RIJKSMUSEUM VOOR DIGITALE ARTEFACTEN

VRIJHEID EXPOSED

BITS OF FREEDOM
Voor jouw internetvrijheid

VRIJHEID EXPOSED

Datagraaiers

Op het internet word je steeds meer gemonitord en wordt je vrijheid ingeperkt

Het internet bestaat steeds meer uit apps. Hoewel deze plekken heel vrij en open kunnen voelen, zijn ze gemaakt door bedrijven die hun eigen regels opstellen. Jouw vrijheid van meningsuiting kan op dit soort plekken niet worden gegarandeerd. Het bedrijf bepaalt hier immers wat wel en niet door de beugel kan.

Je geeft deze apps heel veel informatie over jezelf en je vrienden. Foto's en chats bijvoorbeeld. Maar ook informatie over wanneer je de app gebruikt en waar je op dat moment bent.

Bedrijven en de overheid hebben er veel voor over om inzicht te krijgen in wie jij bent. Wat vind je belangrijk, waar ben je gevoelig voor? Eigenlijk worden deze gegevens altijd gebruikt om jouw gedrag en keuzes te beïnvloeden. Er wordt wel eens gezegd dat data het "nieuwe goud" is. Dat komt omdat zo'n app veel geld kan vragen voor toegang tot jouw gegevens.

Voor bedrijven geldt: hoe meer data hoe beter. Voor jou geldt dat hoe transparanter je bent, hoe kwetsbaarder je wordt. Wie heeft welke informatie over jou?

Doe het zelf!

Voor veel apps bestaan er (privacyvriendelijke) alternatieven.
Ga naar **https://toolbox.bof.nl/detox**

Facebook

Facebook

Facebook Messenger

Instagram

WhatsApp

Google

Google Search

YouTube

Chrome

Gmail

Google Maps

Jouw informatie

Hoeveel geld je hebt

Je vingerafdruk

Waar je bent

Dat je verkering uit is

Met wie je appt

De websites die je bezoekt

Je zoekopdrachten

Het nieuws dat je tot je neemt

Het boek dat je leest

RIJKSMUSEUM VOOR DIGITALE ARTEFACTEN

VRIJHEID EXPOSED

BITS OF FREEDOM
Voor jouw internetvrijheid

Slimme apparaten?!

Slimme apparaten?

Steeds meer van de dingen die we gebruiken zijn met het internet verbonden. Ze bevatten vaak verschillende sensoren en soms camera's en microfoons. Samen vormen ze het "Internet of Things". De thermostaat, koelkast en stofzuiger. Onze telefoons en horloges. De beveiligingscamera's op straat en de auto's waarin we rijden. We noemen deze apparaten "smart", of "slim".

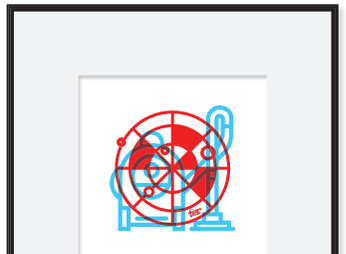
Dit levert ons veel nieuwe gemakken op. Maar "slim" heeft ook een schaduwzijde. Het gebruik van deze producten genereert bijvoorbeeld heel veel data. Die gegevens behoren toe aan het bedrijf dat het product maakt. De televisie weet waar we naar kijken. De speakers weten waar we naar luisteren. Het horloge weet waar we gaan en staan. Deze gegevens zijn vaak een extra - of soms zelfs de enige - bron van inkomsten voor een bedrijf. Adverteerders betalen er namelijk goud geld voor!

Ontdek hier de wondere wereld van het Internet der Dingen.

Doe het zelf!

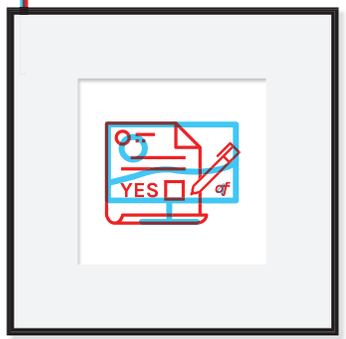
Benieuwd wie wat van jou weet? Vraag bedrijven om inzicht in de gegevens die ze van je hebben!

Ga naar **https://pim.bof.nl** en maak gebruik van de Privacy Inzage Machine!



