**OVERIG MATERIAAL PRIVACY EN DATABESCHERMING
(Crash course Three)**

Wij bieden crashcourses aan op [www.tict.io](http://www.tict.io). Deze zijn in het Engels. Daarnaast hebben we in het verleden veel materiaal gemaakt in het Nederlands, dit is allemaal verzameld in dit word-document.

In dit document staat alles rond crash course twee, technologie algemeen. De Engelse versie staat hier: [www.tict.io/course-three](http://www.tict.io/course-three).

**Introductie**
Op technofilosofie.com doen we aan **toegepaste technofilosofie.**Het is ons doel om zoveel mogelijk mensen na te laten denken over de impact van technologie. Wij denken namelijk dat iedereen dat zou moeten doen. Iedereen zou een beetje een technofilosoof moeten zijn. Of je nu technologie ontwerpt, programmeert, implementeert of gewoon gebruikt. Of je nu een professional bent, of een vader, een coach, een vriend, vakantieganger of gewoon een mens.

Moderne digitale technologie rukt op en wij moeten leren om ons daartoe te verhouden. Het gaat daarbij niet om een abstract gegeven, maar gewoon om onze relatie alledaagse, hedendaagse technologie. Smartphones, e-mail, platformen zoals Uber, Tinder, sociale media, sensoren, slimme meters, en ga zo maar door.

**DAT IS ONZE MISSIE: ZOVEEL MOGELIJK MENSEN ZO GOED MOGELIJK TE LATEN NADENKEN OVER DE IMPACT VAN TECHNOLOGIE**.

We bieden daarom ook materiaal aan, zoals in dit word-document. Hierin staan verwijzingen naar artikelen, video's e.d. De tekst valt onder creative commons, maar de afbeeldingen, verwijzingen, clips en video's niet altijd. Het is dus belangrijk dat je je daar zelf van op de hoogte stelt, als je materiaal wilt gebruiken. Bij twijfel, check de [website](https://creativecommons.nl/) van creative commons.

**Onderwerpen in dit document:**

1. Wat zijn manieren om jezelf te beschermen tegen privacy – schendingen.

En dat natuurlijk allemaal op de manier die je van ons best gewend bent.

# **(BIG) DATA – PRIVACY**Is het jou wel eens opgevallen dat ‘Big Data’ altijd met hoofdletters wordt geschreven maar ‘privacy’ slechts zelden? Dat doen wij dus wel. Op deze pagina verzamelen we allerlei willekeurige inzichten rondom het Privacy en Gegevensbescherming. Wil je daar liever een samenhangend verhaal over lezen, dan verwijzen we je naar [Je Hebt Wel Iets Te Verbergen](https://www.bol.com/nl/p/je-hebt-wel-iets-te-verbergen/9200000088419899/?suggestionType=suggestedsearch&bltgh=rQN9E97USz2NWaSbxuRM0Q.1.2.ProductTitle), het boek van Maurits Martijn en Dimitri Tokmetzis.

Of we verwijzen ja naar deze [column](http://technofilosofie.com/wp-content/uploads/2018/01/Columns_Bron_RensvdVorst_2018_44.pdf) over Privacy (die je in 250 woorden uitlegt dat de wet op de gegevensbescherming wel degelijk zinvol is!). Of deze uitleg rondom het concept [spionagekapitalisme](http://technofilosofie.com/spionagekapitalisme/), dat je uitleg dat er grotere issues zijn dan gerichte advertenties.

Deze pagina is meer een doe – het – zelf – suggestie – toolkit om je eigen Privacy te bewaken. Je vind hier niet de normale [lijstjes](https://www.theguardian.com/technology/2015/mar/06/tips-tricks-anonymous-privacy) (gebruik een lang wachtwoord, geef je gegevens niet zomaar weg, gebruik VPN, gebruik disposable e-mailadressen, en zo….) want we weten allemaal dat dat een achterhoedegevecht is. En het is hard werken. En het is saai! Daarom hebben we hier de leukere, creatievere manieren verzameld om je Privacy te bewaken. Als dat zo belangrijk is, moet het ook een beetje leuk blijven.

**Manieren om te ontkomen aan gezichtsherkenning**
Eén van de grote problemen van privacy is gezichtsherkenning. Deze techniek ontwikkelt zich razendsnel en overal worden systemen ontwikkeld die je steeds beter kunnen herkennen. Zelfs je telefoon herkent je. Er NIET aan meedoen wordt steeds moeilijker, daarom ontwikkelde men in Japan een manier om niet herkend te worden, namelijk de [Privacy Visor](https://www.pcworld.com/article/2969732/how-japans-privacy-visor-fools-facerecognition-cameras.html). Weird, maar heel effectief.

Wil je niet getagged worden op Facebook of op een ander social media platform, dan raden we de [Glamouflage](https://www.theatlantic.com/technology/archive/2013/10/avoid-facial-detection-algorithms-with-a-t-shirt/280253/) aan. Dit is kleding met daarop gezichten van beroemdheden, die de systemen van Facebook verwarren. Het voorbeeld hiernaast zorgt ervoor dat Facebook – Tagging helemaal wild wordt, want Michael Jackson en Barack Obama samen op één foto! Je ziet, het product is al wat ouder, want Michael is niet meer, maar nieuwe varianten met nieuwe beroemdheden zijn te verkrijgen.

