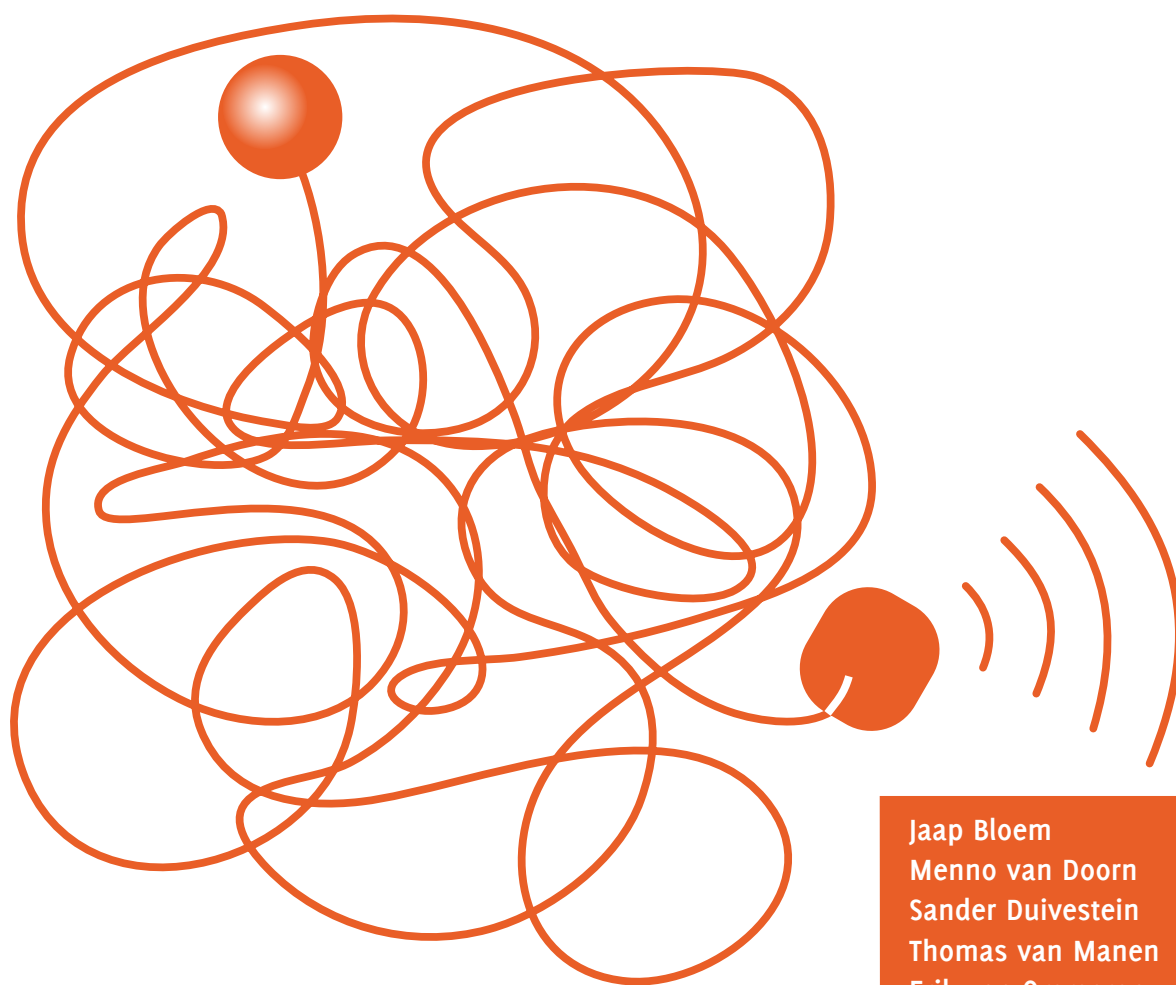


VINT-onderzoeksnotitie ① van 4
VINT-onderzoeksnotitie ② van 4
VINT-onderzoeksnotitie ③ van 4
VINT-onderzoeksnotitie ④ van 4

Privacy, technologie en de wet

Big Data voor iedereen door goed design



Jaap Bloem
Menno van Doorn
Sander Duivestijn
Thomas van Manen
Erik van Ommeren



SOGETI

VINT | Vision • Inspiration • Navigation • Trends

vint.sogeti.com/bigdata

vint@sogeti.nl

Inhoud

De Big Data-onderzoeksnotities van VINT	3
Inleiding	
<i>Vruchten plukken van Big Data</i>	4
1 Een anatomie van Big Data-angst	9
2 Wat is privacy?	21
3 Privacy by Design en de balans tussen PIT's en PET's <i>(Privacy-Invasive versus Privacy-Enhancing Technologies)</i>	36
4 Regelgeving in beweging	45
Conclusie	53
Literatuur en afbeeldingen	56
Over Sogeti	63
Over VINT	63
Privacy prima, en wat nu ...?	63, 64



Naamsvermelding-NietCommercieel-GelijkDelen 3.0

(CC BY-NC-SA 3.0)



De Big Data-onderzoeksnotities van VINT

Sinds 2005, toen het begrip Big Data werd gelanceerd – opmerkelijk genoeg vanuit O’Reilly Media, dat een jaar eerder met Web 2.0 was gekomen – is het onderwerp steeds actueler geworden. Qua technologieontwikkeling en businessadoptie is het Big Data-veld sterk in beweging, en dat is een understatement.

In *Helderheid creëren met Big Data*, onze eerste van in totaal vier onderzoeksnotities, geven we antwoord op de vraag wat het eigenlijk is, waarin het verschilt van bestaande dataduiding en hoe de transformatieve potentie van Big Data wordt ingeschat.

De concrete adoptie en plannen in organisaties raken momenteel vooral het thema van onze tweede notitie *Big Social*: de klantkant kortom, met name geïnspireerd door de sociale netwerkactiviteit van Web 2.0.

De dataexplosie vindt overal om ons heen plaats, maar een belangrijk deel van de discussie betreft de vraag hoezeer organisaties zich in Big Data moeten storten. Het antwoord luidt: met beleid. Beleid van buitenaf en binnenuit raakt de kern van het privacythema, dat uitgebreid in deze derde onderzoeksnotitie aan bod komt.

Wie het in de digitale context over privacy heeft, impliceert in dezelfde adem de bescherming van persoonlijke gegevens (*data protection, Datenschutz, informatique et libertés*) en omgekeerd. We kunnen nog zoveel data willen beschermen, vaak is het misschien het handigst om ze maar gewoon te wissen. De DeleteMe-app van Abine kan worden opgevat als een implementatie van *The Right to Be Forgotten*, dat onder meer de Europese Unie voor onze digitale wereld propageert.

De verschillen in regio’s en landen overal ter wereld zijn nog groot, maar harmonisatie en uniformering van wet- en regelgeving worden steeds meer nagestreefd. Desondanks blijven de uitdagingen legio en ontwikkelt de technologie zich voorspoedig, met name op het gebied van Big Data-verwerking en analyse – zie de VINT-notities 1 en 2.

Van bovenaf (vanuit wet- en regelgeving) en van onderop (vanuit de procedures en de technologie) is men momenteel bezig om inzake digitale privacy toe te werken naar één convergerende *Privacy by Design*-oplossing. Het is de bedoeling om met zo min mogelijk spelregels en gesteund door de technologie die de verandering drijft, onze informatiemaatschappij sociaal en econo-



misch een fundament te geven dat de individuele waarden en waardigheid die we koesteren respecteert.

Met vier Big Data-notities beoogt VINT helderheid te scheppen door ervaringen en visies in perspectief te presenteren: onafhankelijk en aangekleed met voorbeelden. Lang niet alle antwoorden zullen kunnen worden gegeven en er zullen zelfs meer vragen bij u opkomen.

Bijvoorbeeld over de strategische keuzes die u wilt maken. Voor dat onderwerp hebben we onze vierde Big Data-notitie gereserveerd. Vragen zijn er ook over hoe u uw organisatie misschien moet herinrichten. Maar om te beginnen gaan we in deze notitie in op de privacy-issues die Big Data-analyse oproept.

Graag blijven we met u in gesprek over de nieuwe datafocus: online op <http://vint.sogeti.com/bigdata> en natuurlijk in persoonlijke gesprekken. Door actief deel te nemen aan de discussie helpt u uzelf en ons om de gedachten ten aanzien van Big Data aan te scherpen en door voortschrijdend inzicht te komen tot heldere en verantwoorde beslissingen.

Ter inspiratie treft u in deze notitie weer zeven vragen aan waarover we graag uw mening vernemen. In de pdf van dit document kunt u op de betreffende buttons klikken. U wordt dan direct naar de discussie in kwestie geleid. Het antwoord op de hamvraag 'Privacy prima, en wat nu ...?' treft u aan op pagina 63 en 64, de achterzijde van deze Big Data-notitie.

Inleiding

Vruchten plukken van Big Data

Voorspellen en targeten als Grote Truc	4
Transparantie, keuze en Privacy by Design	5
Big Data-gewin voor iedereen	6
Big Data moet privacyvriendelijker	7
De economie van persoonlijke informatie	8

Voorspellen en targeten als Grote Truc

Data is de brandstof van de digitale economie. Wat er tegenwoordig allemaal mogelijk is, kan heel handig en nuttig zijn, maar ook bedreigend, althans ongewenst. De intelligentie van een smartphone komt in de supermarkt goed van pas om te bepalen wat we moeten kopen om 's avonds te kunnen eten, gegeven onze dieet- en smaakwensen. Dat is natuurlijk prachtig, vooropgesteld dat de verzameling en combinatie van data

transparant en discreet wordt afgehandeld. Op die manier is snel digitaal advies op basis van voorkeuren vaak bijzonder welkom. In de retail is Amazon hier ooit mee begonnen, om klanten zo goed mogelijk tevreden te kunnen stellen en houden. De organisatie kent de klant en niemand hoeft zich ooit bekocht te voelen.

Maar in het geval van de Amerikaanse Target-keten – à propos *targeting* – kon men na slimme analyse van koopgedrag onder meer voorspellen wie er zwanger was en ook wanneer de bevalling zou plaatsvinden. Target was niet transparant naar de klant over dit soort praktijken en zo gebeurde het dat de vader van een tienermeisje onaangenaam verrast was door de aanbiedingen van Target aan zijn dochter. Target had het bij het rechte eind, het meisje was inderdaad zoveel weken zwanger, maar in de pers kwam er een flinke discussie op gang over wat organisaties allemaal van ons weten en hoe ze hun Big Data-kennis gebruiken om vooral maar zoveel mogelijk aan ons te kunnen slijten.