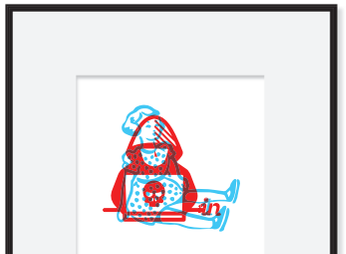
Scant je huis

Door middel van een camera, sensoren en software creëert de robot-stofzuiger Roomba een kaart van jouw huis en bepaalt hij zijn positie op die kaart. De Roomba haalde in 2017 het nieuws omdat bekend werd dat het bedrijf achter het huishoudelijk hulpje van plan is de plattegronden te verkopen van de huizen waarin het rondzoekt. Wie zou deze plattegronden willen kopen? En waar zouden ze voor gebruikt kunnen worden?



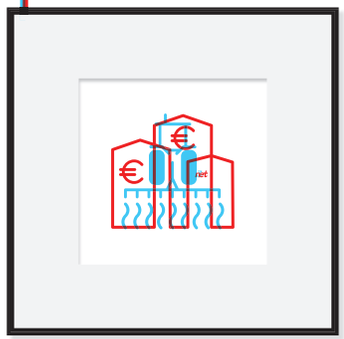
Kijkt met je mee

Wie in 2018 een smart-tv kocht, is waarschijnlijk akkoord gegaan met de voorwaarden van de fabrikant (bijvoorbeeld Sony) en met de voorwaarden van de softwareleverancier (bijvoorbeeld Google). Die voorwaarden en privacybeleid zijn vaak lang en verwarrend. Veel gebruikers lezen deze documenten niet en gaan zonder het te weten akkoord met de verspreiding van hun persoonsgegevens zoals locatie en kijkgedrag. Niet akkoord gaan is trouwens zo simpel niet. De voorwaarden weigeren betekent meestal dat je de televisie niet kunt gebruiken. Is toestemming wel echt toestemming wanneer deze is afgedwongen?



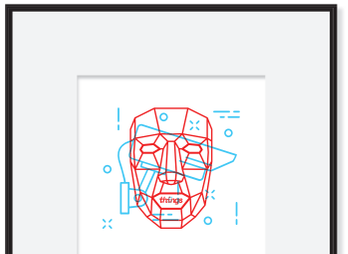
Speelt met je

In 2015 introduceerde Mattel de Hello Barbie: een pop voorzien van WiFi en software die stemmen herkent. Barbie stelt je kind vragen, de antwoorden slaat Barbie op in de cloud. Zo leert Barbie haar gesprekspartner steeds beter kennen. Maar het is niet alleen Barbie die meeluistert. Onderzoekers leerden al snel dat je makkelijk bij de barbiepop in kan breken. Daarmee kunnen kwaadwillenden meeluisteren met gesprekken, of zelf berichten namens Barbie verzenden. "Verbonden zijn" klinkt leuk, maar maken we onszelf soms niet onnodig kwetsbaar? En wat krijgen we er eigenlijk voor terug?



Keert zich tegen de eigenaar

Bij tractoren denk je aan boeren die met hun handen werken en zelf repareren wat stuk gaat. Vanaf 2017 niet meer. Dat jaar kwam tractorfabrikant John Deere negatief in het nieuws. Boeren mochten hun eigen tractor niet repareren. In plaats daarvan moesten ze gebruik maken van speciale John Deere-reparateurs en John Deere-onderdelen. Maar deze waren vaak duurder en niet altijd beschikbaar. Als de boeren toch aan hun eigen tractors sleutelden, zette John Deere op afstand de tractor uit. Met als gevolg dat boeren niet aan het werk konden, een oogst misliepen en zouden zij als eigenaar van de tractor niet zelf mogen bepalen wat ze wel en niet met de tractor doen?



Kan meer dan kijken

In 2016 werd bekend dat de politie al sinds 2009 experimenteerde met bodycams. En in 2017 kreeg "politievlogger" Jan-Willem landelijke bekendheid vanwege de filmpjes die hij tijdens zijn dienst maakte en op YouTube zette. Ook in China maakt de politie gebruik van camera's. Daar controleren beveiligingscamera's op straat of mensen door rood lopen. Omdat de camera's gezichten herkennen, kunnen burgers meteen worden bebost. Camera's kunnen niet alleen gezichten herkennen, maar ook nummerborden. Ze detecteren beweging, geluid en temperatuur. Door beelden meteen te analyseren kunnen ze bijvoorbeeld een winkelier laten weten dat er een potentiële klant aankomt. Moeten we grenzen stellen aan de inzet van deze nieuwe technologie?

RIJKSMUSEUM VOOR DIGITALE ARTEFACTEN

Start

Het is 2045...

