

De datarevolutie



Big Data & Privacy

Nils Boonstra

2014



Grondwet Artikel 10

Iedereen heeft recht op rust en privacy. In de wet kunnen uitzonderingen staan. In de wet kan ook staan dat iemand anders uitzonderingen mag maken.

De overheid mag persoonlijke gegevens van iemand niet zomaar gebruiken.

Iedereen heeft er recht op te zien wat er over hem is vastgelegd. En kan gegevens laten veranderen als ze niet juist zijn.

In dit artikel staat dat iedereen het recht heeft om in de beslotenheid van zijn persoonlijke levenssfeer met rust te worden gelaten en om bijvoorbeeld niet te worden afgeluisterd.

De persoonlijke levenssfeer omvat onder meer:

- Het huis
- De briefwisseling
- De communicatie via telefoon en andere communicatiemiddelen
- Het recht om niet te worden bespied of afgeluisterd
- Het recht op zorgvuldige behandeling van persoonlijke gegevens
- Het recht op eerbiediging van het innerlijk leven
- Het recht op eerbiediging van de lichamelijke integriteit

Mensenrechten Artikel 12

Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.

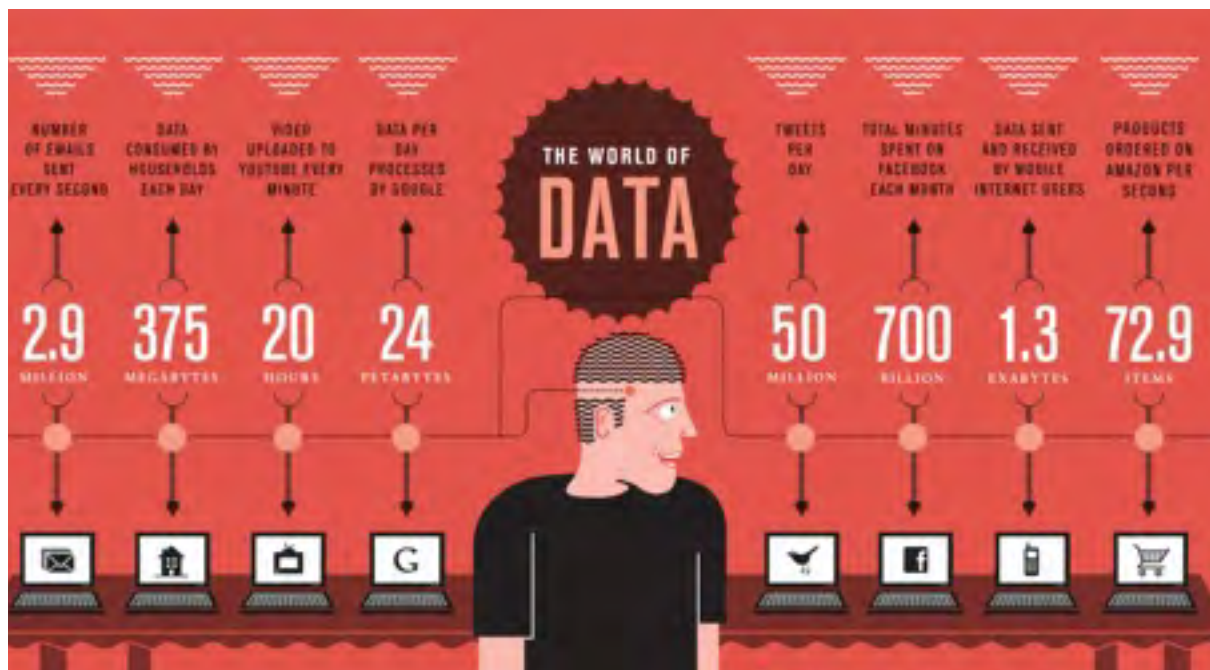
Inhoud

De datarevolutie	1
Grondwet Artikel 10	2
Mensenrechten Artikel 12	2
Inhoud	3
Wat zijn Big Data?	4
Wat is privacy?	5
Wat weten bedrijven van je?	6
Bank	8
Verzekering	10
Slimme meter	11
Terrorisme	13
Angst	13
Legaliteitsbeginsel	14
Zwarte lijst	14
Censuur	15
SMS in de Oekraïne	16
Zelfcensuur	16
Geheime diensten	17
Wat gebruiken ze?	17
‘I’ve got nothing to hide’	19
Toekomst	20
Politie en overheid	20
Reizen	21
Sousveillance	21
Wat kun je zelf doen?	22
Encryptie	23
Tor	25
Conclusie	27
Bronnen	28

Wat zijn Big Data?

Door de onthullingen van Edward Snowden vorig jaar raakte ik geïnteresseerd in het onderwerp privacy op het internet. Daarvoor had ik er eigenlijk nog nooit over nagedacht hoe het komt dat diensten als Facebook en Google gratis kunnen zijn. Ik keek een paar documentaires op het internet en las steeds meer artikelen in tijdschriften en kranten over dit onderwerp. Twee woorden kwamen hierbij steeds naar voren: Big Data.

Big Data is een nieuw fenomeen in de computerwereld, waar steeds meer gebruik van wordt gemaakt. Het gaat bij Big Data om grote hoeveelheden gegevens die met een grote snelheid worden gegenereerd en een grote diversiteit kennen. Ook speelt de mogelijkheid tot analyse een belangrijke rol. Een voorbeeld van Big Data zijn de pintransacties van grote winkelketens. Door die data te analyseren kunnen verbanden worden gevonden, bijvoorbeeld een combinatie van bepaalde weertypen met de verkoop van bepaalde producten, waar de winkel op in kan spelen. Of Facebook, die door verbanden te leggen kan voorspellen wie je mogelijk al kent en als vriend zou kunnen toevoegen. Maar Big Data kent meer toepassingen, je kunt er bijvoorbeeld de reistijd mee berekenen van de snelweg tot het centrum van een stad door middel van camera's die nummerborden registreren en daarbij de tijd ook doorgeven. Big Data zou je kunnen vergelijken met een hooiberg van data, waar data-analisten de waardevolle naalden in zoeken. Door de steeds sneller wordende computers gaat dat elke dag beter en efficiënter.



Ik ga kijken wat de invloed van Big Data is op onze privacy. En wat je kunt doen om jezelf meer privacy te geven online.

Wat is privacy?

De Van Dale omschrijft privacy als: de persoonlijke vrijheid, het ongehinderd, alleen, in eigen kring of met een partner ergens kunnen vertoeven; gelegenheid om zich af te zonderen, om storende invloeden van de buitenwereld te ontgaan, een toestand waarin een mens er zeker van is dat zonder zijn toestemming zo weinig mogelijk andere mensen zich op zijn terrein zullen begeven. Daarbij komt tegenwoordig: zelf bepalen wie welke informatie over ons krijgt, en de wens onbespied en onbewaakt te leven.

Privacy en veiligheid worden vaak door de overheid voorgesteld als aan elkaar tegengestelde waarden. Anderen zeggen juist dat het voor de veiligheid en voor de democratie nodig is dat mensen zich onbespied voelen. Burgers moeten zich vrij kunnen bewegen en in vrijheid hun gedachten en meningen kunnen uiten, zonder dat dit tegen ze kan worden gebruikt.

De grote hoeveelheid wetten en regels die is ingevoerd in het kader van terrorismebestrijding leidt tot maatregelen die de privacy beperken. Ook de grote hoeveelheid persoonsgegevens op het internet zet de privacy onder druk. De verleiding om deze gegevens te gebruiken voor andere doelen dan waarvoor ze bedoeld zijn is groot. Dat geldt voor bedrijven en overheden, maar ook voor criminelen (identiteitsdiefstal).

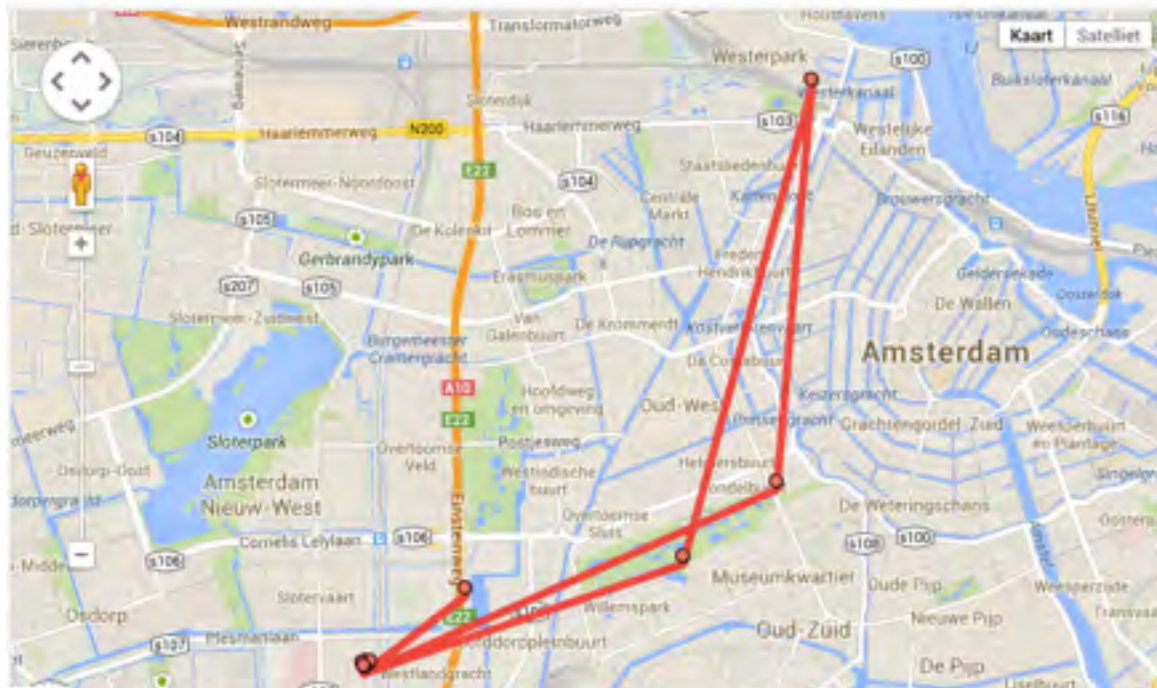
Het steeds verder verzamelen van gegevens leidt tot een profiel voor elke burger. Op basis van dit profiel worden beslissingen genomen over die burger, ook zonder dat hij of zij dat weet. De overheid en haar diensten kunnen fouten maken of gegevens niet goed beveiligen. Dat zorgt voor een afname van de privacy.

Wat weten bedrijven van je?



Bedrijven weten steeds meer over hun klanten. Op basis van zoekgedrag, browsegedrag en smartphones is het mogelijk om van iedereen een profiel op te stellen. Internetbedrijven maken daar gebruik van door gerichte reclames aan te bieden.

Bij Google is het zo dat je advertenties te zien krijgt waar je waarschijnlijk in geïnteresseerd in bent. Dat weten ze door je mail te scannen, je zoekwoorden te filteren en zogenaamde 'tracking cookies' te plaatsen, die volgen welke sites je bezoekt. Als je een Android smartphone hebt weten ze ook waar je bent (via GPS of locatiebepaling met telefoonmasten) en met wie je contact hebt.



