12.09.2016 • Leestijd 13 - 18 minuten

Stel je voor: tientallen onbekenden blijven achter je aan lopen in de winkel en noteren welke producten je bekijkt of afrekent. In ons boek *Je hebt wél iets te verbergen* laten we zien hoe je online doen en laten wordt gevolgd. En nu hebben we de populairste sites in Nederland onder de loep genomen. Deze stalkers en gluurders volgen ons allemaal.

Dit zijn de stalkers, gluiperds en snelle jongens die je de hele dag achtervolgen

Foto: Rein Janssen (voor De Correspondent)

Wat zou je doen als er plotseling 44 wildvreemden in je nek staan te hijgen en over je schouder meekijken als je de ochtendkrant openslaat?

Hoe reageer je als er uit het niets tientallen onbekenden achter je aan blijven lopen in de supermarkt en nauwgezet noteren welke producten je bekijkt en wat je in je karretje legt?

De afgelopen weken hebben wij de populairste sites in Nederland onder de loep genomen. Terwijl wij ons moederziel alleen en onbespied wanen, worden wij op het internet allemaal constant begluurd, geregistreerd, geanalyseerd en vooral: overal gevolgd. Eigenlijk precies zoals hierboven omschreven.

Advertentie- en analyticsbedrijven die met ons meekijken als we boodschappen doen, spelletjes spelen en nieuws bekijken, willen van ons weten wie wij zijn, wat onze voorkeuren zijn en hoe wij ons gedragen. Met deze informatie zijn zij in staat ons te verleiden om op hun advertentie te klikken of om onze

informatie door te verkopen aan adverteerders en datahandelaren.

Dit is big business. Bij elkaar besteden adverteerders inmiddels net zoveel op online media als op televisie, zo'n tweehonderd miljard dollar per jaar. Met behulp van trackers, digitale spionnen, kunnen bedrijven ons gedrag secuur in kaart brengen en leren ze internetgebruikers goed kennen en doorgronden. Welke sites bezoeken ze? Wat lezen, kijken en luisteren ze? Welke apparaten, apps en software gebruiken ze? Met wie communiceren ze? Op welke locatie bevinden ze zich? Hoe ziet hun sociale netwerk eruit? Maar ook: waar houden ze van? Wat kopen ze graag? Waar zijn ze gevoelig voor?

Je hebt wél iets te verbergen

We hebben de verborgen economie van het internet onderzocht en beschreven in ons boek, *Je hebt wél iets te verbergen*. Hierin beschrijven we onze zoektocht naar het belang van privacy die drie jaar geleden begon. Hoewel we beiden al jaren over privacy, technologie en surveillance schreven, hadden we moeite dat ene zinnetje te pareren: ik heb toch niets te verbergen? We voelden aan dat er van alles mis is met deze uitspraak, maar hoe laat je dat zien? Hoe bewijs je het belang van privacy?

Hoewel we beiden al jaren over privacy, technologie en

Drie jaar geleden besloten we onze apparaten - laptops, smartphones, routers, et cetera - figuurlijk open te breken. Konden we door de

surveillance schreven, hadden we moeite dat ene zinnetje te pareren: ik heb toch niets te verbergen?

datastromen te volgen ook het belang van privacy vinden?

Met het verschijnen van het boek keren wij terug naar het onderzoek waar het allemaal mee begon. In augustus 2013 onderschepten we de trackers op de honderd populairste sites in Nederland. In totaal vonden we zo'n tweehonderd, meestal onbekende, advertentie- en analyticsbedrijven die ons volgden.

Neem nieuwssite nu.nl. In totaal vonden wij daar in 2013 44 trackers, van bedrijven die recente surfgeschiedenis en ingevoerde zoektermen verzamelden, je type computer registreerden en je demografische gegevens achterhaalden. Twee bedrijven zeiden in hun privacyvoorwaarden daar 'persoonlijk identificerende informatie' aan te kunnen koppelen die zij van andere partijen kopen of ontvangen, zoals je naam, geboortedatum, je financiële situatie en informatie over je werkgever.

