Internetvrijheid: online privacy

Steven Raaijmakers

May 20, 2016

1 Inleiding

In onze Westerse samenleving is het internet niet meer weg te denken. De toegankelijkheid van het internet stijgt, en lijkt zelfs een ware levensbehoefte te worden. Facebook-baas Mark Zuckerberg ziet toegang tot het internet zelfs als de oplossing voor armoede in derdewereldlanden [4]. Niet geheel onterecht, want toegang tot het internet betekent immers toegang tot een onuitputbare bron van informatie.

Omdat het internet gemeengoed is en net-neutraliteit kent, heeft het internet geen eigenaar. Uit recente ontwikkelingen blijkt echter de behoefte aan een vorm van autoriteit op het internet. De huidige wetteloze cultuur van het internet resulteert namelijk in schendingen van rechten van onze democratie.

Privacy is het voornaamste slachtoffer van de digitalisering van onze cultuur. Dit gaat enerzijds vrijwillig middels de groeiende behoefte om de wereld op te hoogte te stellen van jouw persoonlijke leven. Het is tegenwoordig sociaal geaccepteerd om dagelijks een portretfoto te delen met de wereld of op de hoogte te brengen van je laatste maaltijd. Door deze narcistische trend leveren we vrijwillig een stuk privacy in. Op onvrijwillige manier worden we op basis van vrijwillig gedeelde informatie in de gaten gehouden door commerciële bedrijven en onze eigen overheid. Op basis van jouw persoonlijke informatie kunnen zij namelijk voorspellingen doen over toekomstige keuzes en deze proberen te beïnvloeden.

Men lijkt zich steeds bewuster te worden van de onvrijwillige manier waarop we onze leven delen met derden. Dankzij onthullingen van Edward Snowden werden de privacy schendingen van overheden bekend bij het grote publiek. Eind juli 2013 [9] lekte de oud-medewerker van de Amerikaanse inlichtingendienst NSA geheime documenten waarin de omvang van spionageactiviteiten op het internet van onder andere de NSA aan het licht kwamen. Maar niet alleen de overheden maken zich schuldig aan spionageachtige praktijken, ook bedrijven zoals Facebook doen dit.

In de huidige samenstelling is er onderscheid te maken tussen twee partijen die zich schuldig maken aan inbreuk op onze privacy. Commerciële bedrijven, vaak sociale media bedrijven, en overheden. Beide kennen hun eigen redenen en bewerkstelligen dit op verschillende manieren. Maar hoewel men zich steeds

bewuster wordt van de privacy schendingen lijkt men de ernst hiervan vaak nog niet te begrijpen.

2 Praktijken

Al vrij kort na de oprichting van het internet werden er gedragsregels opgesteld. Deze werden de netiquette genoemd [11]. De meeste van deze regels gingen over het technische aspect van het netwerk, zodat deze op de juiste manier gebruikt werd. Enkele netiquete bevatten ook gedragsregels voor internetcommunicatie tussen mensen onderling. Een van die regels luidde:

> "Houd online dezelfde gedragsstandaard aan als in het gewone leven."

Uit deze regel blijkt dat internet al vroeg als een samenleving werd gezien. Zoals in elke samenleving moeten er regels zijn om deze in goede banen te lijden, maar doordat het internet relatief jong is zijn de meeste wetten uit onze rechtstaat nog niet aangepast op deze digitale cultuur. Hierdoor vallen de praktijken van bedrijven en overheden vaak binnen het kader van de wet. De laatste tijd is er een verandering te zien. Omdat belangenorganisaties rechtszaken [6] aanspannen tegen bedrijven en de overheden krijgen deze steeds minder vrij spel.

2.1 Overheden

Overheden zijn in eerste instantie overactief begonnen met data verzamelen na de trend die ontstond na 11 september, met als doel om terroristen op te sporen [3]. Tegenwoordig verzamelt de overheid echter ook data voor lichtere criminele vergrijpen [8], voor bijvoorbeeld het opsporen van frauduleuze activiteiten. Het grote verschil in het verzamelen van data van de overheid zit in het feit dat de overheid - in tegenstelling tot commerciële bedrijven – ook bevoegd is data op te vragen van particuliere bedrijven.