Mijn eigen locatiegeschiedenis bij Google op 3 januari 2014

De profielen die ze op die manier samenstellen worden gebruikt voor reclames of worden doorverkocht aan andere bedrijven. Google is hierin niet de enige, elke grote website of app doet dit. Veel diensten op internet zijn gratis, en met alle data die ze over je verzamelen verdienen ze hun geld. Het bijhouden van gegevens over je klanten gebeurt al langer, met kortingspasjes of bonuskaarten. Het nieuwe is dat het nu bij iedereen gebeurt, en veel mensen zich er niet bewust van zijn, wat ze makkelijker beïnvloedbaar maakt.

Veel onbekender zijn de zogenoemde 'tracking'-bedrijven. Op elke site zijn er wel een paar te vinden, soms wel tientallen. Eén van deze bedrijven is BlueKai. Via sites zoals Nu.nl plaatst BlueKai een cookie op je computer, een klein stukje software. Die stuurt alles wat je in de browser doet, welke sites je bezoekt en waar je op klikt door naar BlueKai. Dat bedrijf maakt dan op basis van die data profielen aan die ze gebruiken om gerichte advertenties te plaatsen of ze verkopen deze data door. Bedrijven die de data kopen koppelen er dan bijvoorbeeld adressen of telefoonnummers aan.

BlueKai Audience Data Marketplace: Data Types

Data Type	Description	Availability	Qualification	Segmentation
Intent	Consumers who intend to buy a particular product or service in the near term.	100+ million unique	Actions indicating intent to buy on top tier e-commerce, financial, retail, online travel agency sites. Sample actions include interactions with a search function (either via search widget, or entering in a keyword), product comparison, item calculations, etc.	Auto's (e.g. by Make and Model) Financial services (e.g. loans, mortgages, investment products) Travel (e.g. by departure/destination city, length of stay, air travel, hotel, rental cars and more) Education (e.g. by education products and services) Retail (e.g. by product type, categories, brands) Local Goods & Services (e.g. by products and services) Real Estate (e.g. intent to purchase or rent)

Bij deze bedrijven kun je complete profielen kopen, met data die gebruikers zelf beschikbaar hebben gesteld. Maar vaak gaat dat beschikbaar stellen onbewust of staat het ergens ver weggestopt in de 'algemene voorwaarden' die iedereen moet accepteren om een bepaalde dienst te kunnen gebruiken.

Een cookie stuurt ook de gegevens mee over welke browser je gebruikt en welke computer je gebruikt. Daar maken sites waar je online hotels en vakanties kan boeken gebruik van. Mensen met een Apple computer betalen soms wel 30% meer voor dezelfde hotelkamer, omdat bekend is dat ze meer geld over hebben voor een hotel en het makkelijker uitgeven. Op die manier ontstaan er (grote) prijsverschillen die afhankelijk zijn van je computer, browser en van het profiel dat er van je gemaakt is.

Een ander bij het grote publiek onbekend bedrijf, Experian, verzamelt van Nederlandse huishoudens alle data die ze kunnen vinden en maakt daar profielen van. Aan de hand van die profielen bepalen o.a. de banken of je kredietwaardig bent of niet. Maar zelf heb je daar niets over te zeggen, een computer zegt ja of nee en er is geen verdere discussie mogelijk.

Maar ook offline gebruiken winkels steeds meer data van klanten, via bonuskaarten of door klanten te volgen met wifi in de winkel. De Amerikaanse winkel Target kan bijvoorbeeld op basis van gekochte producten voorspellen of een vrouw zwanger is, en tot op de maand precies berekenen wanneer ze gaat bevallen. Zo kreeg iemand in Minneapolis een folder bezorgd met kortingsproducten voor babyspullen. De folder bleek voor zijn dochter te zijn die nog op de middelbare school zat. De man belde boos op naar Target en zei dat ze die folder helemaal niet wilden hebben. Later had hij het er met zijn dochter over en ze bleek inderdaad zwanger te zijn. Target wist in dit geval dus, door slim om te gaan met data van verkochte producten, eerder dat het meisje zwanger was dan haar vader.

Ook de Engelse supermarktketen Tesco heeft grote plannen met Big Data. Bij de tankstations wil het bedrijf camera's ophangen die de gezichten van mensen scant. Op basis van die scans worden de mensen ingedeeld in verschillende categorieën gebaseerd op leeftijd, geslacht en andere uiterlijkheden. De camera's sturen deze informatie door naar een beeldscherm waar dan een reclame op verschijnt die bij de persoon past, een reclame van Lego voor een jongen van acht bijvoorbeeld.

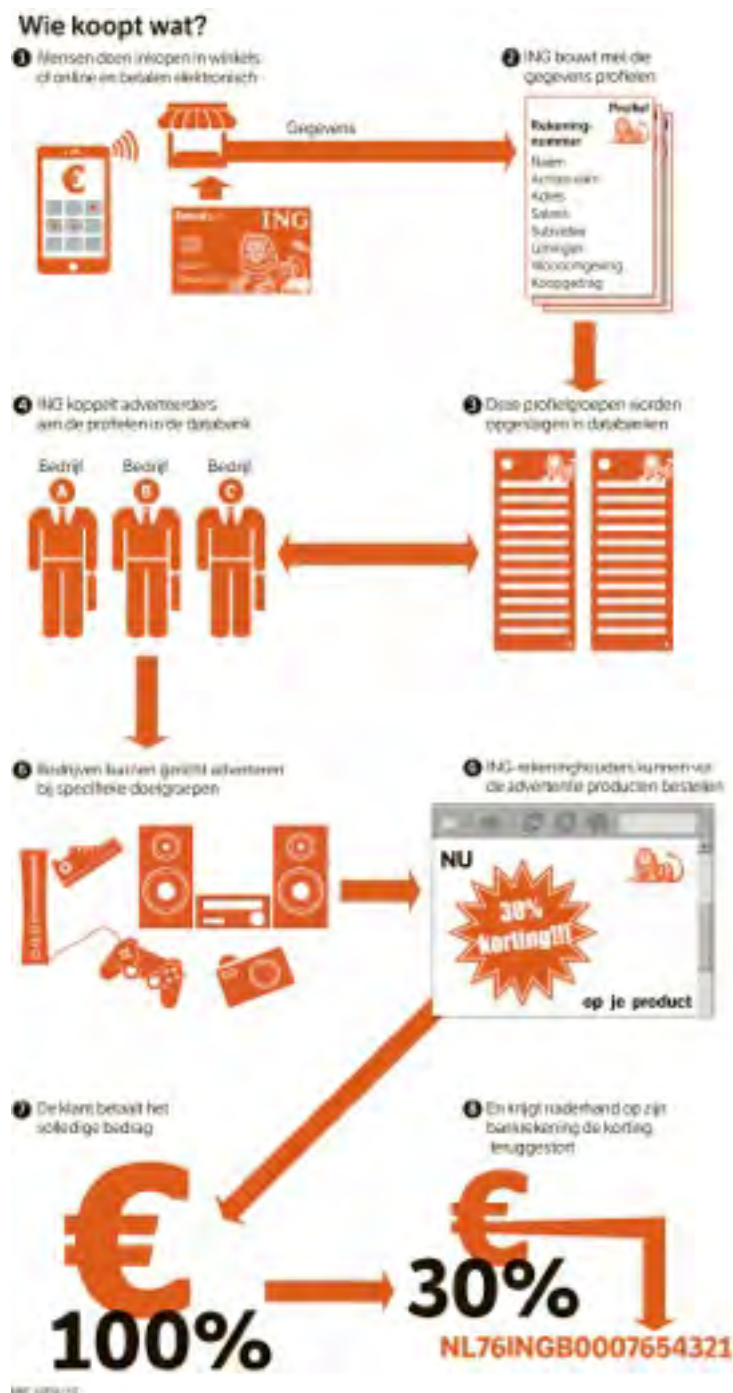
McDonalds heeft voor de Amerikaanse drive-ins een systeem ontwikkeld waarbij een camera scant welke merk auto uit welk bouwjaar en met hoeveel personen erin aan komt rijden. Op basis van die scan berekenen ze welke producten er gaan worden besteld die dan alvast klaargezet kunnen worden. In tachtig procent van de gevallen hebben ze het goed. Webwinkel Amazon is van plan om in de toekomst pakketjes al te versturen voordat ze besteld zijn. Op basis van alle gegevens die ze van hun klanten hebben kunnen ze voorspellen wat je gaat kopen en zetten ze een boek dat je waarschijnlijk wilt kopen alvast klaar in het dichtstbijzijnde distributiecentrum, waardoor de leveringstijd zou kunnen halveren.

Bank

ING wil de data van klanten gaan gebruiken om te verkopen aan adverteerders. Daarbij gaat het om data zoals hoeveel je koopt, waar, op welke plek en op welk tijdstip. 'Een tuincentrum wil graag weten dat je elk jaar in maart 150 euro uitgeeft aan tuinspullen. Hij kan dan op het juiste moment een scherp aanbod doen,' zei de directeur van ING in een interview. ING wil op basis van alle gegevens die ze hebben profielen maken van hun klanten. Bij diensten als Gmail en Facebook gebeurt dit al heel lang, maar voor een bank is het nieuw.

Op dit plan zijn vragen gekomen uit de maatschappij, bijna iedereen was tegen dit plan, van De Nederlandse Bank tot de overheid. Want bij een bank is het vertrouwen dat je gegevens er veilig zijn erg belangrijk.

ING heeft jouw financiële gegevens en wil deze verkopen, en de klant krijgt af en toe een voordeeltje, voor iedereen goed zou je kunnen denken. Maar als je gegevens door de ING verkocht worden, kunnen verzekeringsmaatschappijen er misschien ook wel in kijken, en ligt je koopgedrag voor een klein prijsje op straat. ING wil ook klanten met veel spaargeld en een goed inkomen minder rente laten betalen op leningen, omdat de kans dat ze het terugbetalen aanzienlijk groter is. Dat klinkt fijn, maar betekent ook dat mensen die het lastig hebben, en dus minder goed de lening terug kunnen betalen meer rente moeten gaan betalen. Voor hen zal het dus alleen maar lastiger worden. Dat ING dit doet is wel begrijpelijk. Er valt voor de bank veel geld te verdienen met klantendata.



In de VS gebruiken veel banken deze technieken al, daar is het heel gebruikelijk om een aanbieding van je bank te krijgen. Maar of het ook voor een vertrouwensinstelling als een bank een goed idee is om zo met de privacy van de klanten om te gaan, is nog maar de vraag. ING zelf zegt dat ze voor alles toestemming zullen vragen aan de klanten, en dat de data anoniem aan de adverteerder wordt verkocht. Die adverteerders krijgen daarbij ook niet de data zelf, maar ze kunnen zelf een doelgroep uitkiezen die dan een reclame van de ING te zien krijgt. Net zoals je bij Gmail reclame voor auto's krijgt te zien als je het in mailtjes hebt over het mogelijk kopen van een nieuwe auto. Andere banken zoals ABN-Amro en Rabobank hebben ook al plannen voor het gebruik van klantendata, maar alleen dan voor eigen gebruik.