We waren nog vrij naïef

Eigenlijk stonden we er in 2013 nog vrij bleu in. Onze belangrijkste conclusie toen was dat deze online spionage buiten ons zicht om gebeurt. Zelfs de websitebeheerders van de populairste sites wisten niet door wie hun bezoekers allemaal gevolgd werden en welke informatie daarbij werd buitgemaakt.

Wat als we dit onderzoek opnieuw zouden doen? Hoe kijken we, na drie jaar intensief onderzoek, aan tegen deze

trackingeconomie? De verrassing is misschien weg, maar de conclusies zijn een stuk harder.

Dit keer gebruiken wij een meer geavanceerde meetmethode, die ontwikkeld is door onderzoekers van Princeton University. Het voordeel van deze methode is dat we de meting kunnen automatiseren en zo meer sites onder de loep kunnen nemen. Daarnaast gebruikt de software meerdere browsers en klikt deze ook op links op de websites zelf, zodat we een completer beeld krijgen van wat er op websites gebeurt.

We bezoeken 456 websites die populair zijn in Nederland en vinden iets meer dan 4.000 trackers van ruim vierhonderd verschillende bedrijven.

Op deze sites worden we het grondigst gevolgd.

En dit zijn de bedrijven die ons het dichtst op de huid zitten als we over deze sites surfen.

Door deze nieuwe methode en de grootte van de steekproef zijn wij beter in staat om onderscheid te maken tussen verschillende typen trackers. Zo zijn sommige gluurders actief op slechts één site, terwijl wij andere verspreid over tientallen websites tegenkomen. We komen een paar van de bekendste bedrijven ter wereld tegen, maar ook obscure digitale spionnen. Vier typen digitale spionnen zijn dominant op de populairste sites van Nederland. Wij noemen ze: de Big Brothers, de Snelle Jongens, de Stalkers en de Gluiperds.

Type 1: de Big Brothers van het

De Big Brothers zijn Facebook en Google, de absolute koningen van de wereldwijde online spionage. We vonden maar liefst 642 trackers van Google en 279 cookies van Facebook. We komen trackers van Google tegen op 306 verschillende websites, van nieuwssites tot pornoplatforms en van weersites tot webshops.

Google volgt internetgebruikers met verschillende trackers. De Googledochters DoubleClick en AdSense leveren advertenties op miljoenen sites. De bezoekers van die sites worden door de Googlecookies geregistreerd. Zelfde verhaal voor Google Analytics, dat gratis analysesoftware levert voor websites. En veel sites gebruiken lettertypen, kaarten of andere producten van Google waarop altijd trackers meeliften.

Met andere woorden: Google houdt niet alleen gebruikers van Googlediensten als de zoekmachine en Gmail in de gaten, maar zo goed als het hele internet.

Facebook en Google zijn de absolute koningen van de wereldwijde online spionage

Facebook zien we op 182 sites terug. En ook hier zijn alle soorten sites vertegenwoordigd. Kijk je porno op xhamster.com? Facebook noteert het. Koop je een boek bij Amazon? Facebook is erbij. Facebook kan je op zoveel pagina's volgen, omdat het een aantal adverteerders heeft opgekocht, maar vooral vanwege de vind-ik-leuk-knop. Al jaren volgt Facebook daarmee internetgebruikers buiten

Facebook om, leden en niet-leden.

We zijn geneigd Google en Facebook als hippe technologiebedrijven te zien, maar eigenlijk zijn het advertentiebedrijven. Waar je ook komt op het internet, aan de greep van Google en Facebook valt haast niet te ontkomen.

Beide bedrijven zeggen dat zij privacy hoog in het vaandel hebben. Wie Facebook en Google nauwgezet volgt weet: hun mooie woorden en beloften zijn je reinste bullshit.

