O ja, Privacy!

Rein de Jong

Iedereen praat erover, weinigen die het wat kan schelen. Lezers willen graag weten wat je eraan kunt doen. Helaas heb ik geen toverspreuk die jouw privacy kan waarborgen. Alles heeft te maken met je eigen gedrag; wat doe je online, welke apps gebruik je, welke nieuwssites en fora bezoek je. Ik hoop wat handvatten te kunnen bieden die voorkomen dat je in een bubble wordt gezogen. In de echte wereld worden we geholpen door Covid-19, want door gewoon een mondkapje te dragen ben je al een stuk moeilijker te herkennen door de camera's die her en der hangen.

Veel mensen geven aan dat ze niets te verbergen hebben en dat ze daardoor nergens acht op hoeven te slaan. Ik vermoed dat men bedoelt, weinig te verbergen te hebben voor mensen die ze vertrouwen. Het is echter een ernstige misvatting om zo te denken over organisaties.
In mijn lezingen over veiligheid maak ik graag mensen bewust door vragen te stellen zoals:

- Wat is je inkomen, je pensioenplan?
- Wat is je bezit/spaarrekening/hypotheek/schulden?
- Welke seksuele geaardheid heb je?
  Welke online seks kijk je?
- Namen van je kinderen, leeftijd en waar ze naar school gaan?
- Hoe vaak heb je seks in de week? Waar denk je aan tijdens de seks?

Dat lijken nog relatief onschuldige vragen. Weinigen zijn bereid daar antwoord op te geven. Ga er maar van uit dat Google, Facebook, Amazon en Apple de antwoorden op de eerste drie vragen in grote lijnen al lang hebben. Het antwoord op de laatste vraag kan door kunstmatige intelligentie (AI) wel worden ingevuld. Het zou best zo kunnen zijn dat je nú niet bang hoeft te zijn, maar dat de gegevens die je nu achteloos vrijgeeft je later in grote problemen kunnen brengen. Wat nu is toegestaan, is straks misschien verboden. Kijk bijvoorbeeld naar het misbruiken van het bevolkingsregister door de nazi's.

Privacy is het recht jezelf te kunnen zijn zonder bang te hoeven zijn voor de reacties van anderen.

Er waart een grappig filmpje op internet rond waarin iemand bij woningen aanbelt en vraagt of er foto's van de bewoners gemaakt mogen worden. Daar wordt boos op gereageerd en zelfs met politie gedreigd. Een dag later belt dezelfde persoon weer aan en toont hen foto's van henzelf. Je kunt je de verontwaardiging voorstellen. Mensen zijn nog kwader en uiten bedreigingen. Op de vraag hoe en wanneer de foto's zijn gemaakt, is het antwoord: 'Door jezelf en openbaar geplaatst op Facebook c s.'

De afgelopen tijd zijn er veel artikelen en documentaires verschenen die de ernst van de omgang met privacy, of juist het gebrek daaraan, behandelen. Twee daarvan wil ik speciaal onder de aandacht brengen:

1. **/The Social Dilemma**[1]
   Een ietwat zeurderige documentaire, maar die legt wel goed uit hoe het verdienmodel in elkaar steekt en maakt je bewust van de gevaren van Social Media. Te zien op Netflix.
2. **Volkskrant - complotdenken**[2]
   Een artikel waarin wordt uitgelegd hoe complotdenken ontstaat en de wijze waarop je de discussie op gang kunt houden zonder te oordelen en daardoor de complotdenker verder in zijn rol te duwen.

Er zijn voorspellende programma's, *algoritmen*[3] genaamd, die je berichten en advertenties voorschotelen op basis van je kijkgedrag en al het andere wat je deelt. Deze algoritmen zijn stukjes software die aan de hand van jouw gedrag en de profielen van anderen in een App of op het internet een profiel van jou samenstellen en trachten te voorspellen wat jouw interesses zijn en daarop aanbevelingen doen voor vervolgcontent.
Dat wordt nog eens versterkt wanneer je je privacy veronachtzaamt; hierdoor wordt jouw beeld, en als afgeleide daarvan, jouw mening beïnvloed. Tegelijkertijd worden er advertenties getoond die bij je passen en je beïnvloeden.

Er is maar één doel: geld verdienen!

Het doel van Social Media is advertenties verkopen. Hun gebruikers laten klikken op de advertentie laat de kassa rinkelen. En de ene advertentie levert nu net een paar cent meer op dan de andere, en hoe meer je klikt, des te meer wordt er verdiend. Daarom wordt getracht je aandacht vast te houden door je net een iets uitbundiger of extremer filmpje of plaatje te tonen. Want het doel van de makers van Social Media is het verkopen van advertenties en het verzamelen van je gegevens, met als doel: geld verdienen!

Naast de advertentieverkoop wordt verdiend aan het verzamelen van gegevens over jou en je familie en vrienden, en het doorverkopen daarvan. Die informatie wordt vaak aangevuld met sociale en demografische gegevens die over jou bekend zijn. Er zijn veel officiële openbare bronnen[4], zoals het Kadaster, KvK, CBS, en nog veel meer waaruit geput kan worden. De gegevens worden door gespecialiseerde bedrijven bijeengebracht, denk hierbij bijvoorbeeld aan Cambridge Analytica. Bij dat soort bedrijven wordt vaak 1+1='ongeveer 2' gedaan en dan worden de gecombineerde en geëxtrapoleerde gegevens verkocht aan commerciële partijen. Het doel is dan een profiel van de (potentiële) klant op te kunnen stellen, en dan daarop beslissingen te kunnen nemen of actief aan klant-

benadering te doen. Daardoor kan jou opeens zonder opgaaf van redenen een verzekering of andere dienst worden geweigerd. Maar ook de Social Media zelf maken weer gebruik van die samengestelde gegevens om jou nog beter te leren kennen.

Bij de pogingen om jouw aandacht vast te houden wordt er steeds een stapje verder gezet in het aanbieden van berichten en 'nieuws'. Daardoor wordt de bel/bubbel waarin je verkeert steeds minder divers, totdat je overblijft met een clubje gelijkgestemden. Daardoor wordt kritiek op je eigen mening en inzichten van anderen uitgewist. En laat kritiek nou net dat gratis advies zijn waardoor je geest wordt gescherpt, je argumenten worden geëvalueerd en een aanzet vormen voor zelfreflectie.
Het uitwissen van kritiek en het comfortabel aanschuren en knuffelen met gelijkgestemden is een van de redenen waarom er steeds meer complottheorieën de kop op steken, met een steeds grotere en fanatiekere aanhang.
De bel waar je in verkeert doet denken aan de verzuiling (groepen katholieken, socialisten, protestanten, liberalen) zoals dat in de vorige eeuw gold. Er was in die verguisde 'zuilen' echter meer weerwoord en onderlinge controle dan in de huidige bubbels! Daarom is de stelling gerechtvaardigd dat de bubbels, gevaarlijker zijn en tot meer polarisatie leiden. Kijk naar Amerika, waar de tegenstellingen en het onbegrip tussen groepen alleen maar groter worden. Dit is mede een gevolg van de sturing die de Social Media doen onder invloed van hun doel dat gericht is op geld verdienen. Dat jouw denken en jouw omgeving daarbij een bepaalde kant op worden geduwd, is een ongewenst bijeffect.

Hoe je te wapenen?

Dat is niet zo simpel te zeggen. Veel is afhankelijk van jezelf; je eigen gedrag bepaalt in hoge mate je privacy. Wat wil je, en tegen welke prijs? Bij het gebruik van gratis, niet-OpenSource-programma's zijn jouw gegevens de prijs die je betaalt. Gebruik daarom bij voorkeur OpenSource-programma's. Ik geef hieronder wat algemene richtlijnen waarmee je je privacy beter kunt beschermen. Wil je je privacy écht veilig houden in deze wereld, verban dan alle elektronische apparaten uit je leven en betaal alles cash.
In het algemeen is het goed om ook te kijken naar je internetprovider. Hoe gaat die om met privacy? XS4all was altijd al op privacy gericht, uit XS4all is Freedom[5] voortgekomen, die privacy nog hoger in het vaandel heeft staan. En natuurlijk lees je de privacyverklaringen van de aanbieders voordat je daar 'Ja' tegen zegt.

Kijk eens de 'andere kant' op!
Lees online-artikelen van een andere krant, kijk eens bewust naar media die een ander geluid laten horen. Daardoor kunnen de algoritmen je niet in een hokje plaatsen. Het verruimt wellicht je blik en stemt tot nadenken.

- Lees eens de uitingen van andere partijen.
- Ben je 'Links', kijk dan ook af en toe naar PowNed, Opiniez of De Dagelijkse Standaard[6].
- Ben je 'Rechts', hoor dan ook eens het geluid van de VPRO, Joop of AFA[7].Gebruik je browser goed.

Vermijd de cookies van derde partijen. Wissel regelmatig van browser (Edge, Chrome, FireFox, Safari ...). Stel je browser zo in dat je geen gegevens lekt of gebruik een privacyveilige browser zoals Brave, Aviator of Comodo Dragon[8]. Veel browsers zijn uit te breiden met toevoegingen (extensies) die je privacy verhogen, denk aan: 'uBlock Origin', 'I don't care about cookies', 'Cookie Bro', 'Fingerprint Defender'. Loop de opties van de gebruikte browsers na op ongewenste instellingen. Lees de artikelen die Ruud Uphoff en ik daarover hebben geschreven nog eens goed.

De meeste browsers hebben een incognito-modus die je kunt gebruiken wanneer je heel privacygevoelige zaken wenst op te zoeken. Of verberg je zelf helemaal door de TOR-browser te gebruiken.
Ook is het verstandig om een privacyveilige zoekmachine te gebruiken zoals Startpage.com of DuckDuck Go.

Gebruik Social Media selectief en anders

Kijk uit wat je post, lees het geschrevene nog eens na voordat je op de verzendknop drukt. Wil je wel deelnemen aan de discussie? Wil je wel de bagger die mensen vaak over zich heen krijgen?
Misschien is het een goed idee om meerdere accounts te hebben. Een voor de gezelligheid en een andere, meer anoniem, om je mening en vragen te ventileren.
Post eens iets ironisch, dat snappen 'de algoritmes' minder goed en doet ze de andere kant op 'denken'.

Let op de foto's en filmpjes die je post. Houd de mensen uit beeld of maak ze op een andere manier onherkenbaar. Haal ook de locatiegegevens uit de foto's die je deelt en mogelijk ook alle andere informatie die in de Exif-informatie[9] van de foto staat. Dit kan met verschillende programma's, waaronder ExifDataView van Nirsoft en met Scrambled Exif uit Google Play of ViewExif uit de App Store.

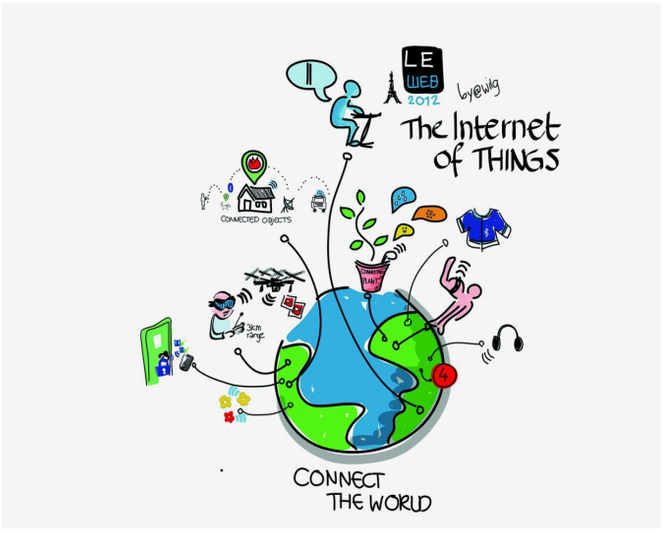
Gebruik alternatieven voor de apps Facebook, WhatsApp[10] en Instagram[11].
Je zou kunnen denken aan Signal, Mastodon en Diasporo. Deze zijn privacyveilig, maar de meeste van je contacten bevinden zich daar (nog) niet. Breng ze ervan op de hoogte dat je verhuist en waarom je dat doet. Als er één schaap over de dam is …

Stel je mobiel goed in
Stel de instellingen van je mobiele apparaten goed in. Loop zowel de algemene instellingen als die van de specifieke applicaties na[8]. Denk hierbij aan advertentietracking, cookies van derde partijen; weiger die en/of gooi ze weg.

Let ook op het openstellen van je contactgegevens en het toegang geven tot je foto's en bestanden. Vergeet niet uit te loggen nadat je Facebook of Google hebt gebruikt. Doe je dat niet, dan kunnen de advertentienetwerken jouw bezoeken aan andere websites blijven volgen.

Let ook op het toegang geven van apps tot je locatie, camera en microfoon. Ter voorkoming van afluisterpraktijken waarschuwden de Nederlandse inlichtingendiensten onlangs nog voor het meenemen van mobiele apparaten in vergaderingen. Denk ook aan de spraakassistent; die staat meestal standaard aan en brieft veel door.

Wil je helemaal veilig mobiel werken, overweeg dan een alternatieve telefoon zoals de BlackPhone.



Internet der dingen (IoT)
Deze term wordt gebruikt voor apparaten die ons moeten bedienen, denk daarbij aan ‘slimme’ speakers, camera’s en domotica. Vaak blijkt dat die veel te open staan. Google’s nest luisterde bijvoorbeeld standaard naar al het geluid in de ruimte waarin het staat, vaak de woonkamer. Er luisterden mensen mee om de algoritmes te verbeteren. De meest gênante gesprekken werden zo door derden beluisterd.

Kijk dus van deze apparaten altijd de instellingen na. Kijk ook of de laatste software is geïnstalleerd, wijzig de standaard wachtwoorden en vergewis je er regelmatig van dat je de laatste veiligheidsupdates hebt geïnstalleerd. Nog beter is het om dit soort apparaten in een apart, van je computers en mobiele apparaten, gescheiden netwerk op te nemen.

Tot slot

Je wapenen tegen aantasting van privacy is een continu proces, waarbij je steeds bewust moet zijn van de consequenties van je gedrag. Je tegen malware wapenen is eenvoudiger. Dagelijks een goede back-up maken, die te benaderen is vanaf je dagelijkse account, is voldoende. Verder moet je zelf kijken welke van de genoemde maatregelen bij je passen. Je zult zelf de afweging tussen nut en noodzaak moeten afwegen. Tenslotte blijft het altijd een kwestie van balans.

Links:

1. /The Social Dilemma http://bit.ly/r-tsd-
2. Complottheoriëen http://bit.ly/r-vk-ct
3. Algoritmen http://bit.ly/r-algo
4. Openbare bronnen http://bit.ly/r-opbr
5. Freedom https://bit.ly/r-bof
6. DDS http://bit.ly/rj-dds
7. AFA http://bit.ly/r-afa
8. Privacy Browser http://bit.ly/r-pvb
9. Exif verwijderen http://bit.ly/r-exif
10. WhatsApp http://bit.ly/r-wa-onv
11. App Alternatieven http://bit.ly/r-altapps

Algemene Links:

- Internet privacy http://bit.ly/r-ipr
- Bits of Freedom http://bit.ly/r-bof
- Privacy First http://bit.ly/r-pf