Het grootste probleem is dat je, als je niet mee wilt doen aan deze plannen, in de toekomst misschien meer moet betalen voor je rekening of dat je dan geen aanbiedingen meer krijgt toegestuurd. Het zou ook heel makkelijk kunnen dat er discriminatie optreedt. Bijvoorbeeld: een verzekeringsbedrijf doet een aanbieding voor een goedkopere verzekering, maar alleen voor mensen met een hoger dan gemiddeld inkomen en die niet bij McDonalds komen. Deze plannen kunnen gevolgen hebben die nu nog niet te bedenken zijn, en daarom is het goed hier niet zomaar mee akkoord te gaan. Er moet goed over worden nagedacht en het moet ook duidelijk zijn voor klanten wat er precies gebeurt. Ook moet het makkelijk zijn om hier niet aan mee te doen, want voor veel mensen is het teveel moeite om van bank te wisselen.

Kortom, een interessante ontwikkeling die in de toekomst bij steeds meer bedrijven zal worden toegepast. Maar ook een ontwikkeling om goed in de gaten te houden, want het wordt al gauw ondoorzichtig en het kan vervelende gevolgen hebben.

Verzekering

Een ander voorbeeld: de 21-jarige Daniël kreeg kanker. Na twee jaar was hij genezen maar toen hij zijn zorgverzekering wilde wijzigen werd hij overal geweigerd. Bij het ONVZ werd hij vergeleken met een 'brandend huis'. Nu is het nog zo dat hij al ziek is geweest, maar in de toekomst zou het kunnen dat hij nog gezond bent en toch wordt geweigerd. Bijvoorbeeld als uit je DNA blijkt dat je een grote kans hebt op een ziekte, of dat je tot een risicogroep behoort. Zorgverzekeraars willen steeds meer gegevens van klanten hebben, om in te kunnen schatten hoeveel geld ze het bedrijf gaan kosten.

Klanten die een groot risico hebben om verlies op te leveren moeten meer premie betalen of worden geweigerd. Een groep verliesgevende klanten zijn bijvoorbeeld mensen met migraine. In de toekomst zou het zo kunnen zijn dat je je medische gegevens, verzameld door je smartphone of een ander apparaat, deelt met je zorgverzekeraar. En dat je als je dat niet doet geen korting krijgt of meer premie moet betalen. Dit zou er voor zorgen dat de zorg minder betaalbaar wordt voor de mensen die het echt nodig hebben.



Slimme meter

Tussen nu en 2020 krijgt ieder huishouden in Nederland een slimme energiemeter. De EU heeft als richtlijn dat 80% van alle huishoudens in 2020 een slimme meter moet hebben. Het idee achter deze meter is dat het energiegebruik beter inzichtelijk wordt, via de pc of smartphone kun je zien hoeveel energie je gebruikt en wanneer. De netbeheerder hoeft niet meer langs te komen voor controles, de gegevens worden automatisch doorgestuurd naar de energieleverancier. Maar er zitten ook nadelen aan deze meter. Zo kun je aan het stroomgebruik zien of er iemand thuis is, of hoe laat iemand gaat slapen. Als je beter naar de grafieken kijkt is het zelfs te zien of de energie door de televisie of door de wasmachine wordt gebruikt.

Dat is misschien handige informatie voor de gebruiker, maar ook voor de leverancier. Het kan verstrekkingen hebben, zo zag een man die zo'n meter in huis had dat zijn kinderen de afspraken over televisiekijken niet altijd nakwamen en dat de schoonmaker minder werkte dan afgesproken was. Dat kun je fijn vinden om te weten, maar het maakt je ook tot spion van je eigen huis.

Bedrijven weten steeds meer over hun klanten. Google weet van iedereen met een Android telefoon waar ze zijn. Ze weten ook met wie je contact hebt, wat je interesses zijn, wanneer je opstaat en zelfs wat je in de toekomst gaat kopen door de zoekopdrachten slim te gebruiken. Facebook kan op basis van gemeenschappelijke vrienden berekenen met wie je een relatie hebt, of gaat hebben. In 33% van de gevallen hadden ze het goed voorspeld. Facebook oprichter Mark Zuckerberg zei ooit eens dat privacy dood is.

Maar ook andere bedrijven zoals Equens, de beheerder van de pinbetalingen in Nederland, weten veel. Ze weten wat je koopt, op welke plek en hoe laat. Met de ov-chipkaart, smartphone en alle camera's in binnensteden weten bedrijven en de politie hoe mensen zich bewegen en waar ze zijn. Door een wet uit 2009 moeten telecombedrijven de metadata van al hun klanten, dat is met wie ze contact hadden, hoe lang en op welke plek, opslaan voor 12 maanden. Het gevolg van al deze dingen is dat er een enorme berg met data beschikbaar is, Big Data genaamd. Nu wordt daar nog niet heel veel mee gedaan, maar alles wordt opgeslagen en in de toekomst zal daar steeds meer uit gehaald kunnen worden.

Terrorisme

Na de aanslagen van 9/11 in New York is er veel veranderd. Hierna vond men dat er iets gedaan moest worden om dit soort aanslagen in de toekomst te voorkomen. De beveiliging op vliegvelden werd veel strenger, en er werden veel nieuwe regels ingevoerd, maar de grootste maatregel was het uitbreiden van de geheime diensten. In oktober 2002 voerde Europa en de VS een nieuwe wet in die het mogelijk maakte voor de CIA om iedereen zonder arrestatiebevel op te pakken en zonder rechtszaak op te sluiten in gevangenissen zoals Guantánamo Bay. Mensen werden opgepakt en gemarteld omdat ze een 'risicoprofiel' hadden, en daar kom je niet zomaar van af. 45 dagen na 9/11 voerde de VS al een andere wet door, de PATRIOT Act, die het mogelijk maakte mensen af te luisteren en zakelijke informatie te onderzoeken. Ook maakt de wet het mogelijk om alle data van bedrijven uit de VS op te vragen, ook data over Europese klanten van Google bijvoorbeeld.



Angst

Tegenwoordig probeert de overheid zo veel mogelijk data op te slaan uit angst voor terrorisme. Terrorismen en criminaliteit worden als argumenten gebruikt om overal camera's op te hangen en data van smartphones op te slaan. Maar de kans om te overlijden door te stikken in een pinda is groter dan de kans om door terrorisme te worden gedood. Meer camera's ophangen heeft ook niet veel effect op de criminaliteit, het is vooral heel duur. Uit angst voor het terrorisme worden er elk jaar miljarden aan terrorismebestrijding uitgegeven en moeten we daar veel privacy voor opgeven.

Dit komt mede doordat de media elke keer als er een aanslag is er een groot verhaal van maken, en politici daar dan iets tegen moeten doen. Als er een schietpartij is in een winkelcentrum kun je dat als politicus niet negeren. Dat lijkt allemaal positief, criminelen worden door technologie eerder opgespoord en kunnen sneller veroordeeld worden. Toch brengen al die databases ook nieuwe problemen met zich mee en het geval Ron Kowsoleea is daar een goed voorbeeld van.

Legaliteitsbeginsel

In 1994 gebruikte crimineel Imro C. de naam 'Ron Kowsoleea' toen hij werd opgepakt. De politie nam die naam over in het proces-verbaal en kwam er al snel achter dat hij een valse, gestolen identiteit had gebruikt. Toch deden ze verder niets met dit gegeven. Toen Imro in 2002 werd veroordeeld voor drugshandel stond die veroordeling dan ook op naam van Kowsoleea. Sindsdien is de echte Ron meer dan 40 keer aangehouden door de politie en is er met 35 man een inval in zijn huis gedaan. Het lijkt een film maar is een waargebeurd verhaal. Ron verloor zijn bedrijf, moest verhuizen en durfde voor lange tijd zijn huis niet meer uit. Hoe is het zo ver gekomen?

In het begin nam Kowsoleea het voorval niet erg serieus, maar toen het maar door bleef gaan ging hij rondvragen en kwam hij erachter dat zijn identiteit was gestolen. Hij liet de bestanden van de politie opschonen, maar het was al te laat. In Nederland zijn er 26 organisaties die hun systemen elke 24 uur synchroniseren, steeds als Kowsoleea werd verwijderd uit een database stond hij nog in een andere en een dag later stond hij er overal weer in. Het heeft 15 jaar geduurd voordat hij als crimineel uit de systemen was verwijderd. Identiteitsfraude komt steeds vaker voor, en als je eenmaal in de bestanden van Justitie staat kom je er bijna niet meer uit. Dan moet je zelf zien te bewijzen dat je onschuldig bent, wat tegen het legaliteitsbeginsel in gaat, dat je onschuldig bent tot dat het tegendeel bewezen is. De overheid heeft veel macht, en dat gaat niet altijd goed.

Zwarte lijst

In bepaalde systemen is iedereen straks Groen, Oranje of Rood. En ben je eenmaal Rood dan kom je daar bijna niet meer van af, zoals Kowsoleea is overkomen. Op vliegvelden worden al systemen ontwikkeld op basis van dit groen, oranje, rood systeem. Mensen zonder risico mogen doorlopen, mensen met een klein risico worden in de gaten gehouden en mensen met een groot risico worden apart genomen voor een gesprek in een kamertje. De risicofactor wordt al bepaald bij het boeken van de reis, lang voordat je op het vliegveld aan komt. Ook wordt er met een zwarte lijst gewerkt (op de Europese zwarte lijst staan meer dan een miljoen mensen) die een land niet in mogen.

Censuur

Nieuwe technologieën kunnen ook gebruikt worden voor censuur, omdat overheden de bevolking wil beschermen of niet willen dat de inwoners bepaalde dingen weten. Het bekendste voorbeeld daarvan is China, dat Twitter, Facebook, Google en veel Japanse en Tibetaanse websites blokkeert, de zogenaamde 'Great Firewall'. In totaal worden er ongeveer 18.000 websites geblokkeerd. Ook landen als Iran, Saudi-Arabië en Syrië censureren het internet op die manier. Er zijn ook andere manieren van censuur, zo is er in 2013 in Engeland een internetfilter ingesteld om kinderen tegen porno te beschermen.