Ter ere van Googles zestienjarige verjaardag analyseerden wij in september 2014 enkele beloften die het bedrijf gedurende zijn bestaan in het openbaar had gedaan. En we ontdekten een opvallend patroon. Een kleine greep:

- Oprichters Sergey Brin en Larry Page beloofden bij oprichting (1998) bij zoekresultaten geen advertenties te tonen. Die belofte werd in 2002 verbroken.
- Brin en Page beloofden bij advertenties geen gebruikersprofielen in te zetten. Die belofte werd in 2007 verbroken.
- Google zou nooit de data van de verschillende diensten – YouTube, Gmail, Calendar – samenvoegen. Die belofte werd op 24 januari 2012 verbroken, waardoor onderwerpen van onze intiemste mailconversaties nu verbonden kunnen worden met waar we ons bevinden.
- En Google beloofde niet zomaar informatie die het bedrijf verzamelt met DoubleClick te koppelen aan andere gegevens. Gebruikers moesten daar expliciet toestemming voor geven. Tot ook die belofte in juni 2016 werd verbroken.

Deze analyse hadden wij evenzogoed van Facebook kunnen maken. Dat bleek recent nog, toen Facebookdochter WhatsApp bekendmaakte dat gegevens over WhatsAppgebruikers toch met Facebook werden gedeeld.

Een uitgebreide Harvardstudie liet in 2015 zien dat de privacyvoorwaarden van Facebook in de loop der jaren consequent minder transparant zijn geworden. In 2009 paste Facebook bijvoorbeeld grondig de privacyinstellingen aan. Zuckerberg vertelde dat de instellingen werden vereenvoudigd om ze voor de gebruikers overzichtelijker te maken. Later bleek wat Zuckerberg bedoelde: met de nieuwe standaardinstellingen werden veel meer data over die gebruiker geanalyseerd dan voorheen. Zuckerberg bood later zijn excuses aan.

Dat moest hij ook doen in 2011, toen Facebook een schikking trof met de Amerikaanse toezichthouder FTC. Facebook had zijn klanten misleid, en niet zo'n klein beetje ook. Zo beloofde Facebook dat het data van gebruikers niet met adverteerders zou delen. Dat deed het wel. Het bedrijf verzekerde zijn gebruikers dat als zij hun accounts deactiveerden of verwijderden, hun foto's en video's niet meer konden worden bekeken. Dat bleek een leugen. En het bedrijf stelde gebruikers gerust door te beloven dat bepaalde informatie privé zou blijven. Ook dit bleek niet waar te zijn.

Conclusie: Facebook en Google verzamelen gegevens over nagenoeg alle internetgebruikers en verbreken consequent de beloften die zij doen over hoe zij met die gegevens om zullen gaan. Onder het mom van privacyvriendelijkheid.

Type 2: de Snelle Jongens

De Snelle Jongens zijn ook de snelste groeiers van de onlineadvertentiewereld: de bedrijven die onze data in milliseconden veilen.

Vlak onder de twee koningen van de online spionage, vinden we bedrijven als AppNexus (103 trackers), BidSwitch (56) en OpenX (47). Wat deze bedrijven doen, is werkelijk verbazingwekkend. Zij zijn zogenoemde *realtime bidders*. Op het moment dat jij een website laadt, gaat een signaal naar een veilingplatform dat iemand een gepersonaliseerde advertentie aan jou mag leveren. Aangesloten adverteerders - soms zijn dat er tientallen - mogen dan bieden op die ene advertentieplek. Ze kijken wie je bent, of ze je al kennen en of het interessant is je een advertentie aan te bieden. De adverteerders bieden dan tegen elkaar op en degene met het hoogste bod mag een advertentie leveren.

Dit gebeurt in de tijdspanne van een hartslag, nog voordat je een pagina laadt. En denk maar niet dat zo'n advertentie veel geld kost: we praten hier over fracties van centen.