Of wat dacht je van het werk van Leo Selvaggio van [URME (You Are Me) Surveillance](http://www.urmesurveillance.com/). Hij maakte een masker van zichzelf, dat gezichtsherkenningssystemen voor de gek houdt. Creepy, maar lang niet zo creepy als de manier waarop deze systemen steeds vaker ingezet worden.

Een andere artiest is Adam Harvey, die weer andere ideeën heeft. Bijvoorbeeld hippe manieren om [mensen op te maken](https://ahprojects.com/cvdazzle/) en om hun haar te doen, waarbij de gezichtsherkenningssoftware volledig van slag raakt. Zou het niet cool zijn als gezichtsherkenningssoftware zou leiden tot een hele nieuwe modetrend? Of, als we het over mode hebben, dan ontwierp Adam ook een [stealthware](https://ahprojects.com/stealth-wear/) kledinglijn. Een modelijn, los gebaseerd op de Burqa, die het onmogelijk maakt voor een drone om je te herkennen.

Wat ik zelf heel intrigerend vind, is een project in ontwikkeling waarbij je gezicht niet wordt afgedekt of onherkenbaar gemaakt, maar waarbij de algoritmes misleidt worden door een [hyperface](https://ahprojects.com/hyperface/) (een object waarin zoveel gezichten te herkennen zijn, dat het algoritme het niet meer trekt).

En dan is er natuurlijk nog de pixelhead Balaclava van Adafruit. Een manier om online en offline te vermengen en tegelijkertijd onherkenbaar te worden.

**Manieren om anoniem te zijn op social media**Natuurlijk kun je eenvoudig een nep – account aanmaken. Alhoewel wel dat ook steeds ingewikkelder wordt. Of je kunt geen social media gebruiken (nog minder eenvoudig). Maar er is een betere en subtielere manier om je privacy te bewaken op de sociale media platforms. Het [Go Rando](https://bengrosser.com/projects/go-rando/) project van Benjamin Grosser is zo’n subtiele oplossing. We weten allemaal dat Facebook – aan de hand van je likes en emoticons – jou snel leert kennen. Go Rando is een plugin die je installeert in je browser en elke keer als je op een ’emotie’ klikt, wordt willekeurig een emotie geselecteerd en gepost. Op die manier wordt er ruis gecreëerd, die de kunstmatige intelligentie van Facebook verwart, voor jou, maar als iedereen het gebruikt, voor iedereen. [Artikel.](https://www.washingtonpost.com/news/the-intersect/wp/2017/02/16/how-to-hide-your-true-feelings-from-facebook/?utm_term=.91d32d1fb323)

Ik ben ook al een tijdje op zoek naar een algoritme of plugin die random allerlei zaken post op Facebook. Gewoon mijn echte naam, en dan maar verwarren van Batik naar Breibart. Van veganisme naar Alex Jones en terug. Maar, ik heb het nog niet gevonden. Ken jij wel zo’n oplossing. Laat mij het weten op rens@technofilosofie.com.

**Manieren om je cookies te fucken**
Firefox heeft een nieuwe website [TrackThis.link](https://trackthis.link/) waarin je kunt kiezen uit 4 profielen ((hypebeast, filthy rich, influencer, doomsday) en vervolgens worden 100 grote websites volgestort met misleidende cookies. Tof. Artikel op [Variety](https://variety.com/2019/digital/news/firefox-track-this-100-tabs-1203253096/) hier.

**Manieren om je (health)tracker te fucken**
Je hoort steeds vaker stemmen opgaan om bepaalde businessmodellen te koppelen aan data.  Bijvoorbeeld, hoe je rijdt combineren met je verzekeringspremie. Of, hoeveel je beweegt, koppelen aan je verzekering. Maar dat is natuurlijk prima te hacken, technisch, maar nog veel beter, mechanisch.

**Manieren om anoniem te zoeken**

Als we jeuk in ons kruis hebben, dan vertellen we dat eerder aan Google dan aan onze vriendin. Steeds meer mensen zien de absurditeit daarvan in en denken na over manieren om anoniem(er) te zoeken. Dit [artikel](https://www.wired.com/story/privacy-browsers-duckduckgo-ghostery-brave/) helpt daarbij.

**Manieren om ID – Fraude te voorkomen**

Je ziet het steeds vaker. Een smartphone van 1000 euro met daarin gestoken een bankpasje en een ID-bewijs. En dan dat uit je kontzak laten steken. Uitlokking tot identiteitsfraude is misschien nog een eufemisme voor deze mensen. Daarom ontwikkelde Tim Schut, lezer van Appen is het Nieuwe Roken, een alternatief insteekhoesje. Laat je inspireren.



**Verder:**

* Bijlage A -> Nog meer informatie en links (achtergrond)
* Bijlage B -> Dingen om van te genieten
* Bijlage C -> Oefeningen & manieren om onze relatie met deze aandachts-tech te ervaren.
* Bijlage D -> Essay over informatie en filters

Op deze pagina vind je hieronder alles wat we verzameld hebben uit eerdere cursussen rond het thema aandacht. Je hoort het misschien wel eens zeggen, we leven in een aandachtseconomie. Maar wat betekent dat nu precies? En wat betekent het voor ons? De tekst die we hebben opgeschreven valt onder Creative Commons, maar de afbeeldingen, verwijzingen, clips en video’s niet altijd. Het is dus belangrijk dat u zich daar zelf van op de hoogte stelt, als je materiaal wilt gebruiken. Bij twijfel, check de [website](https://creativecommons.nl/) van creative commons.