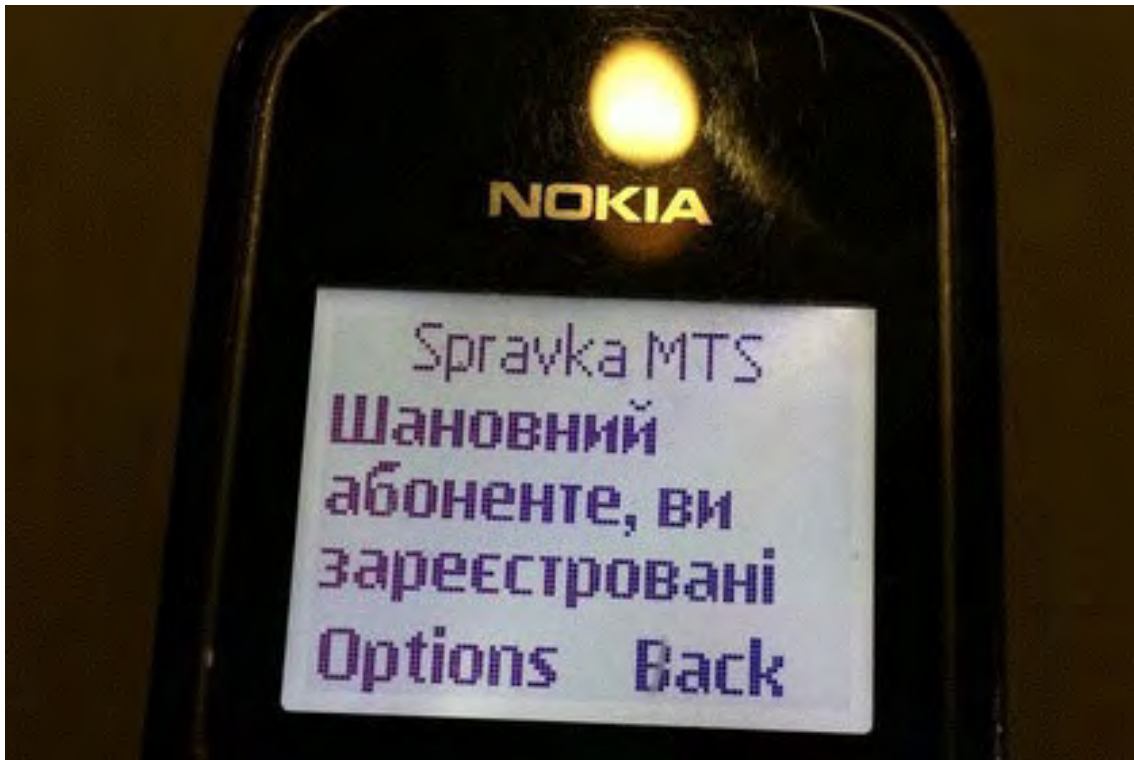
Dit filter was echter te strikt ingesteld en blokkeerde ook sites met informatie over homoseksualiteit, drugs en forums over huiselijk geweld. Torrent sites worden door sommige providers ook geblokkeerd. Dit filter staat automatisch aan en het kost veel moeite om het uit te zetten. Ook is het zo dat als het filter er eenmaal is, de lijst met geblokkeerde sites makkelijk uitgebreid kan worden.

Er zijn ook filters van softwarebedrijven die ouders, werkgevers en scholen op computers kunnen installeren om hun computers toegang tot websites te weigeren. Aan de lijsten van deze software kunnen ook heel makkelijk sites worden toegevoegd waarvan de overheid liever niet heeft dat je ze bezoekt.

In Frankrijk was er tot juli 2013 een wet die er voor zorgde dat je van het internet werd afgesloten als je drie keer iets illegaal downloadde. Door dit soort wetten en filters kan er makkelijk misbruik worden gemaakt van de angst voor porno of andere dingen en komt de vrijheid van het internet in gevaar.

Bij Facebook is het zo dat je alleen de berichten te zien krijgt die Facebook denkt dat je wil zien. Denkt Facebook bijvoorbeeld dat je politieke voorkeur rechts is, dan zal je minder snel berichten van een 'linkse' vriend zien. Ook dit is een vorm van censuur, alleen misschien niet heel schadelijk. Het gevolg is wel dat je alleen nog maar de mensen ziet die het met je eens zijn en er geen kritiek meer langs komt.

SMS in de Oekraïne



Nieuwe technologie heeft ook op andere gebieden invloed, bijvoorbeeld bij protesten. In januari 2014 waren er in de Oekraïne protesten tegen de regering, en die was daar niet erg blij mee. Enkele dagen na de grote protesten kregen betogers een sms'je met daarin dat ze geregistreerd waren 'als deelnemer aan massale verstoringen' (zie afbeelding). De overheid kon dat doen omdat ze van iedereen kunnen zien waar hun mobieltje zich bevond op het moment van de protesten, en zo konden ze dus weten wie er bij de protesten betrokken waren. Door een noodwet was protesteren strafbaar gemaakt. Je kunt dus beter je telefoon thuis laten als je gaat protesteren.

Zelfcensuur

Iets wat veel voor kwam in de voormalige staat DDR was zelfcensuur. Mensen waren bang voor geheime agenten op straat en durfden daarom geen kritiek meer te uiten. Tegenwoordig zijn daar geen geheime agenten meer voor nodig, de smartphone vervult nu die rol. Als iemand iets doet of zegt wat opvalt worden er meteen foto's of video's van gemaakt. Die kunnen vervolgens heel makkelijk op YouTube of Facebook worden gezet. In de toekomst zal dat alleen maar meer worden, met bijvoorbeeld de bril van Google (Google Glass) die ook een camera heeft en alles kan filmen. Ook hangen er tegenwoordig op elke straathoek en in elke winkel camera's. Daardoor worden mensen bewust of onbewust toch beïnvloed en gaan ze zich anders gedragen, zelfcensuur.

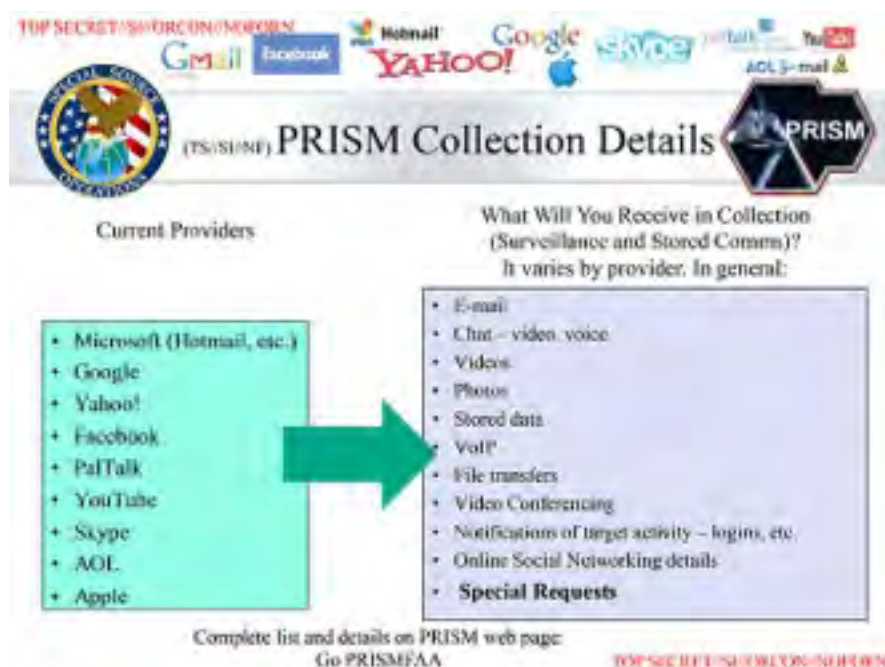
Geheime diensten

Sinds de aanslagen van 9/11 zijn de budgetten voor geheime diensten sterk gestegen. En omdat het nu heel makkelijk is geworden om te spioneren door alle digitale apparaten kunnen ze iedereen in de gaten houden. De geheime diensten gaan ervan uit dat hoe meer ze weten, hoe beter ze aanslagen kunnen voorkomen. Het in de gaten houden van mensen is ook een stuk makkelijker geworden. Grote internetbedrijven hebben veel data van hun gebruikers en die kunnen geheime diensten opvragen, wat ze dan ook voortdurend doen.

Het probleem van geheime diensten is volgens mij dat ze aan symptoombestrijding doen. Ze proberen aanslagen te voorkomen maar daardoor wordt er niet meer nagedacht wat 'terroristen' zo ver brengt een aanslag te plegen waarbij ze waarschijnlijk ook zelf om het leven komen. Ze proberen de aanslagen te voorkomen, maar het echte probleem wordt in 'The war on terror' vergeten.

Wat gebruiken ze?

Dankzij de onthullingen van Edward Snowden is er nu een beter beeld van welke middelen de geheime diensten, en dan met name de NSA, gebruiken. En het blijkt dat als iets mogelijk is, ze het ook doen. Er is weinig toezicht op geheime diensten en er wordt niet veel nagedacht of iets wel nodig is en of het wel mag.



Prism, het systeem dat de NSA van informatie voorziet van alle grote Amerikaanse internetbedrijven.

De meest gebruikte manier om data te krijgen blijkt via de internetgiganten te zijn, grote bedrijven worden betaald om hun data direct naar de NSA door te sturen, en anders worden ze gedwongen via de PATRIOT act. Maar het blijkt veel verder te gaan dan dat, sommige sciencefiction schrijvers zeggen zelfs dat ze het tempo van veranderingen niet meer bij kunnen houden.

Agenten van de NSA houden online games in de gaten omdat ze mogelijk gebruikt zouden kunnen worden door terroristen om te overleggen. Maar ze gebruiken ook speciale apparatuur om mensen af te luisteren. Een NSA agent kan bijvoorbeeld uit een catalogus van meer dan 50 producten kiezen, speciaal voor en door de Amerikaanse geheime dienst gemaakt. Die producten kunnen kleine microfoontjes zijn, maar ook routers die alle data doorsturen naar de geheime dienst. De NSA blijkt ook orders te onderscheppen en er af luisterapparatuur of software op te installeren.

Als de NSA een Amerikaan in de gaten wil houden en hij bestelt bij Amazon een nieuwe laptop, dan maakt de NSA dat pakketje open, stopt er een af luisterapparaatje in en verstuurt het naar de Amerikaan. Zo is het waarschijnlijk ook gegaan met de telefoon van Angela Merkel, die werd afgeluisterd door de Amerikanen. Ze kunnen ook computers en vrijwel alle andere elektronische apparatuur hacken. Dan kan de geheime dienst bijvoorbeeld meekijken met je webcam of worden alle toetsaanslagen doorgestuurd.

Dit alles wordt niet alleen door de NSA gedaan. Het is zo dat er over de NSA veel bekend is geworden door de onthullingen van Snowden en dat ze een groot budget hebben, maar soortgelijke dingen zullen andere geheime diensten zoals de AIVD en het Britse GCHQ ook doen. In Rusland en China net zo. Deze diensten werken voor een deel ook samen, omdat bijvoorbeeld de AIVD niet zomaar Nederlanders mag af luisteren. Maar de NSA mag dat wel. Dan sluiten ze een deal waarbij de AIVD data aan de NSA geeft die zij niet kunnen krijgen en omgekeerd.

‘I’ve got nothing to hide’

Bij discussies over privacy zie je enkele argumenten vaak terugkomen. De één is bang voor 'Big Brother', en de ander antwoordt dan: 'Maar ik heb toch helemaal niks te verbergen? Van mij mogen ze alles weten, ze vinden toch niks.' Maar dat is niet helemaal waar. Er zijn tegenwoordig zoveel wetten (bijna 10.000) dat niemand ze meer allemaal kent. En dus is de kans erg groot dat je ooit wel eens de wet hebt overtreden, waarschijnlijk zelfs dagelijks. Als de overheid alles van iedereen zou weten zou je je aan alle wetten moeten houden en dat is niet te doen.

En zonder mensen die wetten overtreden is er ook geen kans op vernieuwing. Als alle wetten voor 100% worden nageleefd en je anders meteen in de gevangenis zou belanden was het homohuwelijk waarschijnlijk nu niet mogelijk in Nederland. Dan waren alle activisten opgepakt tijdens de protesten en was er nooit iets aan de wetgeving veranderd.