We zien dit ongelooflijk complexe proces in actie als we 's avonds om half elf spelletjes.nl bezoeken. Omdat er meerdere advertenties worden geladen, kunnen we niet exact nagaan hoe de veiling verloopt, maar we zien wel dat er bijna dertig bedrijven actief zijn. We zien bijvoorbeeld ADNX verschijnen, een bedrijf dat de technologie voor de veilingen levert. We komen bedrijven tegen als Turn, AdRoll, Casale Media, Revenue Science, Eyereturn, Chango, Connexity en

Ligatus.

In dertig seconden maakt onze computer meer dan zeshonderd keer contact met hun servers om informatie te geven

Deze bedrijven zijn continu in gesprek met elkaar: in die dertig seconden maakt onze computer meer dan zeshonderd keer contact met hun servers om informatie te geven (over de trackers in onze browser, of de browser zelf, het besturingssysteem, de taalinstellingen en het land vanwaaruit we surfen).

Realtime bidding is een technologisch hoogstandje, maar kan hele vervelende neveneffecten hebben, zo leerden we de afgelopen jaren: het stelt fraudeurs in staat om virussen via advertenties te verspreiden. ‘Malvertising’ wordt dit genoemd, een samentrekking van ‘malware’ en ‘advertising.'

Dit is zorgelijk. Het betekent de facto dat argeloze sitebezoekers slachtoffer kunnen worden van cybercriminelen door simpelweg een site te bezoeken. Wat ook al een aantal keer gebeurde, zoals eerder dit jaar op een aantal grote sites, zoals nu.nl, marktplaats.nl en sbs6.nl. Reden voor het Nederlandse Nationaal Cyber Security Centrum om malvertising tot een van de vier opvallendste ontwikkelingen in de cybercriminaliteit te benoemen.

Malvertising - waar we binnenkort een uitgebreid artikel over zullen publiceren - laat zien hoe ongelooflijk complex adverteren is geworden. Voor de opkomst van realtime bidding, circa vijf jaar terug, had een website-eigenaar, bijvoorbeeld Sanoma (nu.nl) een contract met een

advertentietussenpersoon. Die regelde de advertenties. Sanoma had aardig door wie de bezoekers van nu.nl volgden.

Met realtime bidding is het voor websites haast onmogelijk om erachter te komen welke trackers er actief zijn. Veelzeggend vonden we de reactie van kinderwebsite studio100.be toen we ze er twee jaar geleden op wezen dat 54 cookies werden geplaatst bij het spelen van een paar spelletjes op hun sites. Als we meer informatie over deze cookies wilden, moesten we de *privacy policies* van deze 54 adverteerders maar lezen. Met andere woorden: Studio100 had ook geen idee.

Type 3: de Stalkers

De Stalkers zijn bedrijven die ons blijven volgen, op verschillende sites én verschillende apparaten.

In feite zijn bijna alle trackers stalkers: ze zijn bedoeld om je te blijven volgen. Maar in onze database duiken namen op van bedrijven die zich specifiek richten op wat zij eufemistisch de *customer journey* noemen. We gaan op reis en we nemen mee… een stel onzichtbare codes die ons niet meer loslaten.

Een van hen is Victor. Of, nou ja, wij noemen hem voor het gemak even Victor. Trackercode '441cf651-aa23-4195-9720-d8a460515f93' klinkt zo afstandelijk. Victor is namelijk een intieme vriend, een makker die ons op 31 verschillende websites volgt. Als we naar wehkamp.nl gaan, is Victor daar ook. Bezoeken wij zalando.nl, ja hoor, daar verschijnt hij een paar seconden later. Vervolgens treffen we hem aan op

volkskrant.nl, dropbox.com, geenstijl.nl, adobe.com, soundcloud.com, rtlnieuws.nl, nrc.nl, vi.nl, ebay.nl, trendnieuws.nl, tvgids.nl, kieskeurig.nl, blokker.nl en nog een reeks andere sites.

