CLOUDY WITH A CHANCE OF STORAGE

Data is macht

De vele partijen die data over ons verzamelen, verzamelen letterlijk macht. Wie veel over ons weet, kan die kennis ook gebruiken op manieren die ons niet goed uitkomen. Voor veel mensen zijn de risico's van ‘Big Data’ helaas nog niet duidelijk.

Je zou kunnen zeggen dat die gevaren op twee terreinen liggen. Het eerste terrein is voor de meeste mensen, als ze het eenmaal meemaken, goed te herkennen: misdaad.

Een bekend en meteen ook het meest schokkende voorbeeld daarvan, zagen we tijdens de Tweede Wereldoorlog. Vóór de oorlog had iedere gemeente een bevolkingsregister waarin precies terug te vinden was tot welk kerkgenootschap iemand behoorde. Handig, totdat bleek dat ook de bezetter via deze registers gemakkelijk kon achterhalen wie er joods was[14]. Het ophalen van joden, werd daardoor eenvoudig een kwestie van ‘lijsten afwerken’. De misdaden van de holocaust kunnen we beschouwen als een van de meest gruwelijke collectie misdaden ooit begaan.

Dichterbij ons dagelijks leven komen we allerlei gevallen van identiteitsdiefstal, fraude en chantage tegen. Met behulp van de gelekte ledenlijst van datingwebsite Ashley Madison, een dienst die het eenvoudig maakte om vreemd te gaan, werden na afloop allerlei mensen afgeperst[15]. Dat er een levendige handel in creditcard gegevens is, hebben we langzaamaan ook wel door. Deze negatieve gevolgen van de opkomst van de informatiemaatschappij zijn voor de meeste mensen goed te begrijpen: ze lijken op wat we al kennen.

VOORBEELD

Ashley Madison
In 2015 lekte de ledenlijst van datingwebsite Ashley Madison uit. Deze datingwebsite heeft als doel mensen die willen vreemdgaan met elkaar in contact te brengen. De site had zo'n 30 miljoen leden, waaronder zeker 594 Nederlanders[16]. Door het lek was de lijst online in te kijken, wat flinke gevolgen had. Een onmeetbaar aantal relaties liep op de klippen, minimaal 2 mensen pleegden zelfmoord.

Het tweede gevaar van ‘Big Data’ ligt niet zozeer op het criminele vlak, maar kan wel grote negatieve gevolgen hebben voor de maatschappij. Technologieën die verregaande personalisering van diensten mogelijk maken, maken ook nieuwe, subtiele vormen van discriminatie mogelijk[17]. Zo komt het steeds vaker voor dat de prijs die iemand voor een verzekering betaalt, wordt vastgesteld op grond van een algoritme dat op basis van bepaalde


BIG DATA
IS
WATCHING
YOU

Denk al in de beginfase van een project na over hoe je met privacy en data omgaat. Dat klinkt (hopelijk) logisch, maar in de praktijk blijkt dit vaak niet het geval. In veel producten worden privacy features pas later ingebouwd, in het ergste geval pas na bezwaar door het brede publiek. Dit is niet altijd even eenvoudig, bijvoorbeeld omdat de software niet meer aangepast kan worden, de hardware infrastructuur niet goedkoop te vervangen is, of omdat het gekozen businessmodel het niet toestaat. Soms is privacyschending heel bewust tot stand gekomen, en wordt er gebruik gemaakt van zogenaamde 'dark patterns' om ervoor te zorgen dat mensen per ongeluk meer informatie weggeven dan ze willen. Onwil, bureaucratie en kennisgebrek maken het lastig om deze problemen adequaat aan te pakken. Door er vroeg bij te zijn en deze vraagstukken op tijd te onderzoeken, kunnen deze problemen hopelijk zo goed mogelijk worden ondervangen. → Dark Patterns p.123

Een goed voorbeeld is de OV-Chipkaart. Volgens Marleen Stikker, directrice van de Amsterdamse Waag Society, zijn bij het ontwerp van het OV-systeem duidelijk geen kritische hackers of privacy-deskundigen betrokken geweest[49]. Hierdoor doken er jarenlang veiligheidsproblemen op, die werden aangekaart door journalisten en hackers die zich zorgen maakten. Hoewel de oude OV-chipkaarten inmiddels zijn vervangen door duurdere, beter beveiligde varianten, blijft het systeem nog altijd privacy-onvriendelijk. Zo is het bijvoorbeeld onmogelijk om tegelijkertijd anoniem en met korting te reizen, iets dat voorheen wel kon[50]. Doordat anoniem reizen nu alleen tegen vol tarief mogelijk is, wordt dit effectief ontmoedigd.