Daar komt bij dat de politie en geheime diensten steeds beter worden in mensen in de gaten houden. Via camera's, mobiele telefoons en drones in de toekomst hebben ze een uitgebreid netwerk waarmee ze alles zullen zien. Dan zullen ze dus ook bij iedereen wel iets vinden om ze voor te straffen, zoals hierboven beschreven overtreed iedereen de wet wel eens. In het geval de machthebbers je weg zouden willen hebben zouden ze dan dus altijd bewijs hebben om je voor te straffen, wat tegen de 'onschuld presumptie' in gaat waarin wordt gesteld dat iedereen onschuldig is tot het tegendeel is bewezen. Als je dan iedereen constant in de gaten houdt dan ga je er van uit dat iedereen schuldig kan zijn, en dat je moet bewijzen onschuldig te zijn.

Ik denk dat je om jezelf te ontwikkelen privacy nodig hebt. Als mensen geen privacy meer hebben om voor zichzelf na te denken, is dat een groot probleem. Er wordt vaak gezegd dat er een balans moet worden gevonden tussen privacy en veiligheid. Daarbij moet de laatste tijd veel privacy worden ingeleverd voor een heel klein beetje veiligheid. Het probleem is zeker niet alleen de angst voor aanslagen onder de bevolking, ook de miljardenindustrie van de beveiliging helpt met lobbyen sterk mee om nog meer privacy in te leveren.

Toekomst

Politie en overheid

In de VS is een aantal politiekorpsen die niet alleen meer misdaden probeert op te lossen, maar ze ook proberen te voorkomen. Dat doen ze door data van eerdere misdaden te combineren in algoritmes. Daar komen dan risicogebieden uit voort waar voor die dag meer kans is dat er een misdaad zal plaatsvinden. De politie stuurt er een auto op af en hoopt dan de misdaad te voorkomen door hun aanwezigheid.

Sinds 2005 is er weer een identificatieplicht, die ervoor zorgt dat je altijd een paspoort of ID-kaart moet kunnen tonen als daar om gevraagd wordt. In 1940 werd deze wet nog afgewezen omdat de overheid dan alle burgers als potentiële misdadiger zou beschouwen. Tijdens de Tweede Wereldoorlog werd de identificatieplicht ingevoerd door de Duitsers, waardoor er heel veel joden werden opgepakt. Na de oorlog werd de identificatieplicht weer afgeschaft en was het tijdenlang onbespreekbaar.

De ID-kaart en het paspoort zelf wordt ook steeds uitgebreider. Tot januari 2014 was het een tijdje verplicht je vingerafdruk af te geven. Dat is nu weer teruggedraaid, maar zou zomaar weer worden ingevoerd in de toekomst. De overheid wilde de vingerafdrukken ook centraal opslaan om te kunnen vergelijken met vingerafdrukken die gevonden worden bij misdrijven. Dat is ook niet doorgegaan. De pasfoto moet van voren genomen worden en je mag er niet op lachen, dat is om in de toekomst gezichtsherkenning mogelijk te maken. Dan zou het zo kunnen zijn dat alle pasfoto's in een database van de overheid staan en camera's toegang krijgen tot die database. Wordt er een misdadiger herkend dan kan de politie automatisch een berichtje krijgen van de locatie.

Vanaf 2017 wil de overheid al haar diensten digitaal aanbieden. Om dat veilig te kunnen doen wil de overheid dat in 2015 iedereen een eID heeft, een modernere versie van DigiD. eID bestaat uit een soort pinpas, die je dan met een apparaatje verbind met een computer. De eID kaart heeft net als een normale ID kaart alle gegevens van een persoon er op staan, samen met het adres. Dit alles staat op een chip. De kaart komt er om iets te doen tegen identiteitsdiefstal, en om drank verkoop op internet onder de 18 jaar tegen te gaan.

De kaart zal in de toekomst (in België is de kaart al ingevoerd) gebruikt moeten worden op heel veel websites. Deze sites weten dan met wie ze te maken hebben, anoniem browsen zal op die sites dan niet meer mogelijk zijn. Maar ook veel bedrijven gaan gebruik maken van deze kaart, bijvoorbeeld om toegang te krijgen tot een beveiligd gebouw of bij de sportschool.

Reizen

In Europa zijn de grenzen helemaal verdwenen, je kunt zonder controles van Nederland naar Polen. Maar dat is niet helemaal waar, want van de controles merk je wel niks meer, ze zijn er nog wel. Tegenwoordig wordt al het verkeer dat de Nederlandse grens oversteeft gefilmd en opgeslagen. Dat filmen gebeurt met ANPR (Automatische Nummer Plaat Registratie) camera's bij de snelwegen. Alle nummerborden worden gescand en opgeslagen. Deze camera's worden gebruikt om de reistijd te berekenen die je boven de snelweg op borden ziet, maar ook om mensen die nog boetes moeten betalen op te sporen. En als de overheid die data toch heeft dan willen andere takken, zoals Justitie of de Belastingdienst, er ook gebruik van maken. Als je dan met een lease-auto van de zaak wordt gezien bij de grens en twee weken later weer, dan kan de Belastingdienst concluderen dat je op vakantie bent geweest en krijg je een boete als je meer kilometers hebt gereden dan je hebt opgegeven. En mensen met een uitkering die elke werkdag op een bedrijventerrein worden gezien kunnen ook een controle van de Belastingdienst verwachten.

De ov-chipkaart zorgt ervoor dat ook iedereen in het openbaar vervoer te volgen is. Anoniem reizen kan tegenwoordig niet meer, want ook een anonieme ov-kaart is niet anoniem. Opladen doe je meestal met een pinpas en dan is de kaart toch aan je gekoppeld. En anders doen de camera's op stations en in vervoersmiddelen dat koppelen aan je kaart wel. In Rotterdam zijn er in de trams camera's opgehangen met gezichtsherkenning, iedereen wordt gescand. Mensen die een verbod om met de tram te rijden hebben of die hebben zwart gereden worden herkend en door een beveiligiger uit de tram gezet.

Sousveillance

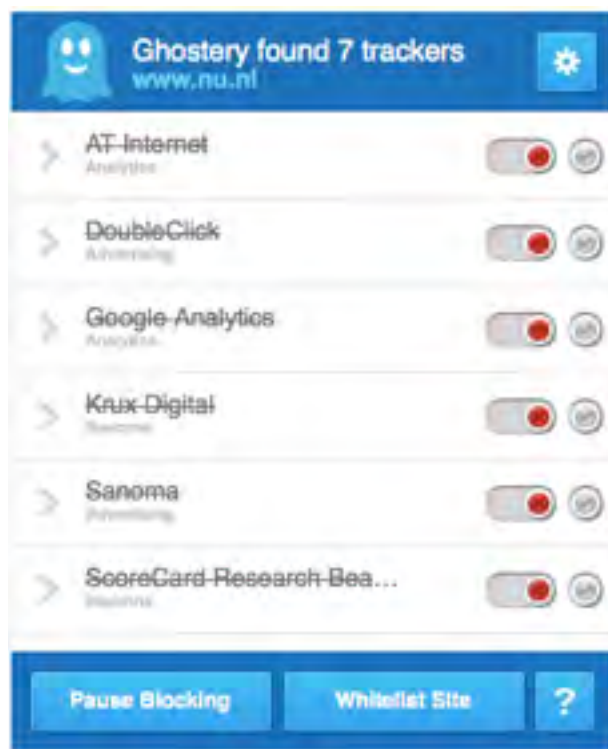


Sousveillance is een omgekeerde vorm van surveillance. Bij sousveillance houdt iemand met een (verborgen) camera bijvoorbeeld de politie in de gaten. Als een agent de wet overtreedt wordt er meteen een foto gemaakt en op Facebook verspreid, of een filmpje op YouTube. Op die manier moeten ook de machthebbers zich ook aan de wet houden.

Wat kun je zelf doen?

Er zijn veel dingen die je zelf kunt doen om je privacy beter te beschermen. In plaats van Google kun je bijvoorbeeld een privacy vriendelijke zoekmachine als DuckDuckGo gebruiken. Je kunt een 'Adblocker' installeren in je browser, zodat je geen reclames meer te zien krijgt. Ook kun je een 'Do Not Track'-plugin installeren die trackers en cookies blokkeert. Ikzelf heb er één, en in de drie maanden dat ik het gebruik heb ik al meer dan 9.000 trackers geblokkeerd. Er zijn ook andere oplossingen, zoals bijvoorbeeld een stickertje dat je op de webcam van je laptop kan plakken.

Vaak kun je ook bij de instellingen van je browser en smartphone nog meer privacy-instellingen veranderen. Bij Android bijvoorbeeld dat je locatie niet meer automatisch met apps gedeeld wordt. Bij Facebook en Google is er ook veel aan te passen bij de instellingen, je kunt er je account afschermen en de persoonlijke advertenties uitzetten. Automatisch staan deze instellingen aan dus het loont om er eens te kijken en wat dingen uit te zetten.



Ghostery, een browser add-on die tracking software blokkeert

Er zijn nog veel meer manieren om je gegevens en privacy beter te beschermen. Je kunt bij de browser instellingen cookies van derden (adverteerders) weigeren of zelfs alle cookies, maar dan wordt het vaak lastig om nog te browsen omdat veel sites cookies verplichten. Cookies worden ook gebruikt om te zorgen dat bijvoorbeeld Gmail onthoudt dat je ingelogd bent en je niet steeds je wachtwoord hoeft in te voeren.

Ook kun je beter niet teveel aanwezig zijn op social media, het is misschien leuk voor je vrienden maar voor een sollicitatiegesprek wordt tegenwoordig eerst online gekeken of je wel geschikt bent. Ook is het natuurlijk beter als bedrijven als Facebook en Google niet al te veel van je weten, want ze zullen het alleen maar gebruiken om geld aan je te verdienen. Criminelen kunnen ook op social media kijken, dus is het niet slim om berichten te plaatsen met daarin dat je op vakantie gaat of boodschappen aan het doen bent. Dan weten ze ook dat je niet thuis bent en wordt een inbraak een stuk makkelijker.

Een goed wachtwoord is ook heel belangrijk. Wachtwoorden zijn vaak te makkelijk te raden en worden op teveel plekken tegelijk gebruikt. Het meest onveilige op een computer is nooit de beveiliging of een programma maar het wachtwoord. Het meest gebruikte wachtwoord is '123456', en de rest van de top tien meest gebruikte wachtwoorden is niet veel beter. Als iemand probeert in te breken op je account zal die als eerste deze wachtwoorden proberen. Woorden kun je beter niet gebruiken, net zoals persoonlijke hobby's of dingen over jezelf zoals straatnaam, geboortjaar etc. Het is heel makkelijk om een computerscript alle woorden uit het woordenboek te laten proberen, alle mogelijke combinaties van tekens is bijna niet te doen.

Een sterk wachtwoord heeft minstens 8 karakters, is een combinatie van hoofdletters, normale letters en cijfers. Het beste zijn wachtwoorden waar niks persoonlijks in voorkomt en die totaal willekeurig zijn, en dan het liefst ook nog voor elk account een ander wachtwoord. Een sterk wachtwoord is bijvoorbeeld J*p2leO4>F. Dat is natuurlijk nooit te onthouden en daarom nemen veel mensen een te makkelijk wachtwoord en gebruiken die op teveel plekken. Er zijn programma's die willekeurige wachtwoorden aanmaken en die veilig opslaan. Je hoeft dan zelf nog maar één goed wachtwoord te onthouden en het programma vult dan automatisch het sterke wachtwoord voor je in. 1Password is bijvoorbeeld zo'n programma.