Een ander voorbeeld van een hardnekkige stalker: Drawbridge. Dit bedrijf koopt onder andere informatie in van andere adverteerders. Het zegt meer dan een miljard consumenten te volgen op meer dan vijf miljard verschillende apparaten. Als je 's ochtends opstaat en iets leest op je tablet, daarna in de trein op je smartphone en op je werk achter je laptop, wil Drawbridge dat weten. Niet alleen dat: Drawbridge heeft ook een database gemaakt van wie welke apparaten heeft, zodat anderen, tegen betaling, het trucje van Drawbridge kunnen herhalen.

In onze dataset zien we Drawbridge voor het eerst op forbes.com en dan wordt-ie vasthoudend. Kom je weleens op een van deze sites: monsterboard.nl, hotelspecials.nl, huffingtonpost.com, telegraph.co.uk, drimble.nl, vertalen.nu, deviantart.com, bcc.nl, autotrader.com, spelletjes.nl, trendnova.nl, spotify.com, tvgids.nl, vi.nl, trendnieuws.nl, adobe.com, voetbalzone.nl, reddit.com, ad.nl of msn.com? Zo ja, dan staan jij en je type smartphone, laptop of tablet in de database van Drawbridge.

Type 4: de Gluiperds

De Gluiperds zijn de bedrijven die ons bespioneren met geavanceerde technologieën die moeilijk zijn te detecteren.

Neem deze voorbeelden:

Als ze rechtstreeks in je brein zouden kunnen kijken, zouden ze dat niet laten

- Sommige websites geven je browser de opdracht een voor jou onzichtbare tekening te maken. Iedere browser doet dat op een net wat andere manier, waardoor de tekening uniek is, en ze je eraan kunnen herkennen. *Canvas fingerprinting* heet deze praktijk. Je kan niet verhinderen dat deze tekening wordt gemaakt.
- Hetzelfde geldt voor *audio fingerprinting*, waarbij je browser de opdracht krijgt een voor jou onhoorbaar audiosignaal te produceren. Ieder signaal is uniek en maakt herkenning mogelijk.
- En dan is er nog SilverPush. Deze adverteerder installeerde zijn software in apps voor smartphones en televisies. Wederom werd af en toe een onhoorbaar audiosignaal geproduceerd, bijvoorbeeld door je tv. Als de software op een van je andere apparaten staat, bijvoorbeeld je smartphone, pikt die het op. SilverPush weet dan dat die twee apparaten, je tv en smartphone, bij elkaar in de buurt zijn en dus waarschijnlijk tot hetzelfde huishouden behoren.

In onze dataset zijn we dit soort praktijken niet tegengekomen. Wél kwamen we een paar zeer brutale bedrijven tegen.

De bontste daarvan is misschien wel GumGum. Dit bedrijf scant foto's die op sociale media verschijnen. Het zoekt naar afbeeldingen van merken. Bijvoorbeeld beeld van dat je een blikje Coca-Cola drinkt. Die informatie wordt dan naar Coca-Cola verstuurd, aangevuld met allerlei socio-demografische gegevens waarmee de frisdrankfabrikant gericht klanten kan benaderen.

We vinden GumGum onder andere op mobiel.nl, centerparcs.nl, forbes.com, bax-shop.nl, huffingtonpost.com en youtube-mp3.org.

Deze voorbeelden laten zien dat sommige bedrijven weinig scrupules hebben. Als ze rechtstreeks in je brein zouden kunnen kijken, zouden ze dat niet laten.

Vier redenen waarom dit een probleem is

Toen wij drie jaar geleden ons onderzoek uitvoerden, hadden we nog geen bevredigend antwoord op de vraag: waarom is dit nou eigenlijk een probleem?

