# Don’t like je Facebookaccount?

27 maart 2018

## Privacy en linking

Op Facebook ben je behoorlijk open en bloot. Wie kijken er allemaal direct mee of via links van jouw vrienden? Daar staat niet iedereen bij stil en op een waterdichte controle behoef je al helemaal niet te vertrouwen!

Maar ik zet daar toch helemaal geen vertrouwelijke informatie of klantgegevens op? Het linken aan personen, locaties, foto’s, geluid of teksten elders kan echter van basale info Deep Data maken.

## Data mining of piracy

Data zijn goud waard. Hele ICT-industrieën, wetenschappers en overheden  zien daar brood in. De grens tussen ethisch verantwoord en crimineelgebruik blijkt nogal eens flinterdun. Kan je Apps die jou helpen om persoonlijke gezondheidsprofielen  op te stellen nog vertrouwen? Zie Cambridge Analytica. Om het over piraterij, cyberwar en spionage nog maar niet te hebben.

Regelmatig is het onduidelijk of onvoorzien waar de data op Facebook uiteindelijk belanden. Dit zowel op plaatsen als in verbanden waar je zeker niet wilt hebben. Invloed heb je daar in de praktijk nauwelijks op. Roddeljournalisten die na medische gegevens van BN-ers hengelen, farmaceuten op zoek naar nieuwe markten, of  tegenstanders die iemand ziek, zwak of gek willen verklaren. Het is allemaal mogelijk.

## Nieuws- en advertentiewaarde

De correctheid en betrouwbaarheid van nieuwsberichten op Facebook is al vaker het punt van discussie geweest. Trollen. politiek correcte (?) betaalde journalisten en richtingsturende filters selecteren het nieuws op geprogrammeerde wijze voor. Wat is waar, manipulatief of onwaar?

Advertenties krijgen een stuk hogere doelmatigheid als zij selectief bij de mensen belanden die daar net emotioneel voor open staan en/of het gewenste profiel hebben. De dataverzamelaars bieden het allemaal precies op maat aan. Stel nu eens dat hier straks ook medische beslissingen en zorgvoorzieningen mee gemanipuleerd worden. Zie al het gedoe om verkiezingscampagnes.

## Blaming en shaming

In toenemende mate gebruiken onverlaten Facebook om te blamen en te shamen. Niet alleen om opponenten of concurrenten in een kwaad daglicht te stellen maar ook om onwelgevallige behandelmethoden onderuit te halen.

Tegenstanders van vaccinaties en traditionele geneeskunde weten daar op de social media goed weg mee. Omgekeerd probeert de tabaksindustrie aan te tonen dat de schadelijkheid van roken wel meevalt.

## Het probleem met Big Data

Overigens is het hiervoor gestelde zeker niet alleen de schuld van Facebook. Alles is inherent aan het verzamelen van Big Data. Het valt vooraf niet goed en veilig te voorzien wat er met al die verzamelde data kan of gaat gebeuren.

Vooraf opgestelde privacyprotocollen kunnen dikwijls niet inschatten wat er morgen gaat gebeuren of worden slim omzeild. En de burger heeft vaak niet in de gaten wat GPS. persoonsgebonden scanners voor huisvuil. OV-passen en het deelnamen aan protestwebsites allemaal aan info voor derden kan opleveren.

## Nieuwe verbanden

Meer gezondheid en een betere veiligheid door wat privacy in te leveren. Klinkt logisch en heeft in de praktijk ook een duidelijke meerwaarde. Data / Insight Driven Healthcare en AI patroonherkenning bij pathologie, biochemie en diagnostiek zijn inmiddels een substantieel deel van e-health geworden. Dat moeten wij dan ook zeker niet wegdoen.

Problemen dreigen er echter als de nieuw gelegde dataverbanden ineens selectie- of beïnvloedingscriteria gaan opleveren die in verkeerde handen kunnen komen. Uitsluiting door verzekeraars, werkgevers en van zorg bijvoorbeeld. Of criminele en ongure mogendheden die onze gezondheidszorg qua kwetsbaarheid in kaart gaan brengen.

## Controle en toezicht blijven lastig

Het bewaken van de privacy wordt steeds lastiger. Overal data entry, sensoren en camera’s. Je kunt wel zeggen dat er wettelijk altijd een noodzaak moet zijn om gegevens te verzamelen en daarvoor de minst belastende methoden te gebruiken. Meteen duiken dan sleepwetten, grote

belangen van derden en nieuwe algoritmen die ineens weer veel meer kunnen analyseren en combineren op.

De toezichthouders lopen te vaak achter de feiten aan of raken stiekem overruled. Burgers hebben daar vaak geen besef van.

Het antwoord op wel/ geen Facebook-account voor gezondheidswerkers blijft een lastige. Als medewerker dien je zelf heel alert te zijn wat er op de privépagina staat en binnenkomt. Bij twijfel het er gewoon niet opzetten. Maakt Facebook deel uit van de multikanaalsbenadering van de klant, huur dan een cyberbeveiligingsexpert in en draag zorg voor een alerte redactie.