Encryptie

Door het internet kunnen geheime diensten iedereen in de gaten houden op een niveau van wat ze 30 jaar geleden alleen bij hoofdverdachten deden. Maar internet geeft ook mogelijkheden om je beter te beschermen, technieken die vroeger alleen door spionnen werden gebruikt zijn nu voor iedereen toegankelijk. Een veel gebruikte manier is encryptie. Encryptie zorgt ervoor dat je berichten kunt versturen zonder dat iemand anders kan meelezen, het is een soort slot op je bericht. Een betrouwbare manier van encryptie is PGP (pretty good privacy). Hiermee kun je mailtjes en tekstberichten versleutelen. Ook kun je met PGP bewijzen dat jij een bepaald bericht of tekst hebt geschreven. Het werkt met twee 'sleutels'. Die sleutels bestaan uit een lange reeks tekens, bijvoorbeeld uit 2048 of 4096. Een sleutel ziet er zo uit:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Comment: GPGTools - <http://gpgtools.org>

```
mQENBFMFaVUBCADQerHn1GHjx8H2me7jLoCWfrrO38TP9y9JhHPP4pBs4riCoJLy
RwUMEV3WneZPGoQ01FGmNdxzIPQWwJQ1VQfjYyH6aXXjKQxNxxHKqushQxw3tsJnK
+NB1DNI24lTOzXe4l+aHoKgthQUcsT2QjDsC4BIeyakTUj6R6S3TMxiL73v75jYx
CEHzQ9UXvvA3Q3qdjoZpslidW45VdSSMpUQNtsngBeU8/N+6qqyMTvenxx7jJSdX
b+oOjWnJcExA/xmN6FjvSKVBWT8NyBwWilbuNKBmTHSmkwb0lu0JBq9xIM7Wpz9m
FhUY+msdgGhCt279RU8/4xuXfMgzoZOYAZw9ABEBAAG0Bkphc3BlcokBPQQTAQoA
JwUCUwUBVQIbAwUJB4YfgAULCQgHAwUVCgkICwUWAgMBAAlcAQIXgAAKCRD5eh4s
9h5Q9OTnB/oDAL/tLmbXL6iMRyGghzDMUCAnnEtvz3++i0eT85TBF4szf5J5bbh
W7qIDHbki8yM8XcEQpLb8UpPwmz8SUEli9Q6d/thFgYllqcLuaomjhS43P1cC0Jo
kPU3sec32dXbBRFFb/h+IGWv6G+c24JNkJDzliv539aXj5a6SHppGHJw7Gcb31R
ulEILXgayv8RSYyJBYPy81Dr1Nc7Ch8ARi4LzyDG6faDfnCwMJ6vvEQh906aPw3L
YZL8stsG17Xakke3qwa3xmTTmj2P9tp2pzUMKkvd8Gkzk1G7OvygR00J/dbYSbcz
bTBdVIqspI9Q6ZQhi075pyqLz34NuelVuQENBFMFaVUBCACt/t864JbnBA8hVRGz
3wsT2xMtabQuQ/ObpPAzYyuD+gSN9Xk+HUDWk6KcSvB/QulBSInsI5vVAaog/5ad
4Pu+9cYq9eVufUnb6hu+RA+VxIAaMiHZFVXrTzg+JuPNAQzipg4p9aVdaQKRCRa6
ZxDz3+FPk5HtqjZZQpQIH4qVm+8Xtfu29zfGYGMvxygJhljRF3U/4ku192i5zZ8+
lkSVrAHjzEMCJmpe9j6Hj1oQHRGjPq9noOEzwPLuLUwEzzDrcS1oaoClDn2P14Wg
7rjhQm2ofS8Rr8oA2m1fmOMoAaBH1WDQRal8NhinATSSaWoFUTQubgw/QMuHK+CC
Dmz7ABEBAAGJASUEGAEEAA8FAIMFAVUCGwwFCQcGH4AACgkQ+XoeLPYcUPSPHQf/
UFR+0eueGAVDFmCrtIwOg2hR1kWrInwaHj49u/JA8buShoDJZ/hIVHilie3MoNyp
IL6Pabki6PSueukWR+FvnA5aCu43oqC6EnM/fyaSsaeh4rsWl2f+61i0zA82rPt8
HPzOwzg5K7CXC/O1teP6YwSz9Hj2GIdUICceAZWBI155iNrjUalE5gJTLiGaq58
FDKIDn71k5bvwbFZ20r6h4wrsIjPL7EZ9Nx+SsDYVt3LZJ8CVZZrJM43J6uHvXe7
qbdD+PWAImGhlzao100rgXQyLpfnv95Wx1/1orenH73wJBsVAgf/LOWMxe1vak
2Um+pQ9qr2PW4sj78EFnlg==
=/EKB
```

-----END PGP PUBLIC KEY BLOCK-----

De ene sleutel is openbaar en de andere sleutel is geheim. Met een computerprogramma, bijvoorbeeld GPGTools, kun je een bericht versleutelen met de openbare sleutel of de privé sleutel. Wil je een mail naar iemand sturen die niemand anders kan lezen dan gebruik je de openbare sleutel van de ontvanger om het bericht te versleutelen. Alleen met de privé sleutel van de ontvanger kan het bericht dan ontsleuteld worden. Het is dan dus wel belangrijk dat de andere persoon de privé sleutel goed geheim houdt. Als je wil bewijzen dat je een tekst hebt geschreven dan gebruik je jouw eigen privé sleutel. Daarmee versleutel je het bericht en met jouw openbare sleutel kan het bericht dan ontsleuteld worden. Alleen jij hebt je privé sleutel dus dan weet je zeker dat iemand iets zelf heeft geschreven. Het is wel zo dat iedereen de boodschap kan lezen, de openbare sleutel kan door iedereen gebruikt worden die hem kent.

-----BEGIN PGP MESSAGE-----

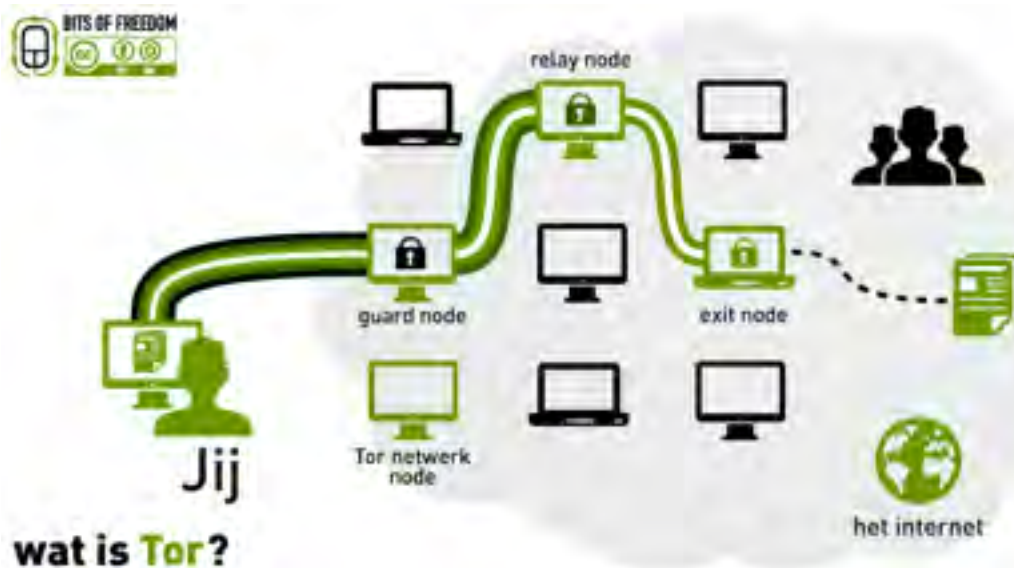
Comment: GPGTools - <http://gpgtools.org>

hQEMAwNwK1v0K94aAQgAlwcFmaSiVCAAxZi/laJwL2hvTHdc+okl4KPiNl/vJqy9
Kk9avn0aOUHJuEmn+AjGWfr2ml2Vixp8dEwO43DXTIxQvYCynW+zzLdGaNR4gPfV
6L7vsgWHIE21jGK/H6nJpsk5bylW7tmGO+EeF9e1GFesgWVDJ7jSX06YQ1X+f6lU
Ymq+8T1AHRFty611ORPadp6nHW9x9wC3YhLgh3r36pkjnoS0BucGL3QvOEcu3++c
YC/TWOTZOjTo1rTIIQyJheSc65ioLtvvWpPgh49dOu9e3lNf/XsRx95ETq3WHwso
2+6puBMVjN85kYgm3ZEcSK0A9WHVB651JOu/z9H4kNLA8gGM3xv7jmb6JgyfFy+d
uOp9iX0+xMN5MmgODOqJJWG8OUCjU6wd/OMhTGTWMZrSsh6ALyf7glgahkpu3/JU
vwgvyDdrnzQC3Y+knCTHY3TISY1MQS9IgE34j1JgR4D9CeAjCy6RuFhESxC3TBah
eo67h153dJ48CtEGQgIf09sUHodPNKyqKKKewz/KJAL2LEi1gzpfAdDNjMV7K7bJ
13PaqrxLTl/qwY2Z6ygDRc55Vvq8HWPOonCCI4zlsYLZDZ0eRXKXSza3XBkxPLkm
qA+wb6wQQ6qDUrqxmmwNIer8f/N9cHLMEZqL+UNnZwxN+logzSUuTlSz48wXibvi
D+3haEhIz5jqYPGHEg7VWN6l/5a5nJODsAdAEi6qPsq1rNtJsv7+vdCqIDH5VQ+5
P5Il5ZYoy7eDLLfhQsPCJDiQoqVZmq/Fi9fFdfUg5R6V8nQhGD0F/7VKPU+8pA1M
D7+P4GeHWC0+++Vqjcm8iAaDW353xvuqRbvSgmZXW6k8HxoMqRnADiN2/xheYrn1
OaqoiU09R2duXLRcoeLk98Dp6J/FE6OTgimcGdlhiWnkFx+y
=2n6E
-----END PGP MESSAGE-----

Hierboven staat hetzelfde als op de vorige pagina, maar dan versleuteld met een geheime sleutel. Met de bijbehorende openbare sleutel en een computerprogramma zou dit bericht ontsleuteld kunnen worden.

Tor

Als je niet gevolgd wil worden online kun je een speciale browser gebruiken. Bijvoorbeeld omdat je een huis wil kopen, of een vakantie wil boeken, zonder dat adverteerders het weten en je beïnvloeden. Of omdat je niet wil dat je data gebruikt wordt door internet giganten zoals Google die er alles aan zullen doen om er zo veel mogelijk aan te verdienen.



Google heeft bijvoorbeeld het recht om je naam, foto en alle andere data van je te gebruiken in hun advertenties zonder dat je het weet. Vrienden van je krijgen dan die reclame te zien, en zo hoopt Google ze eerder te overtuigen. Facebook doet hetzelfde.