Big Data

Het ministerie van justitie heeft afgelopen jaren onderzoek gedaan naar het opsporen van criminaliteit middels Big Data analyse [8]. Hier hadden ze de mogelijkheid om patronen te herkennen die bijvoorbeeld zouden kunnen duiden op witwaspraktijken. Big Data is echter alleen bruikbaar bij het analyseren van veel-voorkomende criminaliteit. Voor Big Data is namelijk enorm veel inputdata nodig om kansen te koppelen aan een bepaald handelen. Hierdoor is Big Data analyse minder geschikt voor ernstige criminaliteit zoals terrorisme. De Wetenschappelijke Raad voor Regeringsbeleid zegt hierover: "[...] Bovendien is elke terroristische aanslag uniek waardoor het lastig, zo niet onmogelijk is daar een patroon op te baseren" [2]

Sleepnet

Afgelopen juli presenteerde de minister van binnenlandse zaken Ronald Plasterk [5] aanpassingen op de "Wet op de inlichtingen- en veiligheidsdiensten". In het nieuwe wetsvoorstel staat onder andere dat de Nederlandse inlichtingendienst AIVD de mogelijkheid zou moeten hebben om al het communicatieverkeer van de Nederlandse burgers te controleren. In de toekomst is het zodoende ook legaal voor de AIVD om naast het aftappen van telefoongesprekken whatsapp-berichten te onderscheppen, ook van onschuldige burgers. Er wordt door tegenstanders daarom gesproken over een sleepnet waarin onschuldige burgers terecht komen, van henhun wordt namelijk evenveel data bewaard als van verdachten.

2.2 Commerciële bedrijven

Commerciële bedrijven hebben als doel hun winst te maximaliseren. Hoewel de geleverde internet diensten vaak gratis zijn wordt je wel gevraagd om relatief veel persoonlijke informatie achter te laten. Deze persoonlijke informatie is de bedrijven zeer waardevol, omdat ze op basis van jouw persoonlijke informatie je toekomstige keuzes proberen te voorspellen en te beïnvloeden. Het beïnvloeden van deze keuzes gebeurd vaak in de vorm van advertenties. Gericht adverteren is namelijk veel effectiever. Een verkoper van te dure cafeïne-cola zal het financieel veel aantrekkelijker vinden om zijn advertenties te tonen aan hippe twintigers uit de grote stad dan aan Jan met de pet.

Op het internet betaald je als het ware met persoonlijke informatie. Een bekende uitspraak over sociale media luidt dan ook:

> "Als je niet betaalt, ben je geen klant. Dan ben je het product."

Safe Harbor

Inmiddles zijn er al enkele wetten om de informatie verzamel drang van bedrijven enigszins aan banden te leggen. In het Safe Harbor-verdrag (bron) van de Europese Unie staat dat een bedrijf jouw gegevens niet mag doorspelen aan andere zonder jouw expliciete toestemming. Bedrijven hebben echter simpele trucs om dit soort wetten te omzeilen. Een veel gebruikte manier om dit te doen is het hashen van gegevens. Hierbij worden je gegevens naar onleesbare tekst omgezet om vervolgens doorverkocht te worden. De bedrijven die deze gehashte gegevens inkopen hebben op hun beurt een manier om het gehashede bericht weer leesbaar terug te hashen naar leesbare tekst mét jouw gegevens, zonder jouw expliciete toestemming.

3 Privacy

Voor het Snowden tijdperk was het prioriteit om het grote publiek te laten zien wat er met onze privacy gebeurd. Nu dat eenmaal duidelijk is lijkt men er de ernst niet van in te zien.

Dit valt te verklaren op meerdere manieren. Enerzijds zien we de groeiende behoefte om persoonlijke informatie te delen met de buitenwereld, waardoor we bewust een stuk privacy inleveren. Ook denkt men vaak voordeel te halen uit het opgeven van een stuk privacy. Bij sociale media mag je "gratis" gebruik maken van hun dienst, dus het achterlaten van wat persoonlijke informatie zou niet meer dan eerlijk zijn. Wanneer je een bonuskaart neemt bij Albert Heijn, registreren ze al jouw boodschappen, maar hiervoor belonen ze jou met korting. Anderzijds zijn we bereid een stuk privacy op te geven als er zo ernstige criminaliteit mee kan worden opgespoord. De vraag is hoe effectief dit eigenlijk is.

3.1 Belang van privacy

Kennis is macht, en hoe meer kennis men heeft over jou hoe meer macht ze hebben. Dit is een kwalijke zaak omdat ze hierdoor grote invloed kunnen uitoefenen op bepaalde keuzes die je gaat maken in je leven. Het verzamelen van data staat hierin gelijk aan kennis over specifieke personen, of groepen. Door het verleden te bekijken kan een voorspelling gedaan worden over de toekomst. Wanneer er bekend is dat iemand al jaren lang op een bepaalde politieke partij stemt, kan geprobeerd worden deze keuze te beïnvloeden door het laten zien van bepaalde advertenties.

Privacy is ook belangrijk bij sociale interacties. Een reputatie van iemand beïnvloed namelijk de kansen die deze persoon krijgt. Als je van te voren al beschikking hebt tot bepaalde persoonlijke informatie van een ander zal je deze persoon bewust dan wel onbewust anders benaderen. Dit kan zijn tijdens een praatje op een borrel maar ook bij een sollicitatiegesprek.

Daarnaast hebben mensen van nature behoefte aan persoonlijke ruimte, de een meer dan de andere. Wanneer iemand vrij is van een omgeving waarin hij in de gaten wordt gehouden zal hij zich meer op zijn gemak voelen.

Daarnaast is privacy belangrijk voor de vrijheid waarin we leven. Je maakt namelijk andere keuzes als je weet dat mensen op je letten. Dit is bijvoorbeeld waarom het stemmen in een stemhokje gebeurd. Wanneer er constant op je gelet wordt heb je de neiging binnen de gevestigde paden te blijven. Daarom is privacy ook belangrijk voor je eigen ontwikkeling. In het leven maak je keuzes waarbij je aan sturing van naasten al voldoende hebt, daar hoeft de overheid of Twitter zich niet mee te bemoeien.

Het is niet slecht om persoonlijke gegevens te delen met andere, maar privacy geeft je de mogelijkheid zelf te bepalen wanneer je dit deelt met andere, in plaats van dat je die keuze bij een derde partij zoals Twitter legt.

3.2 Eenmaal bewust

Gelukkig is men zich steeds vaker bewust het feit dat hun privacy geschonden wordt. Het lijkt echter alsof men dit meer accepteert wanneer een bedrijf dit doet dan wanneer onze eigen overheid dit doet. Dit is vreemd omdat de overheid als hoofdtaak heeft haar eigen burgers te beschermen. Het handelen van de overheid

ontstaat meestal uit vraag van de burger. Na de aanslagen in Brussel was er een roep om nog strengere (internet)-controles [1] en die zullen er ongetwijfeld komen.

Daarnaast wordt de overheid - in tegenstelling tot commerciële bedrijven - gecontroleerd op het correct omgaan met de gegevens die zijn verzamelen conform de "Wet Bescherming Persoonsgegevens". Uiteraard dienen ook commerciële organisaties zich aan dezelfde wet te houden maar hierop worden ze niet gecontroleerd.

Een ander aspect is vaak dat het bijkomende commerciële voordeel zwaarder weegt dan het recht op privacy. De bonuskaart van de Albert Heijn registreert boodschappen om hier vervolgens met Big Data analyse uitspraken over te doen en zo de winst te vergroten, als tegenprestatie krijgt de klant korting op bepaalde producten.

Aan de hand van data kunnen we dus beïnvloed worden in toekomstige keuzes. Op kleine schaal lijkt er niet veel aan de hand, maar wanneer grote groepen beïnvloed worden op keuzes kan er een ontwrichting optreden. Denk bijvoorbeeld aan het verzekeringswezen dat zijn premies aanpast op data van grote groepen en zo de kans verkleint op het uitkeren van verzekering, of aan banken die nog nauwkeurige hypotheken kunnen verstrekken.

Mensen voeren ook vaak als argument aan dat ze niets te verbergen hebben en dat derden met hun gegevens aan de haal mogen, als hiertegenover veiligheid of een andere beloning staat. Een bekend citaat van Edward Snowden hierover luidt:

> "Zeggen dat je het recht op privacy niet belangrijk vindt omdat jij niets te verbergen hebt, is niet anders dan zeggen dat je vrije meningsuiting niet belangrijk vindt, omdat je niets te zeggen hebt"

4 Partijen

Aan de ene kant staan de partijen die onze privacy schenden: overheden en bedrijven. Gelukkig zijn er steeds vaker mensen die kritisch zijn op hun manier van handelen, en die dit aan het grote publiek proberen duidelijk te maken.

Evgeny Morozov

Evgeny Morozov is een internet-scepticus en auteur van *The Net Delusion: The Dark Side of Internet Freedom*. In een VPRO Tegenlicht documentaire [12] betoogd hij waarom het internet in zijn huidige vorm een bedreiging is voor onze democratie. Het aanscherpen van de wetten ziet hij als onderdeel van de oplossing maar veel belangrijker zou een omslag van denken bij de grote menigte. Hij noemt de internetgebruikers van de huidige maatschappij de "gegoede klasse". Een klasse waarin men op de hoogte is van de spionageactiviteiten en de samenhangende privacyschendingen maar dit gedoogd. Ze hebben immers "niets te verbergen" en maken dankbaar gebruiken van internetdiensten.

Daarnaast geloofd hij in de oprechtheid van de overheden. Volgens hem denken ze oprecht haar burgers van dienst te zijn, maar zijn hierin veel te ver doorgeslagen. Morozov illustreert aan de hand van de situatie in Jemen waarom hij dit vindt. In Jemen zijn de Amerikaanse inlichtingendiensten actief op zoek naar data, waaruit zij conclusies kunnen trekken die de Amerikaanse veiligheid bevorderen. Ze kunnen risicoprofielen van Jemenieten die aanslagen zouden willen plegen op Amerika. Ze negeren hierbij echter de oorzaak; het waarom. Want waarom zou iemand een aanslag willen plegen op Amerika? De oorzaak kan mogelijk liggen bij het verlies van familie of vrienden door Amerikaanse *drone*-aanvallen.

Douglas Rushkoff

Douglas Rushkoff is een Amerikaanse mediatheorist. In een documentaire [13] verteld hij waarom het probleem niet bij de overheden ligt maar bij de commerciële bedrijven. Hij kan zich vinden in het feit dat internetbedrijven zoveel mogelijk winst willen halen maar vindt de huidige methodes verkeerd. Ter illustratie spreekt hij van *occupy*. Deze groep demonstranten werd door de media als simpele mensen weggezet omdat ze geen einddoel hadden. Ze protesteerden juist omdat ze de methodes om een doel te bereiken onjuist vonden. De demonstratie tegen de methodes vond hij juist goed. Het doel van een bedrijf om winst te halen is juist, maar de manier waarop - het massaal verzamelen van onze gegevens - vindt hij onjuist.

Overheid

Minister Plasterk noemt de door hem gepresenteerde wet noodzakelijk [7] en speelt in op recente gebeurtenissen. Het internetverkeer aftappen tussen Nederland en Syrië zou volgens hem de veiligheid kunnen bevorderen (bron). Uit vertrouwelijke documenten die de NOS in handen kreeg (april 2016) wordt duidelijk dat Plasterk het ook iets dichter bij huis wil zoeken. Hierin vraagt hij aan Nederlandse providers om berichten af te tappen van bepaalde chat diensten, of het gehele communicatieverkeer tussen bepaalde steden.

De wet is momenteel in behandeling bij de Raad van State. Kees Verhoeven (D66) vraagt zich af hoe noodzakelijk deze wet is. Hij stelt: "Bij aanslagen zie je vaak dat de daders al in het vizier waren. Niet de grootte van de hooiberg is het probleem, maar het omgaan met die gigantische berg aan data." [10]

5 Conclusie

Onze privacy wordt geschonden door overheden en bedrijven, met beiden hun eigen redenen. Commerciële bedrijven proberen aan de hand van onze gegevens onze toekomst te voorspellen en bepalen, meestal door het tonen van gerichte advertenties. Overheden daarentegen proberen de samenleving zo veilig mogelijk te maken, maar zijn hier enigszins in doorgeslagen. Eerst speurden ze vooral

naar terrorisme op het internet, nu ook naar kleinere criminelen vergrijpen als fraude.

De burger wist eerst niet van deze praktijken af, maar dankzij de onthullingen van Snowden is dit bekend bij het grote publiek. Men beseft alleen niet de ernst van de privacyschendingen die plaats vinden, vaak omdat ze er een beloning voor terugkrijgen in de vorm van toegang tot een bepaald netwerk of korting op de dagelijkse boodschappen. Wanneer deze beloning uitblijft zijn mensen kritischer betreft het weggeven van hun data, zoals bij de overheden. De overheden beloven ons echter met iets groters te belonen dan een korting: veiligheid.

Zoals Morozov al zei, de doelen van beide partijen zijn juist. Het is terecht dat bedrijven winst willen maken, en het is goed dat de overheid onze veiligheid wil garanderen. De huidige methodes in de vorm van online zoveel mogelijk data over mensen te verzamelen is alleen niet de juiste. Voor coommerciële bedrijven is dit omdat ze hierdoor te veel macht krijgen en daardoor keuzes kunnen beïnvoeden van grote groepen. Het verzamelen van data door overheden blijkt minder effectief dan we hoopten. Daadwerkelijk terrorisme stoppen met het controleren van internetverkeer blijkt nog niet erg succesvol. Kleinere criminaliteit, zoals fraude is makkelijker te herkennen via de data. De vraag is alleen hoeveel men zijn eigen privacy waard vindt. Zijn we bereid onze privacy in te leveren voor een misdaadloze samenleving waarin we 15% korting krijgen op de bonus aanbieding van deze week?

References

[1] bnr.nl/Marjan van den Berg. *Meer anti-terreurmaatregelen in België*. 2016. URL: `http://www.bnr.nl/nieuws/buitenland/aanslagenbrussel/651044-1603/gratis-meer-anti-terreurmaatregelen-in-belgi`.

[2] A.W.A. Boot et al. "Big Data in een vrije en veilige samenleving". In: *WRR* (2016).

[3] M Goede et al. "Data-analyse en Precriminele Veiligheid in de Strijd tegen Terrorisme". In: *Krisis* 2011.3 (2011), pp. 59–65.

[4] internet.org. *Our Mission*. 2016. URL: `https://info.internet.org/en/mission/`.

[5] De Minister van Veiligheid en Justitie et al. "Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..)" In: (2015).

[6] NU.nl/Jeroen Kraan. *Uitspraak bewaarplicht raakt ook inlichtingendiensten*. 2014. URL: `http://www.nu.nl/politiek/3746791/uitspraak-bewaarplicht-raakt-inlichtingendiensten.html`.

[7] Daphne van der Kroft. "PERSBERICHT: PLASTERK MAAKT NIEUW SLEEPNET VOOR GEHEIME DIENSTEN BEKEND". In: *Bits of Freedom* (July 2, 2015).

[8] fd.nl/Heiko Jessayan en Rob de Lange. *Big data legt onzichtbare criminaliteit bloot*. 2016. URL: http://fd.nl/economie-politiek/1150701/big-data-legt-onzichtbare-criminaliteit-bloot.

[9] David Lyon. "Surveillance, snowden, and big data: capacities, consequences, critique". In: *Big Data & Society* (2014).

[10] Joost Schellevis. *Plasterk denkt na over aftappen chat-apps en wifi-hotspots*. 2016. URL: http://nos.nl/artikel/2100411-plasterk-denkt-na-over-aftappen-chat-apps-en-wifi-hotspots.html.

[11] Virginia Shea and Cirginia Shea. *Netiquette*. Albion Books, 1994.

[12] VPRO Tegenlicht. *Bureau voor digitale sabotage*. 2014.

[13] VPRO Tegenlicht. *De herovering van het nu*. 2014.