Goed getarget en midden in de roos is mooi, maar wat er allemaal van ons bekend is en hoe daar gebruik van wordt gemaakt, dat wordt ons lang niet altijd verteld. Dit soort transparantie is al decennialang een cruciaal onderdeel van de zogeheten *Fair Information Practice Principles* (FIP's, *Data Protection Principles* in Europa), maar er wordt dus nog wel eens de hand mee gelicht. U kent het Target-voorbeeld uit onze vorige onderzoeksnotitie *Big Social* en sommigen zullen ook dit weinig problematisch vinden, maar wat als uw krediet-, hypotheek- of verzekeringsaanvraag wordt afgewezen, omdat de data uitwijzen dat uw financiële situatie en/of uw gezondheid een onaanvaardbaar risico voor de verstrekker opleveren? Om welke informatie gaat het? Waar komt die vandaan? Hoe is die verzameld? Kunt u de gegevens zelf inzien? Kunt u ze wijzigen? Dat soort simpele en fundamentele vragen zijn in het tijdperk van digitale informatie al decennialang een heikel issue. Over de soms kafkaëske voorbeelden van mensen wier situatie ten onrechte in een slecht daglicht kwam te staan, zijn boeken volgeschreven en is er veel jurisprudentie.

Beter kunnen voorspellen en selecteren is in zijn algemeenheid de grote winst die met Big Data geboekt kan worden. Voor organisaties liggen de kansen voor het oprapen: fraudedetectie, efficiëntere energievoorziening, aanbiedingen op maat, epidemieën van tevoren zien aankomen, ga zo maar door. Iedereen profiteert, zou je denken, maar welke gegevens worden er en passant allemaal verzameld door digitale volgsystemen en wat gebeurt ermee? Hebben we daar nog wel zicht op en controle over? De onwetende consument en burger ervaart het vaak als één Grote Truc. Hij voelt zich aangetast in zijn privacy en wordt dat daadwerkelijk ook. Deze derde Big Data-onderzoeksnotitie, *Privacy, technologie en de wet*, gaat over die confrontatie.

Transparantie, keuze en Privacy by Design

Waar komen we dan op uit? In eerste instantie dat elke organisatie die zich met Big Data bezighoudt, van de hoed en de rand moet weten inzake privacy en databescher-

ming. Dit is zeker nog niet overal geland. Zijn we transparant en open over waar we mee bezig zijn, krijgen klanten een heldere keus om informatie te verstrekken of niet, en implementeren we het *Privacy by Design*-principe, dan zijn daarmee de belangrijkste drie stappen gezet. Langs die lijnen wil deze notitie bijdragen aan een fundamenteel privacybewustzijn dat de businesspraktijk vormgeeft als een informatiesituatie met open vizier voor zowel klant als leverancier.

Eén ding staat als een paal boven water: wie op zoek gaat naar de aan- en uitknop voor privacy, kan lang zoeken. Het is veel belangrijker de juiste richting te kiezen, om zo over de volle breedte te kunnen profiteren van Big Data. Waar we op moeten koersen is 'Big Data-gewin voor iedereen'. Dat kan het beste door de privacy-issues te onderkennen, ze in detail bloot te leggen en in alle openheid in geaccepteerde banen te leiden.

Big Data-gewin voor iedereen

Krachtiger dan Meglena Kuneva heeft niemand het ooit gezegd: 'persoonlijke informatie is de nieuwe olie van het internet en de nieuwe munteenheid van de digitale wereld'. Mevrouw Kuneva zei het als eurocommissaris voor consumentenbescherming in haar keynotespeech op een rondetafelbijeenkomst over online datacollectie, targeting en profiling, eind maart 2009 in Brussel. Maar in zijn algemeenheid gaat het om digitale data, zowel online als offline.

Kuneva schetst de situatie als volgt: 'de explosie in het volume van alle verzamelde persoonlijke gegevens bij elkaar en het gebruik daarvan voor commerciële doeleinden is een van de meest belangrijke en meest controversiële issues in de snel veranderende wereld van digitale communicatie'.

Explosie, volume, snelheid, economische waarde en uiteenlopende soorten digitale persoonlijke informatie: welkom in het Big Data-tijdperk. Daarmee dekt digitale privacy een op een de notie van Big Data, die we definiëren als combinatie van *Volume*, *Variety* en *Velocity*, door sommigen aangevuld met *Veracity* en *Value*. Dat is belangrijk en controversieel: een zegen voor de dienstverlening aan klanten, maar met de nodige uitdagingen.

'Internet', aldus Meglena Kuneva in 2009, 'en de nieuwe generatie van digitale communicatie en digitale platformen bieden enorme mogelijkheden voor consumenten. In termen van keuze, toegang en gelegenheid behoren ze tot de meest empowerende tools die consumenten ooit hebben gehad. [...] We willen natuurlijk dat deze nieuwe kansen zich blijven doorontwikkelen en daarom moeten we het vertrouwen stimuleren dat mensen zal aanzetten tot participatie.' Kuneva benadrukt dat 'internet grotendeels een advertentiegedreven dienst is en dat de ontwikkeling van marketing op basis van profielen en persoonlijke data de zaak draaiende houdt'.

Daar plaatst ze de volgende kanttekening bij: 'Ruim 80 procent van de jonge internetgebruikers denkt dat allerlei persoonlijke gegevens op de een of andere manier worden gebruikt en gedeeld zonder hun toestemming en dat is ook zo.' Als oplossing, met het oog op privacybescherming, vindt Kuneva het hard nodig om meer transparant te zijn over de verzameling van data. 'Consumenten moeten weten dat hun gegevens worden verhandeld en moeten de mogelijkheid hebben om daar zelf controle over uit te oefenen.'

Het zijn geen nieuwe geluiden. Al een paar decennia weten we dat het privacylandschap sterk in ontwikkeling is dankzij de toenemende digitalisering. In de inleiding van het boek *Technology and Privacy: The New Landscape* uit 1997 staat het zo:

[Digitale] privacy is het vermogen om sociaal-economische relaties uit te onderhandelen op basis van controle over de eigen persoonlijke informatie. In toenemende mate geven regelgeving, beleid en technologie de relaties vorm die individuen hebben met organisaties en overheden.

Nationaal en supranationaal zijn er grote verschillen in privacyregelgeving, maar over één ding is iedereen het eens, namelijk het geweldige potentieel van de digitale economie. Het is van groot belang om databescherming en businessbelangen goed met elkaar te verenigen en hun relaties coherent vast te leggen in de verschillende wetssystemen.

Big Data moet privacyvriendelijker

Big Data is niet privacyvriendelijk. Brendon Lynch, Chief Privacy Officer van Microsoft, benadrukte het nog eens in november 2012 op het European Data Protection Congress van de International Association of Privacy Professionals (IAPP). Zelfs wanneer er is geanonimiseerd, bepaalde kerngegevens zijn verwijderd of de data zijn 'gescrambled', is het op basis van de verbanden in verschillende Big Data-verzamelingen – online en offline – toch goed mogelijk om specifieke informatie hard te koppelen aan een individu, computer of ander persoonlijk device.

Om deze *linkability* en (her)identificatie tegen te gaan heeft Microsoft nu na jaren van ontwikkeling een technologische Privacy by Design-oplossing operationeel die de kwaliteit van digitale data voor targeting door organisaties garandeert, terwijl afzonderlijke personen met zekerheid niet meer traceerbaar zijn. In Big Data-kringen staat de methode bekend als *Differential Privacy*.

Om kennisgeving en instemming (notice & consent), twee belangrijke privacyprincipes, had bijvoorbeeld Target zich niet bekommerd maar, zo vraagt Brendon Lynch zich af: hoe kun je nu in een Big Data-wereld verwachten dat alles wat er gebeurt in detail wordt gemeld en dat daar concreet toestemming voor wordt gevraagd? Net

zoals de financiële wereld flitstransacties kent, staat onze Big Data-wereld bol van de flitsinformatie.



PbD-vraag 1

Heeft u wel eens te maken gehad met privacy-issues? Een Privacy by Design-aanpak (PbD) is nadrukkelijk bedoeld om dat te voorkomen.

<http://bit.ly/vintR3Q1>

De economie van persoonlijke informatie

Het zogeheten ecosysteem van persoonlijke informatie staat beschreven in het rapport *Protecting Consumer Privacy in an Era of Rapid Change* uit maart 2012 van de Amerikaanse Federal Trade Commission. Dit document bevat uitvoerige aanbevelingen voor organisaties en beleidsmakers langs achtereenvolgens de lijnen van Privacy by Design, simpele keuzemogelijkheden voor consumenten en transparantie. Centraal in het economische systeem staat het individu, en over ons allemaal worden de meest uiteenlopende gegevens verzameld. Dat gebeurt onder andere door media, overheidsinstellingen, energieleveranciers, luchtvaartmaatschappijen, kredietorganisaties, de retailsector, telecombedrijven, kabelmaatschappijen, verzekeraars, banken, ziekenhuizen, artsen, apotheken, zoekmachines, commerciële websites en sociale netwerken. Informatiemakelaars, waaronder kredietbureaus en de advertentie-industrie, gebruiken en combineren deze gegevens, en zo komen ze terecht bij bijvoorbeeld banken, marketeers, media, overheden, juridische organisaties, individuen, wetshandhavers en werkgevers. Het gaat hier om online en offline data, afkomstig van individuen, hun computers of andere devices. De aanbevelingen in het FTC-rapport zijn alleen dan niet van toepassing wanneer een organisatie alleen maar privacyneutrale informatie verzamelt van minder dan vijfduizend mensen per jaar en die op geen enkele manier deelt met derden.

Het mag misschien een wiskundige limiet blijven, maar met de groeiende roep om Privacy by Design zullen transparantie, openheid, kennisgeving, instemming en met name de individuele controle over de eigen verzamelde informatie inzake opslag, verwerking, combinatie en verspreiding steeds concreter vorm krijgen. Organisaties moeten zich daarvan bewust zijn en moeten erop voorbereid zijn. Dat betekent: fundamentele kennis opbouwen en uw operatie ernaar inrichten. Met deze notitie hopen we daaraan bij te dragen.

1 Een anatomie van Big Data-angst

1.1	Digitale ongrijpbaarheid voedt onze angst	9
1.2	Internet en privacy gaan slecht samen	12
1.3	Gegronde verontrusting	14
1.4	Fear, Uncertainty & Doubt	15
1.5	Privacy by Design als oplossingsrichting	16
1.6	Ons landschap van technologie en privacy in vogelvlucht	18

1.1 Digitale ongrijpbaarheid voedt onze angst

Wat millennia lang fysiek bezit en eigendom was – het mijn, dijn, privéterrein en gedrag waar niemand iets (mee) te maken had dan op uitnodiging van de persoon in kwestie – dat is de afgelopen decennia opgeschoven naar digitale informatie. Naar allerlei persoonlijke gegevens in databases en onze dagelijkse handel en wandel op computers en online. Kortom, naar onze digitale *Personally Identifiable Information* (PII), waarvan het eigendom, de toegang, de verzameling, de opslag, het gebruik en de verspreiding in Nederland momenteel worden geregeld door met name de Wet bescherming persoonsgegevens (Wbp).

Hoe meer digitale gegevens er in soorten en maten in omloop komen, des te groter wordt de angst dat er linksom of rechtsom op basis van die data veel meer van ons bekend is dan we eigenlijk zouden willen. Dat loopt uiteen van videobeelden, locatie en sociale media tot aan de inhoud van databases, zoek- en koopgedrag op internet en de data die slimme energiemeters tegenwoordig kunnen verzamelen. Met name de mogelijke koppeling van deze en andere gegevens, dus het daadwerkelijke Big Data-gebruik in al zijn facetten, is nog te weinig transparant en de beveiliging van de informatie lijkt niet altijd goed te zijn geregeld.