Als alles wat wij online doen wordt geregistreerd, dan is dat een privacyprobleem én een directe bedreiging voor de vrijheid van informatievergaring

De afgelopen jaren hebben we de volgende lessen geleerd:

- **Ten eerste hebben deze dataslurpers een gigantische technische infrastructuur opgebouwd die gericht is op surveillance.** Echt iedere stap die je online neemt, wordt door verschillende partijen gevolgd. En niet alleen door adverteerders. Ook criminelen en overheden hebben deze infrastructuur ontdekt. Criminelen verspreiden virussen via de advertentienetwerken. Inlichtingendiensten bespioneren bedrijven als Google, Facebook en advertentiebedrijven die ons bespioneren. En dat niet

alleen: Big Data is doorgedrongen tot andere takken van de overheid.

- **Ten tweede hebben we het hier over informatie- en machts-asymmetrieën.** Terwijl wij niet zien hoe overheden en bedrijven informatie over ons verzamelen, leren zij ons steeds beter kennen. En vergis je niet: onze data worden gebruikt om beslissingen over en voor ons te nemen. In de woorden van Helen Nissenbaum en haar collega Finn Brunton: 'Diegenen die ons kennen, hebben macht over ons. Zij kunnen ons een baan ontzeggen, een lening onthouden, onze bewegingen inperken, ons onderdak, lidmaatschap en onderwijs weigeren. Zij kunnen onze toegang tot het goede leven beperken.'
- **Ten derde maakt deze commerciële surveillance álle surveillance 'normaal.'** Geregeld horen we politici zeggen dat het wel meevalt met de inbreuk op de privacy als ze met een nieuwe maatregel komen: mensen geven toch ook gewoon dezelfde gegevens aan Google en Facebook? En hoe vaak horen we mensen niet verzuchten dat 'ze' toch al alles van ze weten. Maar privacy is een universeel mensenrecht, geen bevlieging uit een ver verleden. En daar zijn goede redenen voor. Zonder privacy geen vrijheid van meningsuiting, geen rechtsstaat of gezonde democratie.
- **Tot slot staat de spionage van de Big Brothers, de Snelle Jongens, de Stalkers en de Gluiperds voor iets groters: een nieuwe maakbaarheidsgedachte.** Het idee daarvan is dit: als je maar genoeg data hebt van mensen, kunnen ze je indelen in verschillende categorieën en op basis daarvan

verschillend behandelen. Niet voor niets luidt de slogan van de baas van de Nederlandse Belastingdienst: 'Iedere belastingplichtige de behandeling geven die hij verdient.'
De Canadese socioloog David Lyon noemt dat *social sorting*. Bedrijven proberen de winstgevende klanten van de verliesgevenden te onderscheiden. Overheden maken onderscheid tussen risicoburgers en niet-risicoburgers. De Belastingdienst rekent uit wie mogelijke fraudeurs zijn. Aan de grenzen probeert de bewaking snel onderscheid te maken tussen de reizigers. Wie zijn onschuldige vakantiegangers en wie mogelijke criminelen en terroristen?
Maar wat als de gegevens niet kloppen? Wat moet je doen als de computer je onterecht als fraudeur of verdachte aanmerkt? En jij ook als zodanig wordt behandeld?

Dit laatste is misschien wel de belangrijkste conclusie van ons boek. Social sorting leidt tot problemen waar we nog onvoldoende antwoord op hebben. Als verzekeraars mensen op basis van hun data gaan weigeren omdat ze het risico te groot vinden, dan is dat niet alleen een privacyprobleem, maar staat ook het wezen van verzekeren zélf onder druk: solidariteit.

Als grensbewakers en politie in toenemende mate mensen gaan tegenhouden, dan is dat niet alleen een privacyprobleem, maar ook een van discriminatie en gelijke behandeling. Als alles wat wij online opzoeken, lezen en bekijken wordt geregistreerd, dan is dat niet alleen een privacyprobleem, maar ook een directe bedreiging voor de vrijheid van informatievergaring.

Bedenk dus dat je iedere keer dat je jouw favoriete site bezoekt, de immer hongerige surveillancemachine voedt met data over wie je bent, wat je doet en wat je drijfveren zijn. En besef: je hebt wel degelijk iets te verbergen.

Foto: Rein Janssen

Meer hierover?

Lees ook: