maken. Dat lijkt verschillende redenen te hebben, deze kan in twee groepen plaatsen: Onwetend- en bewust weggeven van data. De eerste is erg voor de hand liggend. Van de 30 studenten die ondervraagd zijn, waren de meeste wel bewust dat data verzameld werd, maar niet hoe, hoeveel, wat daarmee gedaan werd, hoe ze het uit konden zetten en vonden het daarom ook minder erg dat het hun overkwam. Een enkeling was hier wel al van bewust, na een korte ondervraging bleek dat de student toch veel applicaties is blijven gebruiken — wetende wat de consequenties ervan waren. Het ging om een mannelijke student van 20 jaar en studeert informatiekunde bij de UvA. Hij heeft er al een aantal vakken over gehad, maar voor hem was de overweging tussen gebruikersgemak en privacy makkelijk gemaakt. Hierbij gaf ook wel aan dat als er een privacyvriendelijke applicatie was, met 90% van de gebruikersvriendelijkheid, hij die liever gebruikte. Deze opties zijn echter moeilijk te vinden, te duur (voor de weinig werkende student) of het niet waard. Ditzelfde gold voor het gebruik van verschillende applicaties tijdens en voorafgaand aan het schrijven van dit artikel.

Consequenties van onethisch gebruik van data

De mogelijkheden om data van gebruikers op de verkeerde manier toe te passen zijn nagenoeg oneindig. De gevolgen daarvan kunnen voor de gebruikers ook onmeetbaar zijn, van onveilig voelen, tot levenslange

consequenties. Zo zullen de voorbeelden — en consequenties — die hier volgen in rangorde van vervelend of matig, naar ongekend geschikt worden. Om te beginnen kan er gekeken worden naar het privacybelang van bedrijf Signal, zij waren erg handig met campagne om de meest ‘eerlijke’ Facebookreclame te maken. [Lees 6: Gizmo most honest ad]. Deze reclames werden geplaatst op Instagram en maakten gebruik van de data van Facebook (Meta), het doel was om de gebruiker bewust te maken van de data die Facebook over hen heeft. Voor het ‘targeten’ van gebruikers voor de reclames kan er vrijwel een oneindige reeks aan data gespecificeerd worden, van simpele data, naar steeds specifieker. Facebook was hier geen grote fan van en de reclames hebben de praktijk nog niet gezien, tevergeefs.

Niet alleen Facebook of Google maakt gebruik van userdata, dat wordt ook gezien bij bijvoorbeeld hotels en vluchten die geboekt worden.[Lees 7: Airlines raising prices] Hierbij wordt bijvoorbeeld het apparaat waarmee een gebruiker boekt gebruikt om een prijsdifferentiatie te maken, een macOS-gebruiker kreeg op de site van Orbitz — een online reisbureau — hogere prijzen dan een Windows-gebruiker. Ook leek er gekeken te worden naar de zoekgeschiedenis van gebruikers om artificieel de prijzen te verhogen, erg jammer als je aan het twijfelen bent over je vakantie.

De sprong in ernst zal nu een stuk groter zijn, de consequenties zijn nu niet meer jammer; ze zijn simpelweg onacceptabel. Google heeft een stukje geautomatiseerde software voor Google Photos om verwaarloosde kinderen te spotten, een verkeerde melding heeft nare gevolgen. In dit artikel, zoals de titel aangeeft, heeft een vader een foto van zijn naakte zoon voor de dokter gemaakt. [Lees 8: Google surveillance toddler photo]. De zoon had een geslachtsaandoening en zijn ouders hadden in tijden van de pandemie een foto gemaakt om naar het digitale doktersportaal op te sturen. Hierbij was de hand van de vader zichtbaar om de aandoening duidelijk te maken. Aangezien de foto’s automatisch naar Google Photos gesynchroniseerd worden, werd het algoritme van Google erop los gelaten en direct gemarkeerd als crimineel. Het gevolg hiervan is dat de politie direct gecontacteerd werd, zonder dat dat bekend was bij de ouders en er werd een uitgebreid onderzoek gedaan. Belangrijk om te weten is dat Google het hele account, met **alle** data van de vader, vrij weggaf aan de politie voor het onderzoek. Twee dagen na de foto werd het account van de vader, met meer dan tien jaar aan foto’s, e-mails, agenda-afspraken, zijn bel- en dataplan en telefoonnummer geblokkeerd. Na het onderzoek van de politie was al snel duidelijk dat het geen crimineel geval