Dit blijkt wel uit de verhalen van hackers en cybercriminelen die steeds weer in allerlei digitale systemen weten door te dringen. Om vervolgens bankrekeningen te plunderen, de informatie door te verkopen of gewoon online te zetten, zodat iedereen erbij kan. Hoe de digitale wapenwedloop tussen aanvallers en verdedigers zich ontwikkelt, onttrekt zich grotendeels aan onze waarneming. Ook dat baart zorgen, en bij gebrek aan feiten, deugdelijke risico-inschatting en gegeven de beveiligingslekken die zich voordoen, voedt dit angst en speculatie.

Wat privacy betreft heeft fysiek dus grotendeels plaatsgemaakt voor digitaal. We kunnen nog zo onherkenbaar diep in de jas duiken, onze digitale sporen vertellen vele malen meer en ze zijn voor wie dat wil relatief eenvoudig te bemachtigen. Dat is de toestand van vandaag, althans de gepercipieerde, en zowel de verschillende feitelijke situaties als de beleving zijn voor verheldering en verbetering vatbaar. Een voorbeeld ...

Eind november 2012 besteedde het tv-programma *De Wereld Draait Door* aandacht aan het Elektronisch PatiëntenDossier (EPD). Dat kreeg na eerder verzet in 2013 een doorstart als opt-in-regeling onder de naam Persoonlijk GezondheidsDossier: mensen moeten hun toestemming geven om in het register te worden opgenomen.

Wilna Wind, directeur van de Nederlandse Patiënten Consumenten Federatie, en internetexpert Alexander Klöpping zitten tegenover elkaar. Wind is fervent voorstander van het EPD, Klöpping is tegen en jaagt het publiek schrik aan vanuit zijn banden met de hackerscene. Aan het einde van de discussie vraagt gastheer Matthijs van Nieuwkerk aan de zaal wie er gaat meedoen aan het EPD. Niemand steekt zijn hand op. Ondanks de nieuwe opt-in-regeling zit de angst er kennelijk goed in, niet in de laatste plaats omdat mevrouw Wind bij herhaling te kennen geeft dat de beveiliging van het EPD binnen 6 weken van een schoolcijfer 4 (onvoldoende) naar een 8 (goed) zal zijn getild, terwijl de discussie al jaren loopt.

Wat moeten we hiervan zeggen? Heeft Klöpping gelijk? Kennelijk nemen we liever het risico niet. Om te beginnen moeten zwakke plekken in onze privacy- en databescherming altijd zo goed mogelijk worden gerepareerd vanuit de combinatie van technologie, procedures en regelgeving. We moeten toe naar een structureel Privacy by Design, zoals dat heet: privacy- en databescherming die met diensten en praktijken mee ontworpen is. Zo'n type aanpak is het beste uit te leggen, biedt de meeste zekerheid en geeft het meeste vertrouwen.

Toepassingsgebieden voor de Privacy by Design-benadering zijn momenteel met name de volgende zogeheten potentieel *Privacy-Invasive Technologies* (PIT's). Natuurlijk komen ook de gezondheidszorg en Big Data Analytics in het lijstje voor:

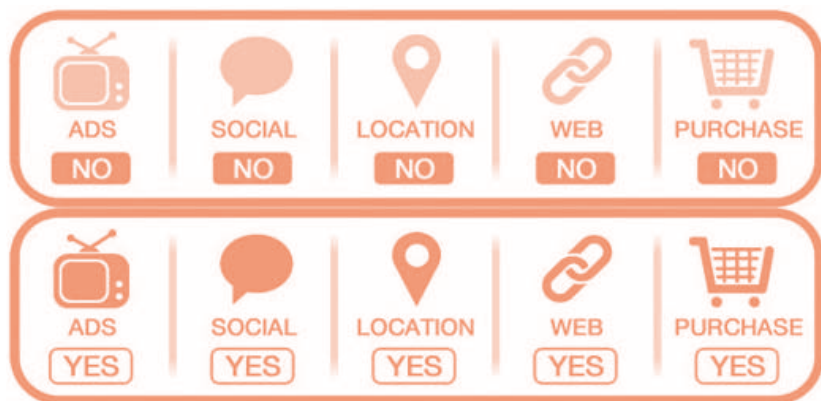
1. Camerabewaking
2. Biometrische herkenning
3. Smart Meters en het Smart Grid
4. Mobiele devices en communicatie
5. Near Field Communications (NFC)
6. RFID en sensors
7. Redesigning IP Geolocation Data
8. Remote Home Health Care
9. Big Data en Data Analytics

<http://www.privacybydesign.ca>

Het is dat trio van uitleg, zekerheid en vertrouwen waarmee we, samen met verantwoordelijk gedrag van organisaties en individuen, het hoofd moeten bieden aan gegronde en zeker ook aan irrationele angst voor privacyverlies. Als voor iedereen duidelijk is hoe de vork in de steel zit en wat de ontwikkelingen zullen zijn, dan kan

op die basis steeds de afweging worden gemaakt voor een uitruil van persoonlijke gegevens met het oog op een betere individuele dienstverlening.

Feiten en de perceptie rondom privacy kunnen we via keurmerken en bijsluiters goed communiceren en adresseren, liefst in één oogopslag. Daartoe heeft onder meer de Amerikaanse Association for Competitive Technology in 2012 de volgende set pictogrammen gemaakt. Ze geven aan wat er wel en niet gebeurt met onze persoonsgegevens in de mobiele apps die we downloaden op onze smartphones en tablets.



In Amerika werkt de AppRights-beweging aan een initiatiefwet, *The Application Privacy, Protection, and Security (APPS) Act of 2013*, die de verzameling van data via mobiele devices en apps moet regelen.



Dit zien we nu steeds meer. Onder meer Mozilla bedient zich van pictogrammen, bijvoorbeeld om aan te geven of een website gegevens deelt, verkoopt of zonder gerechtelijk bevel aan de overheid doorspeelt en hoe lang gegevens worden bewaard.



1.2 Internet en privacy gaan slecht samen

Uit een enquête in 1997 onder de Amerikaanse bevolking – ongeveer een kwart van de Amerikanen had toen internet – blijkt dat men ook toen al flink bezorgd was over privacy op internet. In het *Framework for Global Electronic Commerce* van de regering-Clinton uit datzelfde jaar staat dit aldus verwoord:

Americans [and all other people] treasure privacy, linking it to our concept of personal freedom and well-being. Unfortunately, the GII's [Global Information Infrastructure] great promise – that it facilitates the collection, re-use, and instantaneous transmission of information – can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.

Het internet mag geen vrijplaats zijn voor ongewenst en ongeoorloofd gedrag, want dan blijft de economische potentie onder de maat, zo was de redenatie. Vertrouwen ontbreekt dan, klanten en aanbieders blijven weg en de vrije wereldmarkt ontwikkelt zich niet naar vermogen.

De sociale en economische potentie van internet als alledaags onderdeel van ons leven willen we graag laten floreren. Maar vanwege de openheid en snelheid van internetverkeer is misbruik van toepassingen een groot inherent risico. Daarin moeten alle verschillende stakeholders hun verantwoordelijkheid nemen, idealiter de private sector voorop, want die heeft het grootste economische belang.

Als privacy beter is gegarandeerd, zullen veel meer individuen en organisaties op internet gaan en er actief worden, was in 1997 de gedachte. Maar ook tegen alle privacyzorgen in groeide internet als kool. Wat men zegt is dus niet altijd hetzelfde als wat men doet. Zouden straks de Nederlanders niet ook gewoon meedoen met het nieuwe EPD, tegen alle twijfel van vandaag in?

In hoeverre is de angst voor een EPD en andere Big Data-initiatieven reëel? Hoe makkelijk kunnen we van een beveiligings-4 een 8 maken? Misschien is dat best mogelijk en vaak reageren mensen vanuit een onderbuikgevoel op verandering.

Het antwoord op de vraag of de emotie inzake persoonlijke data zal wegebben of niet, vraagt om meer analyse. De Europese overheid vindt in elk geval in zijn algemeenheid dat de privacy online niet goed geregeld is:

Privacy op internet is niet goed beschermd. Dat vindt de Europese Commissie, die nieuwe regels heeft opgesteld. Het kan nog wel tot 2015 duren voordat de Europese regels echt van kracht worden. Maar daarop vooruitlopend wordt

het in Nederland dit jaar al een stuk strenger. Dat is nodig, want de huidige wet dateert uit 1995 en is sterk verouderd. De belangrijkste veranderingen zijn:

- *Consumenten moeten expliciet toestemming geven voor het gebruik van hun gegevens.*
- *Bedrijven moeten hun privacybeleid in duidelijke taal weergeven.*
- *Consumenten krijgen het zogeheten recht om vergeten te worden. Bedrijven die zich niet aan de regels houden, kunnen boetes krijgen die oplopen tot 2% van de omzet. Bij grote bedrijven kan het om tientallen of zelfs honderden miljoenen euro's gaan.*

RTL Z, 14 januari 2013

Voor de Nederlandse situatie kunnen organisaties onder andere op de website privacychecker.nl eenvoudig hun privacybeleid tegen het licht houden. U kunt er een antwoord krijgen op de volgende kwesties: moeten we een Privacy Impact Assessment doen (10 vragen; zie ook paragraaf 4.8), voldoen we aan de huidige Wbp (12 vragen), en hoe hoog zou vanaf 2015 de boete zijn onder de nieuwe beoogde EU-verordening (19 vragen)?

Privacy Impact Assessment



Moet u een Privacy Impact Assessment doen?

Doe hier de privacy quick scan! →

Wet bescherming persoonsgegevens



Voldoet u aan de Wet bescherming persoonsgegevens?

Doe hier de privacy compliance quick scan! →

Boetemeter



Benieuwd hoeveel boete u riskeert onder de nieuwe privacywetgeving?

Vul de privacy boetemeter in! →

Het is de bedoeling dat in 2015 de zogeheten *Algemene Data Protectie Verordening* EU-breed wordt aangenomen. Dat is niet langer een richtlijn voor nationale wetgeving, maar een Europese 'wet' die in Nederland in de plaats treedt van onze Wet bescherming persoonsgegevens. De nieuwe EU-verordening stelt nieuwe, strenge eisen aan organisaties die persoonsgegevens verwerken. De boete voor bedrijven kan oplopen tot 2 procent van de omzet.

1.3 Gegronde verontrusting

Wie zich waagt aan een anatomie van de angst voor Big Data, komt tot de slotsom dat er grond is voor verontrusting. De eerste grote Big Data-fabrieken, de kredietbureaus, hielden er in de vorige eeuw niet al te frisse praktijken op na. Ze negeerden de wet, fouten in de gegevens werden niet of nauwelijks gecorrigeerd, ze combineerden creatief allerlei databases om zoveel mogelijk persoonlijke informatie te vergaren en ze waren voortdurend verwickeld in rechtszaken en hoorzittingen vanwege hun werkwijze. In 2004 publiceerde Robert Ellis Smith een retrospectief hierover onder de titel *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*.

Amerikaanse kredietbureaus als Equifax, Experian en Trans Union voegden uit allerlei bestanden persoonlijke informatie van burgers samen, gekoppeld aan socialeverzekeringsnummers. Ze gebruikten die profielen en verkochten ze door. Deze kredietbureaus leverden informatie aan banken en overheden die moesten beslissen over een lening voor een auto, een levensverzekering of een uitkering. Ook verkochten ze de informatie door, aldus Robert Ellis Smith.

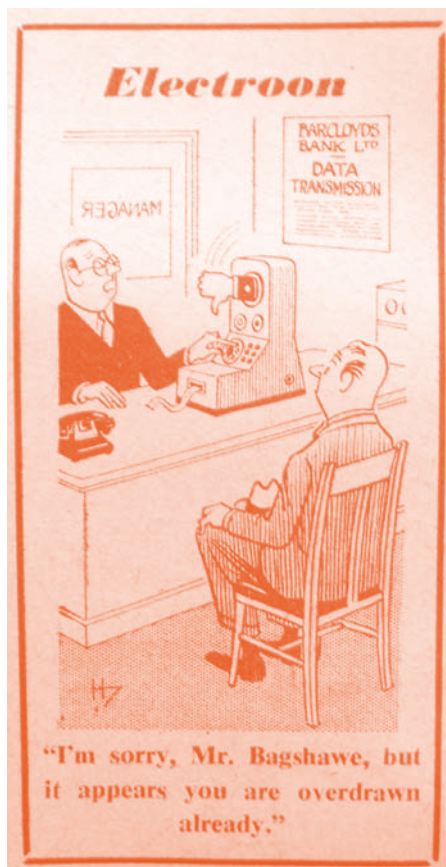
Een negatief kredietrapport kon je te gronde richten. Dat gebeurde met Keith en Phyllis Mirocha, die geen lening voor een nieuwe woning kregen terwijl er sprake was van een persoonsverwisseling. Door al het gedoe en het juridische gevecht dat ze aangingen met in dit geval Trans Union, verloren de echtelieden bovendien beiden hun baan.

De case van de Mirocha's bevat veel elementen die ook nu de Big Data-angst voeden:

- ◆ een ongelijke strijd: grote instituten versus de kleine man;
- ◆ informatie wordt zonder toestemming gebruikt;
- ◆ systemen beslissen zelf, zonder menselijke tussenkomst.

Zie dan je gelijk maar eens te halen. Ook nadat de fout in het dossier van de Mirocha's was opgespoord en Trans Union de gegevens zou aanpassen, kregen ze geen hypotheek. De foutieve informatie zat namelijk nog in het systeem en dat verhinderde de lening. Een zuur geval van de hilarische 'Computer Says No'-sketch uit de BBC-serie *Little Britain*. De cartoon hiernaast uit *Electronics Weekly* van 2 november 1960 laat zien dat deze situatie een lange historie heeft. Let op het Facebook-achtige thumbs-down-handje. Het lijkt wel een toespeling op het voornemen van de Duitse kredietbeoordelaar Schufa om ten behoeve van betere kredietprofielen persoonlijke informatie uit Twitter, Facebook en LinkedIn te koppelen aan hun 66 miljoen mensen tellende klantenbase.

Aan de drie angsten uit de tijd van de Mirocha's kunnen nog twee specifieke Big Data-gerelateerde ontwikkelingen worden toegevoegd:



- ♦ Digitale data schieten heel snel de wereld rond. Mogelijke privacy-inmenging van in het bijzonder Amerika stuit Europeanen tegen de borst.
- ♦ Persoonlijke informatie die mensen delen op sociale media dreigt tegen ons te worden gebruikt door overheidsinstanties, verzekeraars en andere organisaties.

Tot op de dag van vandaag is het 'Computer Says No'-syndroom een heet hangijzer. Dat blijkt bijvoorbeeld zonneklaar uit het eerste Issues Paper dat het South Australian Law Reform Institute van de Adelaide University Law School in mei 2012 publiceerde. De titel luidt namelijk: 'Computer says no: Modernisation of South Australian evidence law to deal with new technologies'.

Het verhaal van de Mirocha's is exemplarisch voor wat er op grote schaal aan de hand was bij Equifax. In een hoorzitting bleek dat medewerkers onder druk werden gezet om een bepaald quotum te halen van negatieve rapportages over consumenten. Dat leidde tot het creatief bij elkaar fantaseren van gegevens.

Op last van de rechter moest Equifax de richtlijnen voor juist gebruik van informatie onder de aandacht van de medewerkers brengen, maar die uitspraak werd jarenlang genegeerd. Hier ligt een belangrijke basis voor de angst dat de wet geen tanden heeft. Vertrouwen wordt op grove wijze geschonden en sentimenten als 'ze doen maar wat en niemand kan ze tegenhouden' vieren hoogtij.

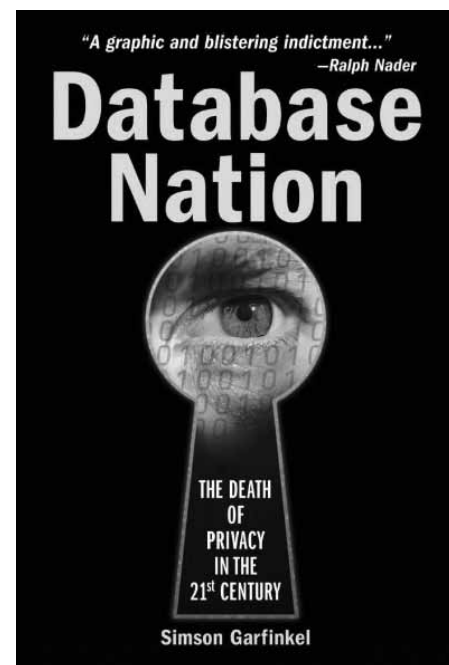
1.4 Fear, Uncertainty & Doubt

De angst voor de teloorgang van privacy door grootschalige toepassingen van technologie werd verder gevoed door de boeken en onderzoeken die de privacyschendingen of mogelijkheden daartoe aan de kaak stelden. Met name *The Naked Society* van Vance Packard uit 1964 bepaalde het sentiment, gevolgd door twee invloedrijke publicaties over Big Data avant la lettre van Alan Westin: *Privacy and Freedom* uit 1967 en *Databanks in a Free Society* uit 1972.

Uiteindelijk bracht *Database Nation: The End of Privacy in the 21st Century* uit 2001 van Simson Garfinkel het publiek helemaal ten einde raad. FUD, het bekende *Fear, Uncertainty & Doubt*, was definitief de norm geworden. Dat was gelijk de kritiek. Werd er echt niets aan dit soort praktijken gedaan? Inspelen op angst en feiten uit het verleden is voorstelbaar uit voorzorg, maar hoe zit het nu eigenlijk echt?

Vier angstlessen uit het vroege Big Data-tijdperk

1. Zonder druk van buitenaf veranderen organisaties hun gedrag niet makkelijk. Via publieke angst en agitatie kunnen correcties tot stand komen.
2. De echte angst betreft het onbedoelde gebruik van data door derden. Zeker als dat doelbewust gebeurt, zoals bij datahandel.





PbD-vraag 2
Is persoonlijke informatie in uw ICT-systemen automatisch veilig, zodat niemand zich daarom hoeft te bekommeren?

<http://bit.ly/vintR3Q2>

3. Uiteindelijk leidde de verontwaardiging over de praktijken van de Amerikaanse kredietbureaus in 1973 tot de *Code of Fair Information Practices*, gevolgd door de *Swedish Data Act*. Beide stoelen op vijf principes van goede omgang met persoonlijke informatie, te weten:
 - Er mogen geen geheime gegevensverzamelingen zijn.
 - Personen moeten kunnen nagaan wat er over hen verzameld is en hoe dat wordt gebruikt.
 - Gebruik van data voor andere doeleinden mag alleen nadat de persoon in kwestie toestemming heeft verleend.
 - Een persoon moet zijn Personally Identifiable Information (PII) kunnen corrigeren of amenderen.
 - Elke organisatie die PII creëert, beheert, gebruikt of verspreidt, moet de betrouwbaarheid van die data garanderen voor het beoogde gebruik en zorgen dat de informatie niet kan worden misbruikt.
4. Ook leren we uit de vroege Big Data-historie dat er kostbare tijd verstrijkt tussen de invoering van wetten en regels en het daadwerkelijk ernaar handelen. De angst lijkt dus gegrond dat partijen de kans hebben om nog een tijd lang de wet aan hun laars te lappen voordat ze zich beter gaan gedragen.

1.5 Privacy by Design als oplossingsrichting

Instituten lijken in eerste instantie minder oog te hebben voor persoonlijke veiligheid en privacy dan voor de business opportuniteiten en efficiencywinsten die nieuwe technologie biedt. Persoonlijke veiligheid is aanvankelijk niet ingebakken in het systeem, dat volgt later pas. Zo duurde het heel lang voordat creditcardmaatschappijen ter verificatie een sms-melding gaven bij een overboeking.

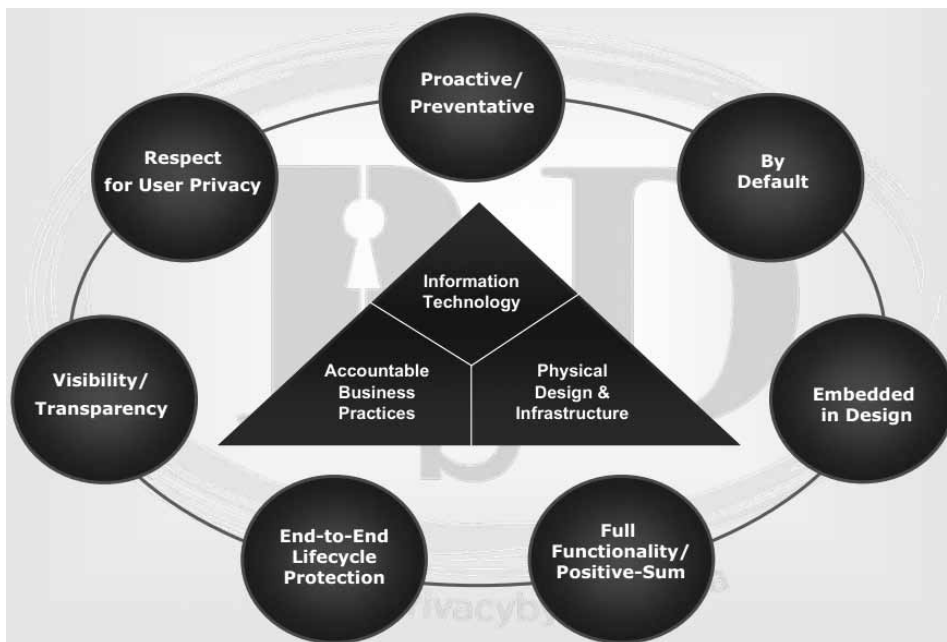
In *Unsafe at Any Speed* uit 1965 analyseert activist Ralph Nader, die ook het voorwoord schreef bij *Database Nation* uit 2001, de desinteresse van de auto-industrie op het punt van persoonlijke veiligheid. De ondertitel van het boek luidt *The Designed-in Dangers of the American Automobile*, maar onveiligheden en negatieve effecten moeten over de hele linie worden geneutraliseerd door tegenmaatregelen in te bouwen, aldus Nader:

A great problem of contemporary life is how to control the power of economic interests which ignore the harmful effects of their applied science and technology.

Veiligheid voor de bestuurder, de inzittenden en het milieu is nu allemaal onderdeel van het ontwerp en dus van de business. Privacy by Design, ook wel de Gouden Standaard genoemd, is zagezegd de autogordel, de kooiconstructie, de airbags en het roetfilter van de Big Data-business. Tegenwoordig zijn die dingen van meet af aan ingebouwd. Privacy by Design is bij uitstek de weg voorwaarts van technologie,

procedures en regelgeving gezamenlijk ontwerpen en inregelen met als doel optimale veiligheid en garanties. De schadelijke effecten en risico's van autorijden zijn niet helemaal weggenomen, maar wel sterk verminderd.

Zo zal ook de interesse van stakeholders in de 'veiligheid' van persoonlijke data blijven groeien. Veiligheid en zeggenschap moeten een integraal onderdeel zijn van het design van systemen en het ecosysteem waarin die functioneren. Daarmee neemt de winsituatie voor alle partijen toe en kunnen economische modellen en kansen floreren, zoals de regering-Clinton in haar *Framework for Global Electronic Commerce* al zei.



Omdat privacy, databescherming en persoonlijke informatie zo'n grote economische en relationele waarde vertegenwoordigen, stelt de Canadese Information and Privacy Commissioner Ann Cavoukian als 'moeder' van Privacy by Design deze zeven basisprincipes voor rondom de kern van elke organisatie, namelijk technologie, ontwerp en infrastructuur, en de operatie zelf:

1. Privacy by Design betekent dat u proactief en preventief te werk gaat: niet reactief, niet repareren achteraf.
2. Privacygarantie moet de defaultinstelling zijn.
3. Privacy moet ingebakken zijn in het ontwerp.
4. Ga voor volledige functionaliteit: geen magere trade-off maar een duidelijk positieve balans.
5. Oplossingen moeten helemaal dichtgetimmerd zijn: end-to-end security door de tijd heen.

6. Zorg voor zichtbaarheid en transparantie: openheid is uw leidmotief.
7. Ga respectvol om met privacy: stel dus vooral het individu centraal.

In de conclusie van deze notitie zijn deze principes verder geoperationaliseerd en in de Privacy by Design-vragen (PbD) in de kantlijn wordt u eraan herinnerd.

1.6 Ons landschap van technologie en privacy in vogelvlucht

Het boek *Technology and Privacy: The New Landscape*, dat ruim vijftien jaar geleden verscheen, bevat al een treffende definitie van digitale privacy. Ook de angst en de hoop daaromtrent wordt aangestipt, en als remedie vanuit convergerende invalshoeken wordt het concept van Privacy by Design al naar voren geschoven, zij het avant la lettre:

Privacy is the capacity to negotiate social relationships by controlling access to personal information. As laws, policies, and technological design increasingly structure people's relationships with social institutions, individual privacy faces new threats and new opportunities. [...]

The essays in this book provide a new conceptual framework for the analysis and debate of privacy policy and for the design and development of information systems. The authors are international experts in the technical, economic, and political aspects of privacy; the book's strength is its synthesis of the three.

We geven hier kort een toelichting op een aantal kernbegrippen (zie verder de literatuurlijst achterin):

Privacy-Enhancing Technologies

Technology and Privacy: The New Landscape bevat een hoofdstuk van Herbert Burkert, getiteld 'Privacy-Enhancing Technologies (PETS): Typology, Vision, Critique'. Momenteel leidt deze emeritus-hoogleraar het onderzoekscentrum voor informatierecht aan de universiteit van Sankt Gallen, Zwitserland.

Privacy-Invasive Technologies

Een jaar later, in 1998, stelde de Australische e-businessadviseur Roger Clarke de afkorting PIT's, Privacy-Invasive Technologies, tegenover PET's. Een actueel overzicht is te vinden op de PET-wiki van het Center for Internet and Society.

Dataveillance

De *Dataveillance* & *Information Privacy*-pagina's van Roger Clarke geven een interessant overzicht van PIT's, PET's en hun context. De term *dataveillance* is een vondst van Clarke. Hij besprak het concept in het tijdschrift *Commu-*

nications of the ACM van mei 1988 in het artikel 'Information Technology and Dataveillance'. Tegenwoordig kunt u behalve *surveillance* en *dataveillance* ook de termen *sousveillance* en *uberveillance* tegenkomen.

PET's en Privacy by Design

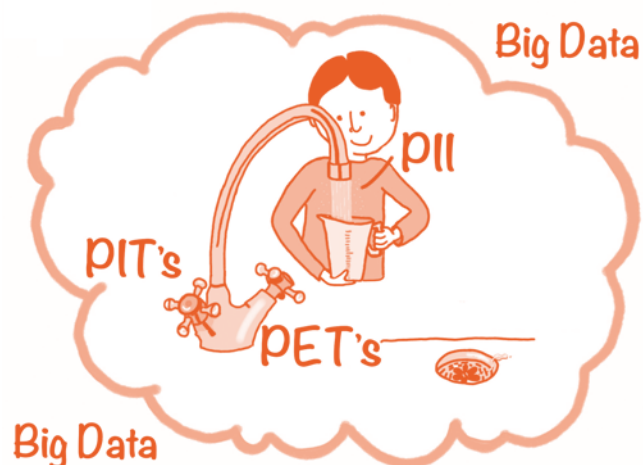
Recente literatuur over PET's en Privacy by Design:

- het *Handbook of Privacy and Privacy-Enhancing Technologies* uit 2003, gewijd aan intelligente software agents;
- *Privacy-Enhancing Technologies: A Review* van HP Laboratories uit 2011;
- *Privacy by Design in the Age of Big Data* van de Canadese Information and Privacy Commissioner Ann Cavoukian en IBM's Big Data-goeroe Jeff Jonas uit juni 2012;
- de brochure *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* uit december 2012 van Ann Cavoukian.

Privacy by Design en PET's zijn sterk in ontwikkeling

De relatie tussen Personally Identifiable Information (PII), PIT's, PET's en Privacy by Design is sterk in ontwikkeling. Een kritische kijk daarop geeft het artikel 'Regulating Privacy By Design' uit 2011 van Ira Rubinstein, onder meer Senior Fellow aan het Information Law Institute van het Center for Democracy and Technology. Rubinstein zet vraagtekens bij het enthousiasme waarmee Privacy by Design en PET's de afgelopen jaren wereldwijd zijn omarmd. Achter die concepten gaan namelijk werelden schuil en daar begint het werk pas, te midden van zich snel ontwikkelende technologieën en datastromen.

Onduidelijkheid over en fouten in de verzameling, de opslag, het gebruik en de verspreiding van persoonlijke informatie hebben de afgelopen decennia de digitale technologieën die dit mogelijk maken neergezet als Privacy-Invasive Technologies (PIT's). Op die ongevraagde koude douche hebben we simpel gezegd een mengkraan van regels gemonteerd. De privacy-inbreuken van de koude PIT's konden zo worden gedoseerd en door warm water in de vorm van PET's bij te mengen kunnen we nu in plaats van een koude douche zelfs een aangename temperatuur kiezen. De gereguleerde datastroom die we opvangen in een maatbeker staat voor onze Personally Identifiable Information (PII). Als daarvan te veel is afgetapt of ze ons toch te koud op het dak valt, dan weg ermee, de gootsteen in. Met als keuze: opnieuw of niet. Het PII-water dient om de economische relatie met allerlei dienstverleners te irrigeren.



Het is een treffende analogie en inderdaad: PII, PIT's, PET's en het bijbehorende Privacy by Design zijn samen de basis om te sleutelen aan privacygarantie. Het doel: privacy-inbreuk op basis van geavanceerde digitale technologie voorkomen.

PET's en Privacy by Design zijn een belangrijke aanvulling op de oorspronkelijke 'kraan' van Fair Information Practice Principles (FIP's), die niet expliciet affiniteit hebben met technologie. De ontwikkeling van het technologisch georiënteerde Privacy by Design, en daarmee van PET's in combinatie met transparantie over en keuzemogelijkheden binnen businesspraktijken en informatiesystemen, is een noodzakelijke Total (Personal) Data Management-aanpak. Alle denkbare stakeholders binnen en buiten organisaties moeten daar actief bij betrokken zijn en hun *Don't Be Evil*-verantwoordelijkheid nemen.

Daarom hamert onder meer Ann Cavoukian, de 'moeder' van Privacy by Design, zo op openheid en transparantie. PII voor iedereen in een gezonde economische context is het doel. Natuurlijk moeten in dit Big Data-tijdperk slimme technologische PET-oplossingen als Differential Privacy daar integraal deel van uitmaken. Net zoals aan de PIT-kant de ongebreidelde datastromen van onder meer slimme verbruiksmeters en biometrische systemen ongerustheid wekken. Alleen experts kunnen hier goed de effecten van inschatten, dus meer technologiekennis is overal gewenst.

Met het voortschrijden van de digitale technologie zullen optimale privacy en vertrouwen een wiskundige limiet blijven. De situatie wordt echter niet anders en dus moeten we daar concreet, kritisch en met een totaalaanpak aan verder werken. In dat verband stelt het rapport *Protecting Consumer Privacy in an Era of Rapid Change* uit maart 2012 van de Amerikaanse Federal Trade Commission het technologisch georiënteerde Privacy by Design voorop, in combinatie met simpele keuzemogelijkheden voor consumenten en transparantie. De traditionele privacy-aanpak blijft dus belangrijk, maar een technologische totaalfocus heeft nu de hoogste prioriteit.

2 Wat is privacy?

2.1	Een eerste schets	21
2.2	Privacy is een fundamenteel mensenrecht	22
2.3	Privacy is er in verschillende smaken	22
2.4	Privacy is een kwestie van menselijke beschaving	24
2.5	Privacy is essentieel voor de economie	24
2.6	Privacy is persoonlijk Total Data Management	25
2.7	Privacy is een set van trade-offs	27
2.8	Privacy is angst, onzekerheid en twijfel	29
2.9	Privacy en Big Data	32
2.10	Een game om privacy te oefenen	35

2.1 Een eerste schets

Als privacy een fundamenteel mensenrecht is, er verschillende smaken zijn, en als privacy bovendien een kwestie van menselijke beschaving is, zoals sommigen beweren, en essentieel is voor de economie, is het om uiteenlopende redenen dan niet doodzonde dat er momenteel zoveel angst, onzekerheid en twijfel is?