Slecht ontwerp kan zelfs levensgevaarlijk zijn. In 2015 bleek het mogelijk om een nieuw model auto's van Jeep via het internet over te nemen en op afstand de remmen in te

drukken of de motor uit te zetten[51]. De enige manier om de software van updates te voorzien, was door een USB-stick met update-software in het dashboard van de auto te steken. Chrysler, het moederbedrijf van Jeep, besloot toen om 1,4 miljoen Jeeps terug te roepen. Zo blijkt maar weer dat er schrikbarend slecht wordt nagedacht over de privacy en veiligheids-issues die kunnen ontstaan gedurende de volledige gebruikscyclus van een product of dienst.

Dit is een probleem dat al langer speelt. Volgens een recente schatting door onderzoekers van het Franse kenniscentrum Eurecom en de Duitse RuhrUniversität is het, voor ongeveer een kwart van de op het internet aangesloten apparaten, zeer eenvoudig om ze over te nemen[52]. Deze apparaten zijn veelal te benaderen met bekende standaard wachtwoorden.

De meeste problemen zullen niet snel worden opgelost. Vaak zijn bedrijven traag met het aanbieden van updates omdat het ze geld kost, iets dat een probleem vormt bij veel Android smartphones. In andere gevallen is er wel een oplossing beschikbaar, maar bereikt die het systeem niet. In het geval van de Jeeps van Chrysler moest er handmatig een USB-stick in het dashboard worden ingevoerd. Zo is er altijd een percentage apparaten dat door haar gebruikers niet geüpdatet wordt[53]. In het ergste geval is het product een flop, bereikt het 'end of life' status of gaat het bedrijf failliet. De meeste mensen blijven deze apparaten toch gebruiken.

Zelfs een up-to-date apparaat kan morgen onveilig blijken wanneer hackers een nieuw lek ontdekken. Software bouwen is en blijft mensenwerk.

Er gebeurt dus van alles tijdens de levensloop van een 'slim' product. Het is belangrijk dat een organisatie samen met een ontwerper op mogelijke problemen anticipeert en snel op in leert spelen. Dat kan door handleidingen en

VOORBEELD

De nationale verjaardagskalender
In 2015 en 2016 onderzoekt het Utrechtse medialab SETUP een interessante vraag: hoe moeilijk is het om een database van alle Nederlanders te maken door online bronnen bij elkaar te sprokkelen? Zou het mogelijk zijn om een dienst te ontwikkelen die van alle Nederlanders de verjaardagen hielp herinneren, en die ook nog eens cadeautjes aanbood op basis van de interesses van de jarigen?

Samen met data-experts werden enkele weekends lang verschillende bronnen bij elkaar gepuzzeld, zoals bijvoorbeeld Schoolbank.nl, voormalig sociaal netwerk Hyves, het telefoonboek, websites van sport- en werkverenigingen, enzovoort. Het bleek verrassend eenvoudig: geen enkele website bood weerstand tegen het massaal kopiëren van de gegevens.

Andere criminaliteit is meer gericht. De Amerikaanse familie Straters werd jaren geterroriseerd door een

cybercrimineel genaamd Kivimaki[63]. Hij liet pizza's en andere bezorgdiensten langskomen (die ze dan zouden moeten betalen), sloot online de elektriciteit af en misleidde politieagenten tot het plegen van gewapende bezoeken naar aanleiding van leugenachtige telefoontjes. De stress werd na jaren teveel, de ouders zijn nu gescheiden.

> *De meeste mensen denken bij het woord 'hacker' aan een crimineel, maar experts maken onderscheid tussen twee soorten hackers: white-hat en black-hat, 'ethische' en criminele. In elke grote stad vind je zogenaamde 'hackerspaces': clubhuizen van ethische hackers die daar samenkomen. Ze kunnen je vaak meteen met technologische vragen helpen. Op Hackerspaces.nl vindt je een lijst van Nederlandse hackerspaces. Ze organiseren ook open dagen.*

Hackers hebben tegenwoordig een grote invloed op het ontwerp van digitale systemen. Zij wijzen met plezier alle gaten aan. Een groot aantal hackers is maatschappelijk begaan: naast de praktische gevaren voor identiteitsdiefstal en ander crimineel misbruik herinneren zij ons vaak ook aan grotere maatschappelijke vragen. Ethische hackers zijn voor een belangrijk deel het geweten van de digitale maatschappij en houden vaak rekening met de situatie dat de maatschappij 'minder gezellig' zou kunnen worden.