was, maar een bezorgde vader die een foto maakt voor de dokter. Toch blijft Google steenvast, eenmaal gemarkeerd kan daar geen verandering in gebracht worden — eventueel een rechtszaak wel — zelfs het politierapport dat het tegendeel bewees was niet genoeg. In 2021 waren er 4260 kindslachtoffers bij autoriteiten aangegeven, waar het geval hierboven ook meegeteld werd. Dit is, en zal zeker niet de enige zijn waarbij het een verkeerde melding was. In het artikel werd rond dezelfde tijd ook een ander geval behandeld, maar dat zijn twee ouders die het durven aan te geven. Het feit dat Google dit mag doen, zonder enige toestemming-, vraag naar context-, of coöperatie bij een verkeerd geval- is onnavolgbaar.

Maar ook in een nieuwe auto kan een gebruiker de dupe zijn van onethische schending van privacy, hier was het echter geen automatisch systeem of algoritme dat onethisch was. Hier waren het mensen, medewerkers van Tesla, die video’s en foto's van de gebruikers bekeken, deelden, en grappen over maakten. [Lees 9: Tesla workers shared images]. Tesla maakt gebruik van mensen om hun algoritmes te trainen, wat een stopbord is, waar voetgangers lopen, wat een garage is. Zo krijgt een gebruiker de optie om (met onder andere analytische data) te helpen Tesla te verbeteren. In het artikel zijn er verschillende ex-Tesla-medewerkers geïnterviewd, waaronder dit antwoord:

> “I’m bothered by it because the people who buy the car, I don't think they know that their privacy is, like, not respected ... We could see them doing laundry and really intimate things. We could see their kids.”

In het kantoor in San Mateo werken voornamelijk veel jonge medewerkers en vonden het vooral erg grappig om tijdens het labelen van fragmenten memes te maken en die te delen onder het team. Het rijden in een Tesla auto werd door een aantal van de medewerkers zelf ook minder fijn, zoals een ex-medewerker zelf zei:

> “Knowing how much data those vehicles are capable of collecting definitely made folks nervous"

Dit tekent natuurlijk niet een goed beeld, dat een medewerker van een bedrijf zo over hun eigen product praat.

Maar Tesla is niet de enige die meekijkt, Amazon Ring camera's zijn ook een goed voorbeeld van hoe het niet zou moeten. [Lees 10: Amazon Ring cameras used to spy] Bij Amazon Ring kon elke medewerker — en ook de derde partijen uit Oekraïne — elke camera inzien en alles wat daarbij kwam kijken, dat kan en heeft wat nare gevolgen. Naast het feit dat het bizar is dat dit initieel kon, is het natuurlijk onethisch om mensen te bespieden terwijl hier geen idee van was. Onverwachts werd hier verkeerd gebruik van gemaakt, waardoor een specifieke medewerker gek genoeg alleen maar inspecties deed bij hele knappe dames, pas daarna gingen er een aantal bellen rinkelen bij de baas. Daarna werden toegankelijkheden veranderd en werd het iets strenger, zo moesten gebruikers eerst toestemming geven om een medewerker mee te laten kijken. Dat had niet heel veel gedaan, blijk uit het artikel, want in 2018 was er niet veel verbetering:

> However, Ring continued to allow hundreds of other employees and third-party contractors access to all video data, regardless of whether they actually needed it in order to perform their jobs.

Daarbij komen ook een aantal buitenstaande partijen kijken, die eigenlijk helemaal geen toegang zouden moeten hebben. Hackers kunnen redelijk makkelijk binnen dringen op iemands netwerk als dit niet goed beveiligd wordt, dit gaat meestal via printers gek genoeg. Printers zijn vaak verbonden met het internet, maar veel gebruikers zetten geen of een erg zwak wachtwoord op hun printer; zo kan een hacker gemakkelijk binnen komen op niet alleen hun printer en alles daarin, maar ook de rest van het netwerk. Als die eenmaal binnen zijn, is een Ring camera relatief eenvoudig om te openen. Ook dit wordt in het artikel behandeld, waarbij vrouwen in bed hackers hoorden praten via de Ring camera.

Water in de zee dragen

Voor een gemiddeld persoon is het niet mogelijk om helemaal 'data-loos' te leven, maar door bewust te leven in het digitale landschap kan een gebruiker zich beter beschermen. Het gaat hierbij dus niet om totaal 'off-the-grid' te leven, maar eerder om vaker nee te zeggen tegen sommige cookies van

browsers, niet direct alle gebruikersgegevens weg te geven, of bijvoorbeeld een andere browser te gebruiken.

DuckDuckGo

In het begin van het artikel is er gebruik gemaakt van DuckDuckGo om de trackers die Nu.nl op zijn site heeft te zien. Deze browser houdt expliciet rekening met privacy en doet veel voor privacy in het digitale landschap.[Zie 11: DuckDuckGo]. Door naar beneden te scrollen op de link, is hier meer informatie over hen te vinden. Daarnaast zijn er voor veel applicaties mogelijkheden om gebruikersgegevens te verwijderen van een account, [Zie 12: Google activity]. Hier kan een gebruiker in drie stappen datatracking en zijn data verwijderen. Google, Facebook en andere applicaties worden hierbij ook direct afgeraden, maar het is begrijpelijk als deze nog steeds gebruikt worden. Google Maps is een grote boosdoener, maar ook deze kan bij '*myactivity*' uitgezet worden.

Mobiele trackers

Een mobiele telefoon heeft een privacysectie, waar de applicaties die verschillende privacytoestemmingen nodig hebben verzameld worden. Het is een aanrader om door de applicaties te gaan en na te gaan welke applicaties nu echt die toestemming nodig hebben, sommige applicaties zijn lachwekkend.

Afsluitend

Dit artikel heeft me enorm aan het denken gezet. Ik heb zelf veel van Google en Facebook hun services uitgezet en data verwijderd. Toch gebruik ik nog steeds Maps, omdat het nu eenmaal in de auto van mijn vader zit. Daarnaast denk ik dat het belangrijk is om niet helemaal door te slaan in mijn privacybubbel, maar dat we zeker met kleine dingen scherper kunnen zijn op ons gebruik. Ik geef niet meer direct toestemming en hoef niet altijd een gepersonaliseerde advertentie te hebben.

Ik heb het artikel een beetje vereenvoudigd en er zijn nog een hoop toevoegingen die ik uiteindelijk zou willen maken, maar dat zal voor een volgende versie zijn.

Voor nu kan ik je het boek 'Je hebt wel iets te verbergen' van Maurits Martijn en Dimitri Tokmetzis aanraden. Het komt uit 2016, maar is nog steeds akelig actueel.

Bronnen

1. Lees 1: DuckDuckGo: Tracker radar
2. Lees 2: Facebook shares messages between mother and daugher
3. Lees 3: Reading policy cost
4. Lees 4: NYT location data privacy
5. Lees 5: Credit Card MIT
6. Lees 6: Gizmo most honest ad
7. Lees 7: Airlines raising prices
8. Lees 8: Google surveillance toddler photo
9. Lees 9: Tesla workers shared images
10. Lees 10: Amazon Ring cameras used to spy
11. Zie 11: DuckDuckGo
12. Zie 12: Google activity