Dat geldt des te meer voor digitale privacy en de waarde van Personally Identifiable Information: in commerciële transacties, in de gezondheidszorg, voor energiemanagement, in de relatie burger-overheid enzovoort. Gegevens beschikbaar stellen omtrent persoon en gedrag in ruil voor efficiënte dienstverlening op maat kan een prima deal zijn met instanties, bedrijven en overheden, mits we weten wat er met onze data gebeurt en wat de risico's zijn. Is dat bekend en ook voor de toekomst geregeld, dan kunnen we op die basis afwegingen en afspraken maken en zagezegd ons Vendor Relationship Management (VRM) in eigen hand nemen of uitbesteden.

Deels zijn angst, onzekerheid en twijfel nu eenmaal de aard van het beestje, want privacy behoort toe aan het fragiele individu dat stand moet zien te houden in de maalstroom van de moderne maatschappij met alle tegenstrijdige belangen van dien. In deze digitale tijd van steeds meer Privacy-Invasive Technologies en datasurveillance moet alle hens aan dek om de angel van de angst te verwijderen.

Dat doen we door ons te richten op persoonlijk Total Data Management – controle kortom over onze PII, onze Personally Identifiable Information. Technologie staat daarbij centraal in de balans, of de wedloop zo u wilt, tussen Privacy-Invasive Technologies (PIIT's) en Privacy-Enhancing Technologies (PET's).



PbD-vraag 3
Maken privacy-requirements integraal deel uit van het ontwerp en de architectuur van uw ICT-systemen en businesspraktijken?

<http://bit.ly/vintR3Q3>

Idealiter moet die balans in de praktijk steeds 'volautomatisch' en met opperste nauwkeurigheid tot stand komen via Privacy by Design. Het betekent dat de PEr's integraal moeten zijn afgestemd en ingeregeld op de juiste procedures, regelgeving, de fysieke omgeving enzovoort, zoals voorgesteld aan het eind van paragraaf 1.5 en in de conclusie van deze notitie.

In dit hoofdstuk brengen we het (digitale-)privacythema ter oriëntatie op zeven verschillende noemers. We sluiten af met de toenemende rol van Big Data en een game om privacy in sociale netwerken te oefenen.

2.2 Privacy is een fundamenteel mensenrecht

No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation.

Universele Verklaring van de Rechten van de Mens, 1948, art. 12

Privacy is een onvervreemdbaar mensenrecht in de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties en komt over de hele wereld als recht voor in handvesten, grondwetten, gewone wetten en verdragen. In resolutie A/HRC/20/L.13 van de VN-Mensenrechtenraad uit juli 2012 over 'de promotie, bescherming en het bezit van mensenrechten op internet' staat dat alle mensenrechten offline en online moeten worden beschermd, in het bijzonder de vrijheid van meningsuiting. Dat is bovendien bevorderlijk zo niet essentieel voor het economische verkeer.

2.3 Privacy is er in verschillende smaken

De eerste privacywet stamt uit 1361, toen in Engeland gluren en afluisteren strafbaar werd gesteld. Moderne privacyopvattingen onderscheiden verschillende categorieën, bijvoorbeeld persoonlijk, informatieel, organisatorisch, spiritueel en intellectueel, of 'bodily privacy (private parts), territorial privacy (private places), communications privacy (private messages), information privacy'. Onze online privacy wordt ook vaak *ePrivacy* genoemd. Digitale privacy is niet noodzakelijkerwijs online en naar de letter hoeft informatieprivacy niet per se digitaal te zijn. Wat digitale Personally Identifiable Information tegenwoordig allemaal kan zijn, somt de afbeelding op pagina 26 op.

Behalve dat er verschillende soorten privacy zijn, kan ook de mate van privacy verschillen. We zien dit bijvoorbeeld in onze browserinstellingen:





Privacy-niveaus vinden we ook terug in de consumentengegevens die organisaties over ons verzamelen (de illustratie is van Magenta Advisory):

<p>1. Identification data</p> <ul style="list-style-type: none"> • Name • Address • Phone number • Invoicing information • Date of birth • Email address • IP address 	<p>2. Behavioral data</p> <ul style="list-style-type: none"> • Purchasing history • Search and web-browsing history • Salary information • Likes on Facebook • Rating & Reviews
<p>3. Derived data</p> <ul style="list-style-type: none"> • Profitability • Loyalty • Interest • Behavioral models • Analytical models 	<p>4. Permission and preferences</p> <ul style="list-style-type: none"> • Accepted terms and conditions • Marketing permissions • Orders (e.g. newsletter) • Settings



Het is de ongecontroleerde combinatie van dit soort digitale data die ons momenteel veel privacyzorgen baart.

2.4 Privacy is een kwestie van menselijke beschaving

De bekende en zelfs enigszins controversiële Russisch-Amerikaanse schrijfster Ayn Rand (1905-1982) stelde onze maatschappelijke beschaving kernachtig gelijk aan optimale privacy:

Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.

A. Rand (1943), *The Fountainhead*

In de achttiende eeuw verwoordde de Franse politieke denker Jean-Jacques Rousseau het nog ironisch aldus:

The first man who, having enclosed a piece of ground, bethought himself of saying "This is mine," and found people simple enough to believe him, was the real founder of civil society.

Rousseau (1754), *Discourse on the Origin and Basis of Inequality among Men*

We hoeven ons niet te kunnen vinden in de nuances van deze waarnemingen om in te zien dat digitaal en online het verschil tussen mijn en dijn tegenwoordig steeds minder duidelijk is, evenals het verschil tussen publiek, persoonlijk en geheim en dat tussen gratis en betaald. Wat zegt dat over onze 'beschaving'? Zijn we die aan het verliezen; heeft maatschappelijke beschaving niet altijd juist een averechts effect gehad; of moeten we met onze tijd meegaan en niet zeuren over hoe menselijke constructen als privacy nu eenmaal opschuiven?

2.5 Privacy is essentieel voor de economie

Het inzicht van Rousseau is de start van het artikel 'Privacy: Its Origin, Function, and Future' uit 1979. Daarin benadrukt de Amerikaanse econoom en hoogleraar Jack Hirschleifer de economische dimensie van privacy. In het richtingwijzende *Framework for Global Electronic Commerce* van de regering-Clinton uit 1997 komt dit heel expliciet tot uiting, zoals we in paragraaf 1.2 hebben gezien.

Privacy, zegt Hirschleifer in 1979, is tegenwoordig niet zozeer een traditionele 'secrecy'-kwestie – een zaak van je kunnen afzonderen en van geheimhouding – centraal staat juist de 'autonomy within society.' Die autonomie van individuen en groepen is synoniem met actief economisch handelen en Hirschleifer was gespecialiseerd in de relatie daarvan met onzekerheid en informatie: wat betekent het als mensen niet goed

weten en kunnen inschatten wat er allemaal over hen bekend is? Privacy als ‘a way of organizing society’ in plaats van ‘withdrawal’, zoals Hirschleifer het in zijn artikel letterlijk onderstreept.

2.6 Privacy is persoonlijk Total Data Management

Volgens de schrijver Gabriel García Márquez heeft elk mens drie soorten levens: een publiek leven, een privéleven en een geheim leven. Al in 1948 beschreef George Orwell in zijn boek *1984* wat devices en het internet daarmee zouden doen:

It was terribly dangerous to let your thoughts wander when you were in any public place or within range of a telescreen. The smallest thing could give you away.

Dat was toen en is gelukkig nog steeds bijzonder overdreven, maar het geeft goed de angst weer waarmee we de huidige *surveillance & dataveillance society* ervaren. Op straat en online kunnen alle denkbare datastromen continu in de gaten worden gehouden.

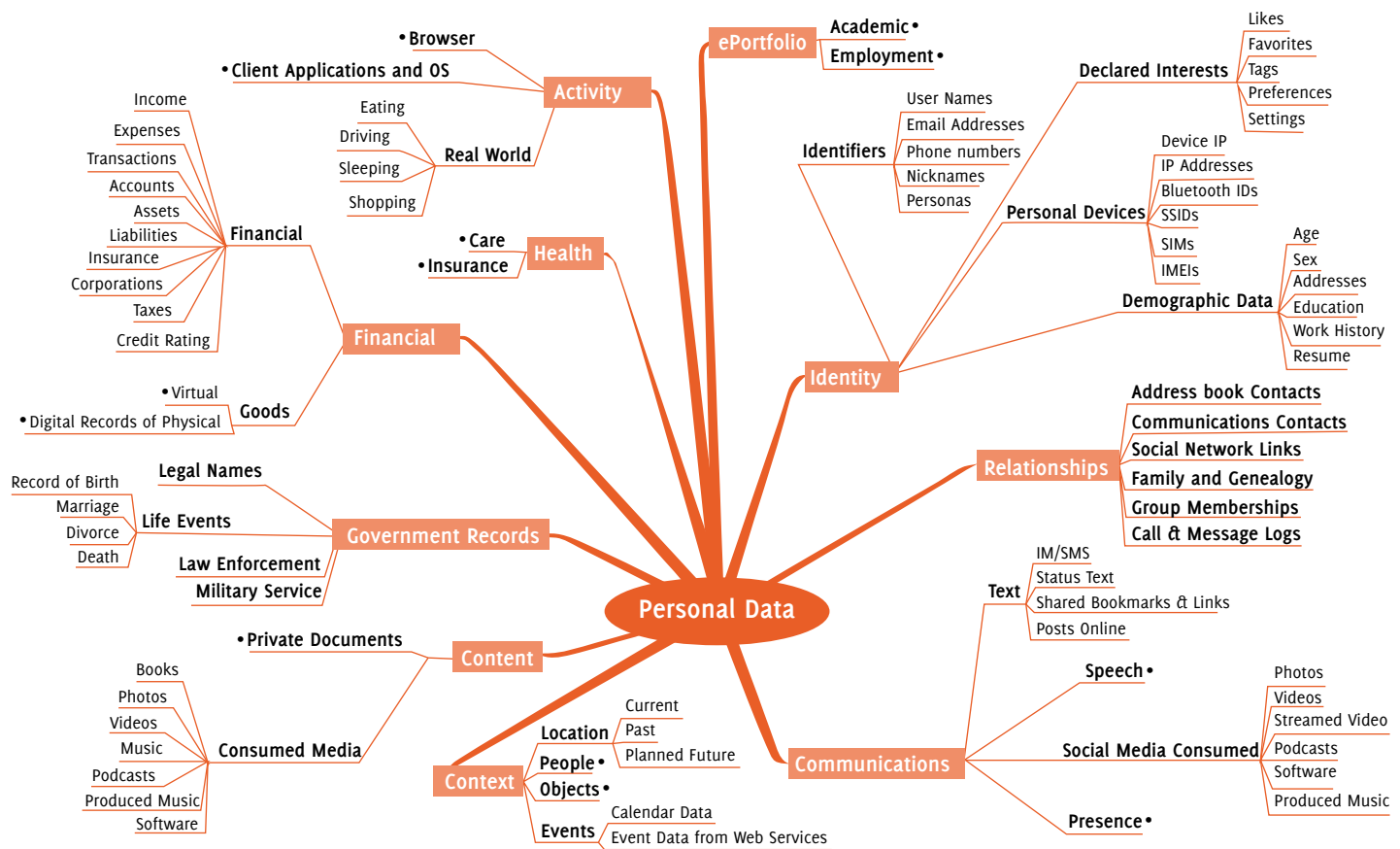
De enige plek waar we nog een beetje privacy hebben, zo lijkt het, is thuis op het toilet. *Privacy*, *private* en *privy* liggen niet voor niets direct in elkaars verlengde. De titel van deze *Digital Life eGuide* speelt met die betekenisverwantschap:



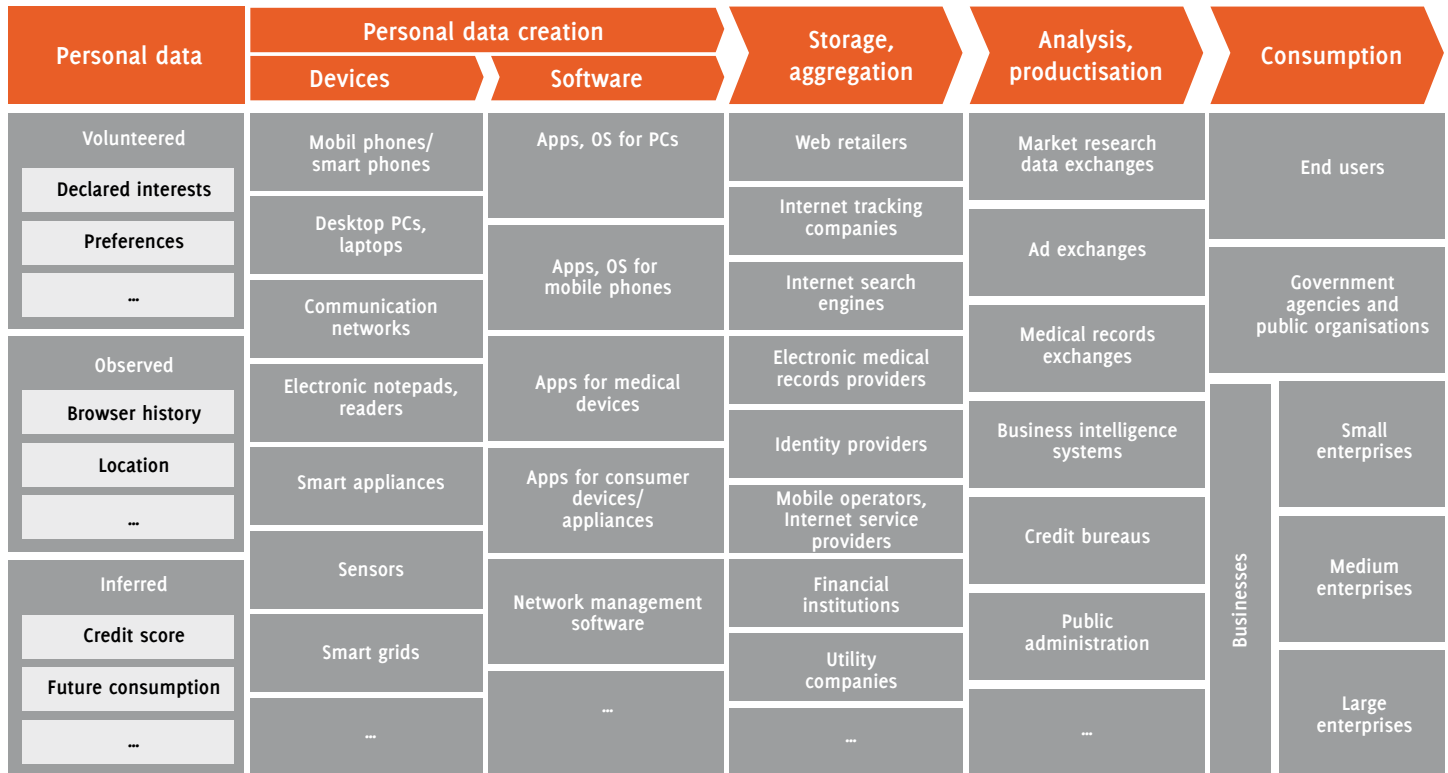
Het verschil tussen publiek, privé en geheim is de essentie van het privacythema, zeker in de context van persoonsgegevens en andere persoonlijke informatie. De bescherming daarvan – gegevensbescherming, data protection, Datenschutz – is bij wet geregeld.

In Nederland hebben we de Wet bescherming persoonsgegevens, Duitsland heeft zijn *Datenschutzgesetz* en de Europese Unie heeft haar *Data Protection Directive*. Die laatste richtlijn zal worden veranderd in een bindende wet voor alle lidstaten en moet in 2015 in werking treden, zo is de bedoeling. Met alle digitale activiteit vandaag de dag is het onderscheid tussen publiek, privé en geheim nog nooit zo vloeidend en kneedbaar geweest.

Kaliya Hamlin, online onder meer bekend als Identity Woman, maakte de volgende mindmap van de wolk met persoonlijke digitale gegevens of Personally Identifiable Information (PII) die we allemaal tegenwoordig in meerdere of mindere mate om heen hebben hangen: deels publiek, deels privé en deels geheim. Bij elkaar geeft dit op elk moment een compleet beeld van wie we zijn, waar we mee bezig zijn, wat we denken en wat we interessant vinden; dus waar we op de een of andere manier voor zouden willen betalen of mee gechanteerd zouden kunnen worden.



De PII-levenscyclus van creatie tot consumptie ziet er volgens het World Economic Forum-rapport *Personal Data: The Emergence of a New Asset Class* schematisch als volgt uit:



Persoonlijke digitale data in maten en soorten vormen samen het domein van digitale privacy. Dan gaat het er niet eens zozeer om dat onze kostbare PII koste wat kost geheim blijft als wel dat we zelf in de hand hebben wat we er wel en niet van willen ruilen of verkopen, zoals Jack Hirschleifer in 1979 met zijn *autonomie* al zei. Om die autonomie als organiserend maatschappelijk en economisch principe optimaal te kunnen uitoefenen, moeten we steeds weten hoe onze PII zich concreet verhoudt tot de twee overzichten hiervoor, wat er onbedoeld van ‘weglekt’ en hoe daar gebruik van wordt gemaakt.

2.7 Privacy is een kwestie van trade-offs

Als we zeggen dat privacy – of gewoon je vrij voelen, lekker in je vel zitten – essentieel is voor een geoliede digitale economie, dan komt ons onmiddellijk ook het economische begrip *trade-off* in gedachten. Situationeel en van persoon tot persoon maken we verschillende keuzen in wat we wel en niet in een bepaalde uitruil zullen willen toestaan ten aanzien van het verzamelen, delen en gebruiken van informatie, immers:

- *Privacy is “the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values.”*

- *There is no free lunch: We cannot escape the trade-off between locking down information and the many benefits for consumers of the free flow of information.*

Berin Szoka, Senior Fellow, The Progress & Freedom Foundation,
op 7 december 2009

Privacy is een ruilobject op vele fronten: *trade-off is the name of the game*. Als ouders in Facebook-posts van hun kinderen snuffelen, dan is er een trade-off tussen privacy en opvoeding. In ons digitale tijdperk hebben we het zelfs over de *privacy paradox*: aan de ene kant anoniem willen zijn en aan de andere kant de welhaast ongeremde drang om ons hele hebben en houden met de wereld te delen.

Bekend is ook de trade-off tussen privacy en gezondheid. Een Elektronisch PatiëntenDossier breekt misschien in op onze privacy, maar we hebben er baat bij voor wat betreft de duur en de kwaliteit van leven. Hetzelfde geldt voor de meest gangbare cookieanalyses op internet en een betere service van organisaties aan klanten en prospects. Privacy-trade-offs zijn er in verschillende vormen, bijvoorbeeld:

- ◆ privacy versus opvoeding;
- ◆ privacy versus gezondheid;
- ◆ privacy versus fraudebestrijding;
- ◆ privacy versus betere dienstverlening;
- ◆ privacy versus efficiënte energiesystemen;
- ◆ privacy versus zelfexpressie;
- ◆ privacy versus veiligheid.

Omdat (digitale) privacy een trade-off is, is het per definitie een economisch goed. In de goede traditie van Hirschleifer zegt onder anderen Alessandro Acquisti, co-director van het Carnegie Mellon Center for Behavioral Decision Research, dit in het paper *The Economics of Privacy*. De economie die zich nu steeds verder rond privacy ontwikkelt, gaat van het *minen* en verkopen van persoonlijke informatie tot de aanschaf van producten om als consument onze privacy te beschermen.

Een van de belangrijkste trade-offs is privacy versus veiligheid in de zin van ons zonder in onze fysieke en ethische integriteit te worden aangetast kunnen bewegen in de fysieke en digitale ruimte. Een overheid die surveilleert op internet op zoek naar kinderporno vinden we acceptabel, camerabewaking ook en vingerafdrukken nemen idem dito. Maar tegelijkertijd groeien de scepsis en de angst. Tegenwoordig staat het Big Brother-sentiment haaks op de kansen die Big Data biedt, commercieel en maatschappelijk.

Ver voor er sprake was van data volume, variety en velocity was Big Brother al een issue. De geschiedenis van de registers, de volkstellingen, allerhande registraties en later de bevolkingsstatistieken is direct verbonden met deze scepsis, die vaak de over-

heid betreft. Daarnaast gaan digitaal en media tegenwoordig hand in hand, wat voor de gewone burger het meest herkenbaar is in de middelen waar onze *Surveillance Society* zich van bedient. Dit thema werd onder meer in 2006 uitgebreid belicht in *A Report on the Surveillance Society for the [British] Information Commissioner* van het Surveillance Studies Network.

Over de trade-off van veiligheid versus privacy wordt druk gedebatteerd en de noodzaak van een trade-off wordt zelfs betwist, bijvoorbeeld door Daniel Solove in zijn boek uit 2011 getiteld *Nothing to Hide: The False Trade-off between Privacy and Security*. Vanuit het VRM-kamp wordt geredeneerd dat privacy dankzij Vendor Relationship Management helemaal geen trade-off hoeft te zijn.

In de Amerikaanse Burgeroorlog van 1861-1865 werd het Big Brother-gevoel sterk gevoed toen het bevolkingsregister werd gebruikt om mogelijke militaire kampen in de zuidelijke staten op te sporen. De opkomst van totalitaire regimes en ideologieën, en de desastreuze uitwerking daarvan inspireerden sciencefictionauteurs tot scenario's die zo dystopisch zijn dat ze de lust voor welke Big Data-achtige samenleving onmiddellijk doen vergaan. We kennen de klassiekers uit het genre:

- ♦ 1924 *We*, Yevgeny Zamyatin
- ♦ 1932 *Brave New World*, Aldous Huxley
- ♦ 1948 *1984*, George Orwell
- ♦ 1951 *Foundations*, Isaac Asimov
- ♦ 1951 *Fahrenheit 451*, Ray Bradbury

Elk van deze boeken geeft een eigen kijk op hoe gedrag van het individu bespied en bestuurd kan worden met behulp van technologie. Daarna, ten tijde van de Koude Oorlog, was in Amerika het vertrouwen in de overheid een stuk groter en was men meer bevreesd voor de vijand dan voor de Grote Broer in eigen land die burgers aan het bespieden was. De communistenjacht van senator McCarthy werd in de jaren vijftig bijvoorbeeld breed gedragen.