Mocht je liever de geïnstitutionaliseerde hackerswereld willen ontmoeten, ga dan op zoek naar 'ICT security audit' bedrijven. Grote Nederlandse namen zijn Madison Gurkha en Fox IT.

Met de opkomst van partijen als Uber lijkt het bijvoorbeeld vanzelfsprekender te worden om GPS zenders aan de scooters van pizzabezorgers te koppelen. Wie een pizza bestelt kan online precies zien waar zijn pizza blijft, door de bezorger op een kaart te volgen[68].

Dit is een inbreuk op de privacy van de pizzabezorger. Die kan niet meer zo makkelijk van koers veranderen zonder de kans te lopen dit later aan zijn of haar baas te moeten uitleggen. Er zijn legio legitieme redenen om dat te doen, bijvoorbeeld om religieuze redenen, om medicijnen op te halen, of omdat mensen dit om sociale redenen doen. Als je bij deze voorbeelden denkt 'maar dat kan je toch gewoon uitleggen' dan mis je het punt: zonder antropologisch onderzoek is de kans groot dat er bepaalde gevoelige culturele, praktische of onvoorziene situaties ontstaan die je met je beperkte kennis niet had kunnen bedenken.

Er zijn oplossingen te bedenken die voor iedereen werken en die minder data opslaan. De klant wil niet het aantal kilometer tot zijn pizza weten, maar het aantal minuten. Berekenen hoe lang het duurt voor de pizza er ongeveer is, is voor navigatie-algoritmes geen enkel probleem. Door alleen het aantal minuten tot de aankomst aan te geven, heeft zowel de klant als de baas minder privacy-schendende informatie in het systeem.

Zo zijn er veel gevallen waar langer en kritischer nadenken leidt tot een oplossing die zowel de privacybelangen en het design als de bedrijfsprocessen ten goede komen.

PRINCIPE 4

BESCHERM JE DATA

Je zult informatie willen verzamelen over het gebruik van je creatie. Het opslaan van die informatie in de ‘cloud’ kan dan verleidelijk of zelfs onvermijdelijk worden. Maar het zou niet vanzelfsprekend moeten zijn.

De ‘cloud’ is in wezen een mooie naam voor ‘andermans computer’. Door deze vervanging worden de spanningen al beter zichtbaar: van wie is die computer? In welk land staat die computer? Vele critici hebben er op gewezen dat termen als ‘cloud’ en ‘cyberspace’ misleidend zijn omdat ze ons doen geloven dat het internet een grenzeloze en non-politieke plek is. Maar andermans computer staat altijd in een bepaald land, en dat land heeft eigen regelgeving over privacy en data-eigendom.

Sommige landen spelen hier actief op in. Zo profileert IJsland zich als een land waar journalistieke vrijheden ook naar het internet worden doorgetrokken. Ierland is ook een populair land voor de opslag van grote hoeveelheden data, precies vanwege de flexibele lokale regelgeving. Ook Nederland is enorm sterk aanwezig op het internet, maar dat is voornamelijk historisch zo gegroeid. Een van de eerste grote internet knooppunten, de Amsterdam Internet Exchange, werd hier ontwikkeld.

De eerste vraag die elke ontwerper zich zou moeten stellen is: is het essentieel om deze data in de cloud (andermans computer) te bewaren? Neem bijvoorbeeld fitness trackers. Deze hebben toegang tot extreem persoonlijke informatie, en die informatie wordt in veel gevallen standaard naar 'andermans computer' verzonden, bijvoorbeeld om het gemakkelijk online te kunnen delen. Maar in theorie is het niet nodig om de data naar het internet te uploaden. Fitness trackers zouden de data ook lokaal op de smartphone kunnen bewaren, en van daaruit de informatie eventueel kunnen vergelijken of verrijken met andere via het internet verkregen data. Ook het delen op sociale netwerken zou dan nog steeds mogelijk zijn.

Als de data online wordt opgeslagen is de vraag in welk land dat gebeurt. De Europese Unie biedt de eindgebruiker in theorie een betere privacybescherming dan de Verenigde Staten[69].

VOORBEELD:

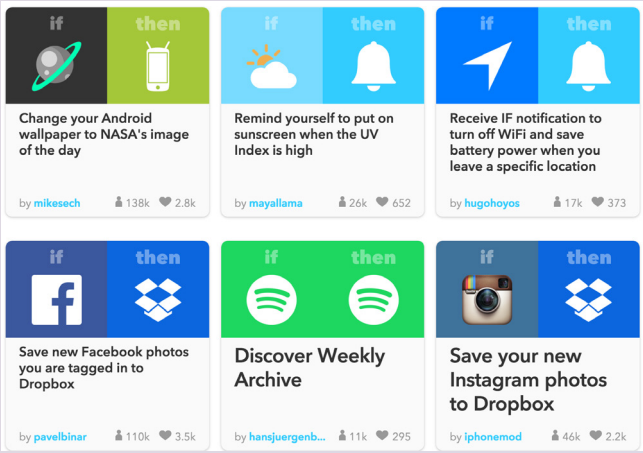
Citizen Ex project van James Bridle
Het Citizen Ex project toont je waar de websites die je gebruikt eigenlijk fysiek staan. Het kunstproject genereert een nieuwe vlag, waarin de vlaggen van alle landen waarin je data worden opgeslagen, worden vermengd. Het zal je niet verbazen dat de servers van veel populaire diensten in de Verenigde Staten staan.

veel meer rekening moeten houden met bestaande, ingesleten, culturele patronen. Een slimme fiets zou in de Nederlandse cultuur bijvoorbeeld ander ‘gedrag’ moeten vertonen dan in de Amerikaanse cultuur.

→Lucy Suchman, p.139

Wanneer slimme producten en diensten goed aan te passen zijn, kunnen de eindgebruikers dit 'laatste stukje' zelf oppakken.

Er lijken allerlei veelbelovende nieuwe interfaces te ontstaan die hiermee spelen. Een mooi voorbeeld is ‘If This Then That’, een website waarop mensen diensten kunnen koppelen op een manier die op een sterk versimpelde vorm van programmeren lijkt[83]. In een wereld waarin bijna alles in onze omgeving een technologische component heeft, is het helemaal niet zo’n gek idee om iedereen een klein beetje te leren programmeren, zodat iedereen op zijn minst de werkwijze van deze apparaten leert kennen.



Voorbeelden van recepten op ifffttt.com

In een wereld die is doordrenkt met genetwerkte technologie worden ontwerpers uitgedaagd deze educatieve rol op te pakken. In plaats van afgeronde producten te maken die ‘vanzelf’ werken, zouden we lego-achtige interfaces moeten ontwikkelen[84]. Dat zou de gebruiker op een toegankelijke manier controle geven over het gedrag dat deze creaties kunnen vertonen. Met name het complexe gedrag dat tussen systemen kan ontstaan is anders moeilijk inzichtelijk en controleerbaar te maken.

In het meest ideale geval ontstaat er een maatschappij waarin mensen naar technologie kijken zoals ze nu naar koken kijken. Het is namelijk best raar dat we allemaal een fascinatie hebben voor koken, want in theorie is koken een ‘opgelost probleem’ Sinds de ontwikkeling van de magnetron en de kant-en-klaar maaltijd hoef je in principe nooit meer zelf te koken en zou je kunnen vertrouwen op de koks van die maaltijden en de markt waarin dit eten ontstaat.

De praktijk is echter anders. De meeste mensen eten liever zelf bereid voedsel, en kijken neer op magnetronmaaltijden. We koken juist heel graag zelf, we vinden het leuk en interessant. We ontwikkelen onze eigen recepten en passen gerechten naar eigen smaak aan. Wie voedsel kan ‘programmeren’ (koken), wordt zelfs sexy gevonden.

Net zoals je een traditionele interface zou willen aanpassen aan de cultuur van de gebruiker (grotere knoppen voor ouderen bijvoorbeeld), zou je het gedrag van de slimme omgeving ook willen kunnen aanpassen aan de lokale situatie. Dat kan eigenlijk niet zonder de hulp van de gebruiker. Maar die moet dan wel het lef en de kennis hebben om dat te doen. Gebruiksgemak en eenvoud zijn mooi, maar we zouden gebruikers ook altijd moeten uitdagen om meer te blijven leren en meer te ontdekken over wat er kan, om hem zo tot mede-ontwerper van zijn of

Privacy productanalyse

Privacylabel

EFFICIËNT

MINDER EFFICIËNT

NIET EFFICIËNT

Product Xiaomi Mi Band

PRINCIPE 1 Het is lastig in te schatten hoe goed Xiaomi van tevoren heeft nagedacht over privacyvraagstukken. De reputatie is niet al te goed[93]. En ook de onderstaande punten doen vermoeden dat privacy en veiligheid niet genoeg aandacht hebben gekregen.

PRINCIPE 2 Over creatief misbruik lijkt niet goed nagedacht, getuige de slechte beveiliging. Wel is het goed om te beseffen dat Europese en Chinese normen en waarden nogal verschillen. Wat wij als ongewenste surveillance kunnen zien, zien zij als geoorloofde controle.

PRINCIPE 3 De armband verzamelt non-stop data, en dat is ook nodig voor de beloofde functionaliteit. Dat is in ieder geval helder. Ze meet ook maar één ding, beweging, dus ook dat is niet zo complex. Xiaomi lijkt de data echter in zijn geheel door te sturen naar haar servers, en niet slechts een samenvatting, wat in theorie meer dan voldoende zou zijn[94].

PRINCIPE 4 De data worden niet versleuteld opgeslagen op het apparaat of op de smartphone[95]. Er zijn door hobbyisten stukjes software ontwikkeld waarmee de

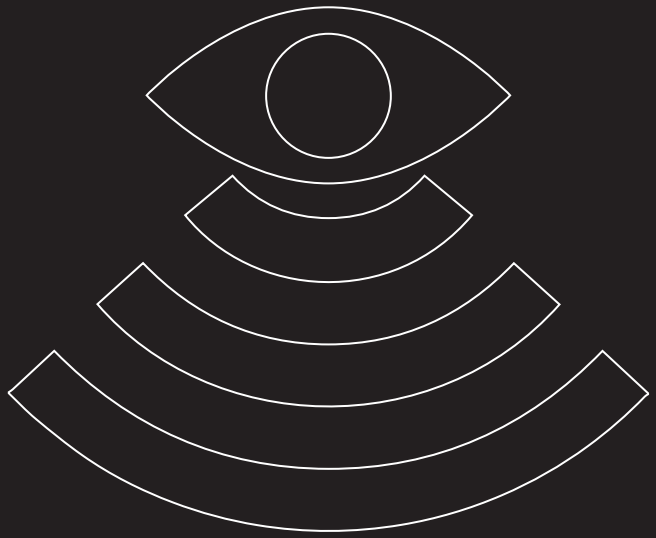
data van de telefoon te halen zijn. Hopelijk worden de data op de server wel versleuteld opgeslagen, maar dan nóg zou dat alleen dieven weerhouden. De Chinese overheid regelt gewoon toegang tot de data. Dit kan omdat Xiaomi de encryptiesleutel zou hebben en die dan zou delen. De overheid kan kortom achterhalen hoe je dagelijkse leefritme eruitziet. Een positieve noot: de connectie met de webserver wordt wel beveiligd opgezet.

PRINCIPE 5 De app dwingt de gebruiker tot het aanmaken van een online account, maar er is geen dwang om een echte naam te gebruiken[96]. Bovendien is het überhaupt jammer dat een identiteit en communicatie met een server nodig zijn. De armband zou bij anoniem gebruik dezelfde inzichten kunnen bieden.

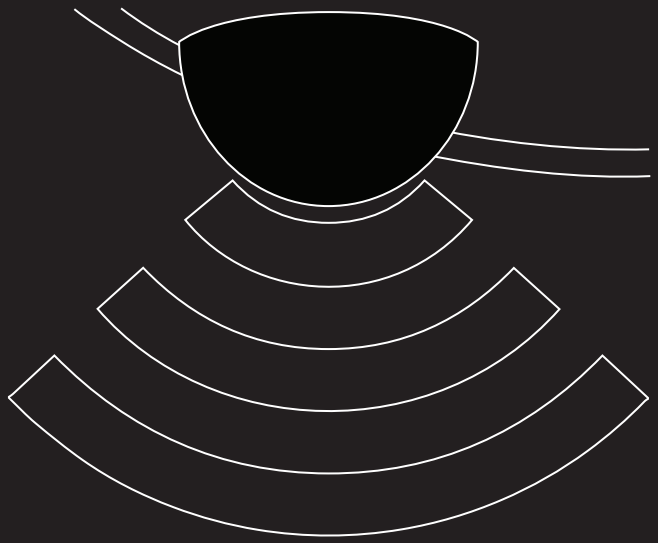
PRINCIPE 6 Het is niet duidelijk hoe de algoritmes hun werk precies doen[97]. Wat is volgens Xiaomi 'diepe slaap'? Zou de werking van een algoritme in de handleiding opgenomen kunnen worden? Hoe communiceer je de verborgen voorkeuren van een algoritme naar de gebruiker toe? Dit zijn onbeantwoorde design vragen.

PRINCIPE 7 Je data wordt naar de webservers van Xiaomi verzonden. Er wordt je geen keus geboden.

PRINCIPE 8 De prescriptieve mogelijkheden van de Mi-Band lijken beperkt doordat het apparaat niet eenvoudig te koppelen is aan andere diensten. Hoe de algoritmes bepalen waar de grens tussen diepe slaap en lichte slaap ligt, is onduidelijk. Het apparaat maakt verder geen nota van de gezondheidstoestand.



WATCH
OUT
FOR



NOT
BEING
WATCHED