Als je dat niet wil dan kun je gebruik maken van een browser die werkt met het Tor-netwerk. Via dat netwerk kun je anoniem browsen, het nadeel is dat browsen wel erg traag gaat. Met een normale browser maakt je computer rechtstreeks contact met de website die je wil bezoeken. Je browser stuurt je IP-adres mee zodat de website weet wie je bent en waar de data naartoe moet. Met Tor heb je niet rechtstreeks contact met een website, het Tor-netwerk stuurt de gegevens eerst door naar een computer die deel is van het netwerk en die stuurt het ook weer door. Nadat je data een aantal keer is doorgestuurd (dat maakt het zo traag) komt de data bij de website terecht, maar dan lijkt het alsof de data komt van de computer die het voor het laatst doorstuurde, en lijkt het dus ook of jij dat IP-adres hebt. Geheime diensten kunnen achterhalen wie je bent, maar dat kost ze wel veel moeite en dat zullen ze niet bij iedereen doen. Ook is het zo dat hoe meer mensen gebruik maken van het Tor-netwerk, hoe beter het werkt en hoe lastiger het is voor geheime diensten om erachter te komen wie je bent.

Conclusie

Hoe gaan Big Data privacy in de toekomst veranderen? Niemand die het zeker weet, en de ontwikkelingen gaan zo snel dat het lastig is ze bij te houden. Het zal goede gevolgen hebben, processen kunnen efficiënter worden ingericht als er meer data beschikbaar zijn. Bijvoorbeeld in het verkeer of bij het zoeken naar oplossingen voor ziektes. Het zal ook nadelige gevolgen hebben. Bijvoorbeeld dat de overheden en grote multinationals te veel macht krijgen door de gegevens die ze van iedereen hebben. Daardoor kunnen ze makkelijk mensen beïnvloeden of chanteren. Bedrijven kunnen gaan discrimineren door verliesgevende klanten te weigeren of geen korting te geven, waardoor kansarme mensen nog minder kansen krijgen.

Er is een gezegde ‘if it’s free, you’re the product’ en bij online diensten zoals Gmail of Facebook is dat ook zeker zo. Je geeft je privacy en je persoonlijke data en daar krijg je een dienst voor terug. Bij Google is het zo dat alles wat je maakt met hun diensten, bijvoorbeeld een mailtje met Gmail, eigendom is van Google. Google mag dus met jouw mails, foto’s, contacten en alle andere dingen die ze van je hebben alles doen wat ze willen.

In de toekomst zullen bedrijven kijken naar hoeveel winst de klant ze gaat opleveren in zijn/haar leven. Daar zullen ze hun prijzen op aanpassen, wat je nu al ziet met hotels en vliegtickets. Ze zullen ook kijken naar het risico dat ze hebben bij een klant. Iemand met meer kans op ziekte zal meer premie moeten gaan betalen of zelfs helemaal worden afgewezen. En een vrouw die volgens de data binnenkort zwanger gaat worden zou geweigerd kunnen worden bij een sollicitatiegesprek.

Door de overheid wordt iedereen als mogelijke dader gezien, en alle data die online over je beschikbaar is kan tegen je worden gebruikt. Zo lang je niks fout doet is er niets aan de hand, maar overtreed je een keer (per ongeluk) de wet dan heb je in de toekomst een groter probleem dan nu. Alles wordt opgeslagen, het internet vergeet nooit. Als er een heel ander regime dan nu zou komen, hebben ze veel data over iedereen.

Al die data die overheden en bedrijven hebben moet dus goed bewaakt worden. Het geeft ze veel macht en daarom moeten ze er goed mee om gaan. Of de voordelen groter zijn dan de nadelen of andersom weet ik niet, wel weet ik dat de veranderingen heel snel gaan.

Er zijn steeds meer mensen die inzien dat privacy van belang is, en ook daar zullen grote bedrijven en overheden naar moeten luisteren. Sinds 2010 is er in Nederland een politieke partij met privacybescherming als een van de hoofdstandpunten, de Piratenpartij. Door dat soort bewegingen en door klokkenluiders zoals Edward Snowden beseffen steeds meer mensen dat privacy erg belangrijk is. En mede daardoor is privacy nog niet dood.

Bronnen

Ik heb voor het eindwerkstuk vooral online dingen opgezocht, dus mijn lijst met bronnen bestaat voor het grootste deel uit websites. Dat waren nieuwsberichten en sites zoals Wikipedia, waar veel informatie te vinden is. Op het internet staat ook een hoop onzin, dus heb ik niet zomaar alles overgenomen dat ik heb gevonden online. Ik heb dit op andere sites gecontroleerd en er met gezond verstand over nagedacht. Verder heb ik ook enkele documentaires en films gekeken en ook boeken en tijdschriften gelezen, die staan uiteraard ook in de lijst.

Boeken:

De digitale schaduw, Dimitri Tokmetzis

Tijdschriften:

De Groene Amsterdammer, jaargang 138, Nr. 7, blz. 34/35/37

Documentaires/films:

‘Panopticon’ door Peter Vlemmix op YouTube

‘Big Data’ van Tegenlicht (uitzending VPRO)

‘Bureau van digitale sabotage’ van Tegenlicht (uitzending VPRO)

Websites:

Big data - Wikipedia	http://nl.wikipedia.org/wiki/Big_data
Digital me	https://www.qiy.nl/en
Wolfram Alpha Personal Analytics	http://www.wolframalpha.com/facebook/
Google Dashboard - Accountgegevens	https://www.google.com/settings/dashboard?ref=home
Geld vragen voor eigen data	http://www.nrc.nl/nieuws/2013/10/29/terugkijken-experts-zeggen-in-tegenlicht-dat-jouw-data-geld-waard-zijn/
Google dwingt fabrikanten	http://www.onemorething.nl/2013/11/de-ironische-wereldvreemdheid-van-de-google-adept/
Google dataprofielen	http://edition.cnn.com/2012/01/24/tech/web/google-privacy-policy/
Google to Sell User Profiles	http://blogs.wsj.com/digits/2013/10/11/google-to-sell-user-profiles-and-photos-in-ads/
Don't be evil	http://en.wikipedia.org/wiki/Don%27t_be_evil
Googlization	http://en.wikipedia.org/wiki/Googlization
iOS en privacy	http://www.onemorething.nl/2013/11/ios-en-privacy-tros-radar-snapt-het-niet/
Big data: van haarbal naar goudmijn	http://www.computable.nl/artikel/opinie/datamanagement/4921024/4445906/big-data-van-haarbal-naar-goudmijn.html
Big Data: Tesco	http://www.forbes.com/sites/forbesinsights/2013/11/13/big-data-tesco-probes-the-frontiers-of-privacy/
Big Data: Target	http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/
Facebook dating	http://gawker.com/5543723/facebook-knows-who-youll-hook-up-with
Facebook voorspeld	http://newsfeed.time.com/2013/10/29/facebook-knows-when-youre-going-to-get-dumped/
Google projecten	http://www.rediff.com/business/slide-show/slide-show-1-tech-googles-unbelievable-projects-that-will-change-the-world/20131014.htm#3
Debtscan	http://blog.iusmentis.com/2013/08/22/mag-debtscan-kentekens-van-willekeurige-autos-fotograferen/
Scanauto	http://www.citionsblog.nl/blog/het-alziende-oog-van-de-scanauto
Cameratoezicht politie	http://www.politie.nl/onderwerpen/cameratoezicht.html#ik-ben-gefilmd-mag-ik-de-beelden-opvragen
What Google Knows About Me	http://live.wsj.com/video/what-google-knows-about-me-and-you/7E661810-7F4C-4CCF-934C-B690543AFD36.html#!7E661810-7F4C-4CCF-934C-B690543AFD36

YouTube	https://www.youtube.com/features
Reform Government Surveillance	http://97.74.205.113/
Stop Saying 'If You're Not Paying, You're The Product' Techdirt	http://www.techdirt.com/articles/20121219/18272921446/stop-saying-if-youre-not-paying-youre-product.shtml
AT&T ontwikkelt technologie om filesharing te bestrijden	http://tweakers.net/nieuws/93212/at-en-t-ontwikkelt-technologie-om-filesharing-te-bestrijden.html
Politie gebruikte nep-webwinkels	http://tweakers.net/nieuws/93198/politie-gebruikte-nep-webwinkels-om-kopers-zwaar-vuurwerk-op-te-sporen.html
Ton deelde zijn metadata	http://www.nrc.nl/longreads/2013/12/20/ton-deelde-zijn-metadata-en-nu-weten-we-best-veel-van-hem/
Hoe je onschuldige smartphone bijna je hele leven doorgeeft aan de geheime dienst	https://decorrespondent.nl/528/hoe-je-onschuldige-smartphone-bijna-je-hele-leven-doorgeeft-aan-de-geheime-dienst/13532640-9489ce82
eID	http://www.nrc.nl/nieuws/2013/12/19/opvolger-digid-gepresenteerd-eid-moet-veiliger-zijn/
DigiD krijgt nieuwe beveiligingslaag: eID	http://www.volkskrant.nl/vk/nl/2686/Binnenland/article/detail/3423714/2013/04/11/DigiD-krijgt-nieuwe-beveiligingslaag-eID.dhtml
USA PATRIOT	http://nl.wikipedia.org/wiki/USA_PATRIOT_Act
Data mining	http://en.wikipedia.org/wiki/Data_mining
Use Big Data to Predict Your Customers' Behaviors	http://blogs.hbr.org/2012/09/use-big-data-to-predict-your-c/
Cameron's "pornofilter" blokkeert veel meer #zaplog	http://zaplog.nl/zaplog/article/camérons_pornofilter_blokkeert_veel_meer
Tesco	http://www.bbc.co.uk/news/technology-24803378
Nothing to hide argument	http://en.wikipedia.org/wiki/Nothing_to_hide_argument
If You've Got Nothing To Hide, You've Actually Got Plenty To Hide Techdirt	http://www.techdirt.com/articles/20130613/12180423457/if-youve-got-nothing-to-hide-youve-actually-got-plenty-to-hide.shtml
Why 'I Have Nothing to Hide' Is the Wrong	http://www.wired.com/opinion/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/
Russia planning 'PRISM on steroids'	http://www.theverge.com/2013/10/6/4809282/russia-planning-prism-on-steroids-for-winter-olympics
SORM	http://en.wikipedia.org/wiki/SORM
Mass surveillance	http://en.wikipedia.org/wiki/Mass_surveillance#China
panopticondefilm.nl	http://panopticondefilm.nl/
Prison Planet.com	http://www.prisonplanet.com/police-state-study-ranks-us-as-6th-worst-in-the-world.html