De afgelopen jaren hebben burgers gestreden voor de bescherming van hun privacy. En met succes! Bedrijven hebben een einde gemaakt aan hun privacyschendende praktijken. Adverteerders zijn teruggefloten, massasurveillancewetten teruggedraaid. Burgers worden niet meer gevolgd en geprofileerd. De vrijheid van de burger in het digitale tijdperk is beschermd!

Op 5 mei vieren we dat we in een vrije, democratische rechtsstaat leven. Dat is ook in Nederland niet vanzelfsprekend. Digitale technologie geeft burgers grote vrijheid, maar maakt ons ook kwetsbaar. Het Rijksmuseum voor Digitale Artefacten heeft een tentoonstelling gemaakt waarin privacyschendingen nog de normaalste zaak van de wereld waren. Hoeveel weet jij van de geschiedenis!?

Vrijheid EXPOsed

Speel mee & Test je kennis!

BITS OF FREEDOM

Voor jouw internetvrijheid

RIJKSMUSEUM VOOR DIGITALE ARTEFACTEN

VRIJHEID EXPOSED

BITS OF FREEDOM
Voor jouw internetvrijheid

Zou het echt waar zijn?

Onschuldige burgers zijn steeds vaker in het vizier van de overheid

In 2017 werd de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (ook wel de "sleepwet" genoemd) aangenomen. In deze wet wordt geregeld wat de geheime diensten wel en niet mogen.

De geheime diensten beschermen de veiligheid en de democratische rechtsorde. Dat doen ze door het verzamelen en analyseren van informatie. Ze kunnen bijvoorbeeld informanten raadplegen, Facebook-groepen monitoren, of internetverkeer onderscheppen. Met de nieuwe wet mag daarnaast communicatie van grote groepen Nederlanders stelselmatig en op grote schaal worden afgeluisterd. De verzameldrift van de overheid verandert iedere burger in een potentiële bedreiging. Dat staat haaks op wat hoort in een vrije samenleving. Het is dan ook niet gek dat bij het referendum op 21 maart 2018, een meerderheid tegen deze wet stemde!

Maar deze wet staat niet op zichzelf. Het past binnen een bredere trend waarin burgers steeds vaker in het vizier zijn van de overheid.

Foto's van kentekens worden gefotografeerd en vier weken bewaard. Passagiersgegevens, zoals wie wanneer waar naartoe reist, worden uitgewisseld binnen en buiten Europa. De overheid wil dat gegevens over wie waar communiceert worden opgeslagen. De Nationale Politie houdt zich steeds meer bezig met "predictive policing". Predictive policing is de praktijk waarbij je, aan de hand van big data, criminaliteit probeert te voorspellen. De gegevens die daarvoor worden gebruikt zijn onder andere criminaliteitscijfers, maar ook informatie over inkomen en afkomst, en bijvoorbeeld de afstand van een woonwijk tot de dichtstbijzijnde snelwegoprit. Met een beetje pech word jij geprofileerd als een risico-burger en een grote kans bestaat dat je niet zult weten waarom. Bepaalde bevolkingsgroepen zullen op basis van de gekozen "criteria" en bestaande vooroordelen meer pech hebben dan anderen. Hoe is dit rechtvaardig?

Doe het zelf!

Steun het werk van Bits of Freedom. Word vrijwilliger, partner of doe een financiële bijdrage. Kijk op **www.bitsoffreedom.nl**