Democracy Going Dark: The Electronic Police State by Tom Burghardt	http://archive.lewrockwell.com/orig10/burghardt1.html
Dataretentie	http://nl.wikipedia.org/wiki/Dataretentie
Hoeveel ANPR-camera's zijn er eigenlijk?	http://sargasso.nl/hoeveel-anpr-cameras-zijn-er-eigenlijk/
Rittenregistratie en kentekenherkenning	http://www.jongbloed-fiscaaljuristen.nl/tips_&_trucs/tips_auto_van_de_zaak/rechtspraak/rittenregistratie_en_kenteken_herkenning/
2013	http://en.wikipedia.org/wiki/2013_global_surveillance_disclosures
nsa	http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
David Cameron's internet porn filter is the start of censorship creep Laurie Penny Comment is free The Guardian	http://www.theguardian.com/commentisfree/2014/jan/03/david-cameron-internet-porn-filter-censorship-creep?CMP=tw_t_gu
FBI Drops Law Enforcement as 'Primary' Mission	http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission
Zorgverzekeraars willen ex-kankerpatiënt niet verzekeren Gewoon-Nieuws.nl	http://www.gewoon-nieuws.nl/2013/12/zorgverzekeraars-willen-ex-kankerpatient-niet-verzekeren/#.UtKCCfakCF6
ternus.github.io/nsaproductgenerator/	http://ternus.github.io/nsaproductgenerator/
NSA's ANT Division Catalog	http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/
DailyTech - Tax and Spy	http://www.dailytech.com/Tax+and+Spy+How+the+NSA+Can+Hack+Any+American+Stores+Data+15+Years/article34010.htm
A guide to the arguments against NSA surveillance	http://www.reddit.com/r/restorethefourth/comments/1g9xyg/a_guide_to_the_arguments_against_nsa_surveillance/
PrivacyFirst	https://www.privacyfirst.nl/
Bits of Freedom	https://www.bof.nl/
Google - Webgeschiedenis	https://history.google.com/history/
De onbekendheid met Big Data Adformatie	http://www.adformatie.nl/blog/de-onbekendheid-met-big-data
De Electronische politiestaat Vrijspreker.nl	http://www.vrijspreker.nl/wp/2009/05/de-electronische-politiestaat/
De 'talkshowelite' van Nederland is blootgelegd en in kaart gebracht - nrc.nl	http://www.nrc.nl/nieuws/2014/01/16/de-talkshowelite-van-nederland-is-blootgelegd-en-in-kaart-gebracht/
Infographic google	http://numrush.nl/2013/09/11/infographic-deze-data-analyseert-google-om-je-op-maat-te-bedienen/
The Intercept	https://firstlook.org/theintercept
De wereld 'vecht vandaag terug' tegen de inlichtingendiensten - De af luisterpraktijken van de NSA - VK	http://www.volkskrant.nl/vk/nl/13524/De-af-luisterpraktijken-van-de-NSA/article/detail/3594929/2014/02/11/De-wereld-vecht-vandaag-terug-tegen-de-inlichtingendiensten.dhtml

Zoekresultaten uit uw Google-producten - Google Zoeken Help	https://support.google.com/websearch/answer/1710607
Spying by N.S.A. Ally Entangled U.S. Law Firm - NYTimes.com	http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?hp&_r=1&referrer=
Politie kijkt met steeds meer particuliere camera's mee	http://www.nrc.nl/nieuws/2014/02/15/politie-kijkt-met-steeds-meer-particuliere-cameras-mee/
Dit is het toezicht van de toekomst	http://www.nrc.nl/next/van/2014/februari/15/dit-is-het-toezicht-van-de-toekomst-1346119
How News Feed Works Facebook Help Centre	https://www.facebook.com/help/www/327131014036297/
What Is EdgeRank?	http://www.whatisedgerank.com/
Tegenlicht - Big Data: de Shell search	http://tegenlicht.vpro.nl/afleveringen/2013-2014/big-data-de-shell-search.html
Oekraïne volgt betogers via mobiel signaal	http://www.nu.nl/tech/3681069/oekraïne-volgt-betogers-via-mobiel-signaal.html
Whatsapp	http://waag.org/sites/waag/files/public/Publicaties/vprogids201243_whatsapp.pdf
Geef je maar over aan Big Data, verzet is zinloos	http://www.trouw.nl/tr/nl/6700/Wetenschap/article/detail/3605794/2014/03/02/Geef-je-maar-over-aan-Big-Data-verzet-is-zinloos.dhtml
Tegenlicht - Anoniem het web op	http://tegenlicht.vpro.nl/nieuws/2014/maart/veilig-online-gids4.html
De toekomst is nu Piratenpartij	http://www.piratenpartij.nl/blog/thijsmarkus/de-toekomst-nu
Consumentenbond: plannen ING in strijd met privacywetgeving - nrc.nl	http://www.nrc.nl/nieuws/2014/03/10/consumentenbond-plannen-ing-in-strijd-met-privacywetgeving/
Facebook Turns 10: The Mark Zuckerberg Interview	http://mobile.businessweek.com/articles/2014-01-30/facebook-turns-10-the-mark-zuckerberg-interview
'CIA bespioneerde computernetwerk Amerikaans Congres'	http://www.nrc.nl/nieuws/2014/03/11/cia-bespioneerde-computernetwerk-amerikaans-congres/
Wat is de prijs die ING betaalt voor het delen van jouw betaalgegevens? - nrc.nl	http://www.nrc.nl/nieuws/2014/03/11/wat-is-de-prijs-die-ing-betaalt-voor-het-delen-van-betalgegevens/
Tegenlicht: Bureau voor digitale sabotage	http://www.uitzendinggemist.nl/afleveringen/1401232
internet verspreid snel dingen	http://www.nrc.nl/nieuws/2014/03/12/erdogan-demonstraties-niet-democratisch-waterkanonnen-ingezet-in-istanbul/
big data vliegtuigen	http://www.nrc.nl/nieuws/2014/03/24/kijken-vliegbewegingen-boven-nederland-voor-en-tijdens-de-nucleaire-top/
Mag Google de mails lezen van Nederlandse wetenschappers? - Economie - VK	http://www.volkskrant.nl/vk/nl/2680/Economie/article/detail/3624016/2014/03/28/Mag-Google-de-mails-lezen-van-Nederlandse-wetenschappers.dhtml

ING haalt 'Big Data' kastanjes uit het vuur voor de andere banken - Emerce	http://www.emerce.nl/ opinie/ing-haalt-big-data-kastanjes-uit-vuur-andere-banken
Drie vragen over Big Data, privacy en de ING « Bits of Freedom	https://www.bof.nl/2014/03/10/drie-vragen-over-big-data-privacy-en-de-ing/
Notificatieplicht: driedubbelplus winst	https://www.bof.nl/2014/04/03/notificatieplicht-driedubbelplus-winst/
www.piratenpartij.nl/blog/interminded/cameraplan-opstelden-gevaar-voor-nederlanders-en-nederland	http://www.piratenpartij.nl/blog/interminded/cameraplan-opstelden-gevaar-voor-nederlanders-%C3%A9n-nederland
economische spionage	http://www.huffingtonpost.com/nikolas-kozloff/nsa-spying-on-petrobras-f_b_3965148.html
ID-scanners in supermarkten Piratenpartij	http://www.piratenpartij.nl/blog/erwt/id-scanners-supermarkten
Is Albert Heijn de nieuwe Big Brother?	http://www.frankwatching.com/archive/2012/01/03/is-albert-heijn-de-nieuwe-big-brother/
Alle informatie over slimme meters voor elektriciteit en gas	http://www.slimmemeters.nl/
Hoe data gelijkwaardigheid, solidariteit en rechtszekerheid kunnen ondermijnen	https://decorrespondent.nl/830/hoe-data-gelijkwaardigheid-solidariteit-en-rechtszekerheid-kunnen-ondermijnen/40418510-3743911c
Experian Nederland zakelijke gegevens, analyses en marketing diensten www.experian.nl	http://www.experian.nl/
Privacypamflet	http://shawnbuckles.nl/privacypamflet/
Big Business is watching you	https://decorrespondent.nl/66/big-business-is-watching-you/3214002-df572412
bluekay	http://www.abine.com/blog/2012/bluekai/
Tegenlicht 2	http://tegenlicht.vpro.nl/afleveringen/2013-2014/bureau-voor-digitale-sabotage.html
Mini-docu: Met één druk op de knop virtueel iemand anders zijn	https://decorrespondent.nl/764/mini-docu-met-n-druk-op-de-knop-virtueel-iemand-anders-zijn/43078904-b548e74c
Zo word je minder makkelijk vindbaar in de digitale wereld	https://decorrespondent.nl/854/zo-word-je-minder-makkelijk-vindbaar-in-de-digitale-wereld/43776040-9afdd3f
PGP	http://nl.wikipedia.org/wiki/Pretty_Good_Privacy
NSA datacenter	http://www.wired.com/2012/03/ff_nsadatacenter/
† Democratie (300 v. Chr. - 2013)	https://decorrespondent.nl/349/-democratie-300-v-chr-2013/9839357-3f450e2b
Gezichtherkenning pasfoto	http://nl.wikipedia.org/wiki/Biometrische_gezichtsherkenning
DDR	http://www.vrijspreker.nl/wp/2013/03/nl-passeert-de-ddr-in-het-wantrouwen-tegenover-haar-eigen-burgers-anpr/
Whatsapp versleuteld	http://www.privacynieuws.nl/images/001-Yatta/Docs/Nu_ook_WhatsApp_is_versleuteld_is.pdf
'In de Tweede Wereldoorlog hadden we wél wat te verbergen'	https://decorrespondent.nl/1138/in-de-tweede-wereldoorlog-hadden-we-wl-wat-te-verbergen/98053418892-55165f01

Hoe wapenen we ons tegen de machine die nooit vergeet?	https://decorrespondent.nl/586/hoe-wapenen-we-ons-tegen-de-machine-die-nooit-vergeet/15019180-90ec42d7
Meet The Woman Who Did Everything In Her Power To Hide Her Pregnancy From Big Data ThinkProgress	http://thinkprogress.org/culture/2014/04/29/3432050/can-you-hide-from-big-data/
Hoe Spotify leerde naar big data te luisteren - NRC Q	http://www.nrcq.nl/2014/05/26/waarom-big-data-onverbiddelijk-de-waarheid-vertelt
Google Flu Trends Netherlands	http://www.google.org/flutrends/nl/#NL
big data - zoeken - nrc.nl	http://zoeken.nrc.nl/?q=big+data&sort=date
Deze negen bedrijven weten nog meer van je dan Facebook en Google Motherboard	http://motherboard.vice.com/nl/read/deze-negen-bedrijven-weten-nog-meer-van-je-dan-facebook-en-google
Nee, je hebt wél iets te verbergen	https://decorrespondent.nl/209/nec-je-hebt-wl-iets-te-verbergen/6428004-ab2d5fc2
My Experiment Opting Out of Big Data Made Me Look Like a Criminal TIME	http://time.com/83200/privacy-internet-big-data-opt-out/
Tegenlicht - Anoniem op het web	http://tegenlicht.vpro.nl/nieuws/2014/maart/veilig-online-gids.html
The Power and the Pitfalls of Big Data on Vimeo	http://vimeo.com/51769055
Information Fiduciary: Solution to Facebook digital gerrymandering New Republic	http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering
DELETE YOUR FACEBOOK - YouTube	https://www.youtube.com/watch?v=EfnKmPQdapw
De les na één jaar Snowden: de misstanden van de NSA zijn stelselmatig overdreven	https://decorrespondent.nl/1298/de-les-na-n-jaar-snowden-de-misstanden-van-de-nsa-zijn-stelselmatig-overdreven/44003239698-59db81b4
Docu: 'Terms and Conditions May Apply' - Mediaredactie	http://www.mediaredactie.net/2013/10/11/docu-internetgebruiker-ben-500-dollar-waard/
Predict Crime Predictive Policing Software PredPol	http://www.predpol.com/
Privacy - Wikipedia	http://nl.wikipedia.org/wiki/Privacy#Privacy_versus_veiligheid