RIJKSMUSEUM VOOR DIGITALE ARTEFACTEN

VRIJHEID EXPOSED

BITS OF FREEDOM
Voor jouw internetvrijheid

VRIJHEID EXPOSED

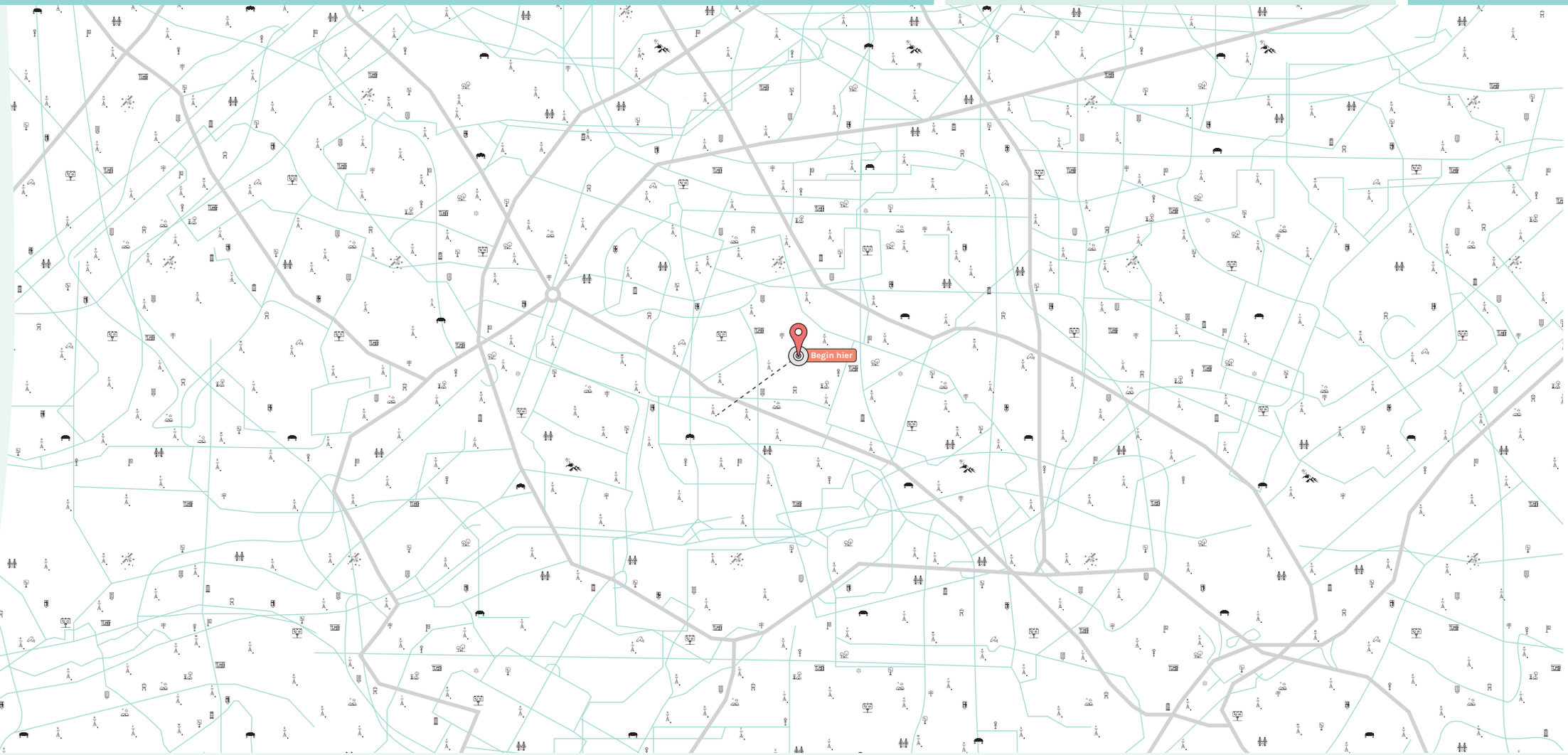
Spoorzoeker

Door onze mobiele telefoons zijn we heel makkelijk te volgen

De meeste smartphones beschikken tegenwoordig over GPS, WiFi en Bluetooth. Deze technieken worden gebruikt voor het bepalen van je locatie. Dat is voor jou soms hartstikke handig. Als je de weg moet weten, bijvoorbeeld. Of zodat je telefoon, zodra je thuis bent, automatisch gebruik maakt van je eigen internetverbinding.

Maar het maakt ons ook gevoelig voor "tracking". Tracking in de online wereld ken je misschien wel: informatie over wat we online lezen, luisteren en kopen wordt opgeslagen zodat die gegevens samen als "profiel" verkocht kunnen worden aan adverteerders. Maar ook offline gebeurt dit steeds vaker. Winkeliers volgen je gang door hun winkel, of door de winkelstraat. Reclamezuilen monitoren jouw reactie op de reclames die je te zien krijgt. Mobiel verkeer wordt ook gebruikt om mensenmassa's in de gaten te houden tijdens grote evenementen. En om achteraf te kunnen achterhalen wie er eigenlijk bij die demonstratie of voetbalwedstrijd waren.

Het is een vervelende gedachte: kun je je telefoon wel bij je hebben zonder dat je deze gevoelige informatie over jezelf "weggeeft"?



Doe het zelf!

Weet jij met welke bedrijven jij je locatie deelt? Kijk nu wie je allemaal toegang geeft.

iPhone
Ga naar: Instellingen > Privacy > Locatie-voorzieningen

Android
Ga naar: Instellingen > Beveiliging en locatie