2.8 Privacy is angst, onzekerheid en twijfel

Over onzekerheid inzake privacy op basis van technologie zei William Douglas, het langst zittende lid van het Amerikaanse Hooggerechtshof, in 1966 al het volgende:

We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government.

Tegenwoordig vinden we het normaal om in een surveillance- en een dataveillance-society te leven. We hebben te maken met PIT's (Privacy-Invasive Technologies) en aan de andere kant met PET's (Privacy-Enhancing Technologies). De Amerikaanse National Security Agency bouwt momenteel een quantumsupercomputer, Vesuvius



PbD-vraag 4

Hoe gaat u om met privacy versus security? Denkt u dat ze allebei in harmonie gerealiseerd kunnen worden?

<http://bit.ly/vintR3Q4>

gedoopt, om letterlijk alles en iedereen ter wereld via digitale datastromen in de gaten te kunnen houden. Uit naam van nationale veiligheid en bescherming van de democratie, en vooral in het strengste geheim.



Bob Englehart in de Hartford Courant op 22 januari 2006 via <http://www.gsmnation.com/blog/2012/09/25/the-fbi-wants-permission-to-wire-tap-your-facebook-account/google-and-the-feds/>

Onder die geheimhouding vallen bijvoorbeeld ook het gebruik van Palantir-opsporingstechnologie en de relatie van de NSA met onder meer Google. Dat gaat weer een heel stuk verder dan het boek *Database Nation: The End of Privacy in the 21st Century* van Simson Garfinkel uit 2001. Het spectrum van *Fear, Uncertainty & Doubt* waarin fragiele individuen en minderheidsgroepen zich bevinden, kunnen we als volgt weergeven:

DOOD ANGST WANTROUWEN PESSIMISME ONZEKERHEID | ZEKERHEID OPTIMISME VERTROUWEN HOOP LEVEN

We zien vijf categorieën links en recht van het dunne blauwe lijntje, dat ons wiebelige privacygevoel markeert. Hard gekoppeld aan de centrale vraag naar zekerheid, die direct verband houdt met het bekende trio *data – informatie – kennis/begrip*, is de methodische twijfel van Descartes uit de zeventiende eeuw. *Doubt* dus, die, als we haar niet kunnen wegnemen, gauw doorschiet naar angst. Omdat angst verlamrend werkt, willen we er goed mee kunnen omgaan, de twijfel kunnen invullen. Angst willen we kunnen begrijpen met een anatomie als doel. We willen aan de hand van onderdelen kunnen uitleggen wat er aan de hand is om zo de angst te neutraliseren.

Opmerkelijk is nu dat een anatomie van hoop, het tegenovergestelde van angst, vaak ook uit vanuit een negatieve beleving wordt beschreven; in de illustratie hierboven is dat ziekte. En inderdaad, onze privacy zien we vaak als ziek, althans, we vinden dat zij zich ongezond ontwikkelt.

Wat privacygevoel betreft, bevinden we ons bovengemiddeld vaak ver in het rood, bang als we zijn voor Big en Little Brothers die ons te na komen en overvleugelen vanuit met name de technologie. Bij herhaling is de afgelopen tijd verkondigd dat we privacy als verworvenheid in het digitale tijdperk maar helemaal moeten vergeten.

Juist dat ‘vergeten’ is dankzij internet, alle databases die er zijn en nu dan Big Data een groot issue geworden. *The Right to Be Left Alone* heeft er in 2012 een aanscherping bij gekregen in *The Right to Be Forgotten* van EU-commissaris Viviane Reding. Hoe, met welke technologieën en welke procedures, is dat eigenlijk nog te garanderen? Met de DeleteMe-app van Abine? De kans dat we definitief in de rode zone belanden is levensgroot aanwezig, met alle economische en maatschappelijke gevolgen van dien. Zo kan privacy een showstopper worden voor de mooie kansen die datamining en Big Data op veel intermenselijke terreinen bieden.

De Chaos Computer Club slaat alarm

In deze context is onhandig omgaan met Big Data de ene kant van de zaak en doelbewust de regels met voeten treden de andere. Twee voorbeelden uit Duitsland lichten die uitersten toe. Op het jaarcongres van de Chaos Computer Club werd eind 2011 duidelijk dat de slimme energiemeters van leverancier Discovery slecht beveiligd waren. Onnodig werd om de twee seconden het verbruik gemeten en bovendien waren de datastromen niet versleuteld. Daardoor kon nauwkeurig het verbruik per apparaat in een huishouden in kaart worden gebracht met alle analysemogelijkheden betreffende bijvoorbeeld kijkgedrag en internetgebruik van dien. De data die de onderzoekers hadden bemachtigd, waren afkomstig van standaard verzegelde ‘smart meters’. De slechte beveiliging had tevens tot gevolg kunnen hebben dat hackers die verder het systeem wisten binnen te dringen, in staat waren de energievoorziening van miljoenen huishoudens plat te leggen.

In het verlengde van het hierboven aangestipte alomvattende datamonitoringproject Vesuvius van de geheime Amerikaanse National Security Agency staat de ontdekking

van een computervirus door dezelfde Chaos Computer Club afkomstig van de Duitse overheid, eveneens in 2011. De code was in staat een computer compleet te infiltreren, alle handelingen in de gaten te houden, ze op te slaan, en nieuwe virussen aan te brengen. Camera, screenshots, internettelefoonverkeer, toetsaanslagen en natuurlijk alle bestanden op de harde schijf waren compleet onder controle van de af luistersoftware, aldus de *Frankfurter Allgemeine Zeitung*.

2.9 Privacy en Big Data

Sinds de ontwikkeling in de negentiende eeuw van mediatechnologie als fotografie, telefoon en telegraaf is privacy een steeds prominenter aandachtspunt geworden. De maxime *Privacy Is the Right to Be Left Alone* stamt uit het Amerika van 1890. Toen begonnen de ontwikkeling van technologie en onze behoefte aan privacy elkaar in de wielen te rijden:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be left alone.” [...] Numerous [...] devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the rooftops.”

Dit citaat geldt nog steeds. Zonder de fotografie, de kranten en het woord mechanisch, die we bewust uit het citaat hebben weggelaten, had niemand kunnen vermoeden dat deze woorden uit 1890 stammen, uit het artikel ‘The Right to Privacy’ van Samuel Warren en Louis Brandeis in de *Harvard Law Review*. Daarmee startte de hele moderne privacydiscussie. En nog steeds spelen fotografie en paparazzi een centrale rol in privacyvraagstukken.

Dat Big Data tegenwoordig extra privacyzorgen oplevert, bleek onder andere toen de grootste Duitse kredietbeoordelaar Schufa aankondigde dat ze ten behoeve van betere profielen informatie uit Twitter, Facebook en LinkedIn zou koppelen aan haar 66 miljoen mensen tellende klantenbase.

Met deze aanval op het recht van mensen om controle te hebben over hun eigen data vreesde Duitsland ‘Amerikaanse toestanden.’ Ilse Aigner, de minister die consumentenrecht in haar portefeuille heeft, liet weten dat sociale netwerken niet systematisch ingezet mogen worden om kredietaanvragen te beoordelen.

In 2012 vielen onder meer de volgende drie artikelen op, die het gecombineerde thema behandelden van privacy, databescherming en de opkomst van Big Data:

- ♦ Het eerste, getiteld ‘Privacy in the Age of Big Data: A Time for Big Decisions’, verscheen in het februarinummer van *Stanford Law Review*.

- ♦ Nummer twee, 'The Challenge of Big Data for Data Protection', zag het licht in het meinummer van het *Oxford Journal on International Data Privacy Law*.
- ♦ En het derde, 'Privacy by Design in the Age of Big Data', kwam in juni van het Office of the Information and Privacy Commissioner of Ontario, Ann Cavoukian. Haar medeauteur is IBM's Big Data-goeroe Jeff Jonas.

Het artikel 'Big Data for All: Privacy and User Control in the Age of Analytics' gaf in februari 2012 op de website van het tijdschrift *Stanford Law Review* goed aan wat er in het licht van Big Data aan de hand is met privacy en databescherming. De redenering is als volgt: Big Data is realiteit; er zit bijzonder veel waarde in, maar het voedt ook het onbehagen inzake privacy. Tussen organisaties en individuen moeten we hier dus een goede balans in zien te creëren. Gelijk aan het begin maken de auteurs, Omer Tene en Jules Polonetsky, de volgende zeven punten:

De Big Data-realistieit

1. *Ontwikkelingen in data mining en analytics en de enorme toename van rekenkracht en dataopslag hebben de informatie waarover organisaties en overheden kunnen beschikken, explosief vergroot.*
2. *Gegevens kunnen nu buiten gestructureerde databases om in ruwe vorm worden geanalyseerd. Daardoor kunnen er veel beter verbanden worden gelegd en komen er nieuwe, onvermoede toepassingen voor bestaande informatie.*
3. *Tevens heeft het groeiende aantal mensen, devices en sensors die verbonden zijn door digitale netwerken, een revolutie teweeggebracht in de creatie, de communicatie, het delen van en de toegang tot data.*

De waarde en privacy-uitdaging van Big Data

4. *Data zijn van grote waarde voor de wereldeconomie als grondstof voor innovatie, productiviteit, efficiency en groei. Tegelijkertijd stelt de datavloed ons voor privacyvraagstukken die mogelijkwjs leiden tot regelgeving die de dataeconomie en innovaties tot staan brengt.*
5. *Om een balans te vinden moeten beleidsmakers een aantal van de meest fundamentele privacyconcepten adresseren, zoals de definitie van Personally Identifiable Information (PII), de rol van controle daarover door het individu en de principes van minimaal en doelgericht gebruik van data.*

Een goede balans voor organisaties en individuen

6. *Als individuen op een toegankelijke manier kunnen beschikken over hun data, kunnen ze de rijkdom die de informatie in zich bergt delen. Op die basis kunnen waardevolle klanttoepassingen worden ontwikkeld.*
7. *Uiteraard zijn organisaties verplicht hun beslissingscriteria duidelijk te maken, want in een Big Data-wereld zijn vaak de conclusies die worden getrokken aanleiding tot zorg, niet zozeer de data zelf.*

Het artikel 'Big data for All', dat nog zal verschijnen in het *Northwestern Journal of Technology and Intellectual Property*, geeft een overzicht van de voordelen van Big Data op verschillende terreinen en in verschillende economische sectoren. Vervolgens komen de bedenkingen aan bod, gevolgd door een aantal centrale uitdagingen en tot slot ook oplossingen.

Fundamenteel ondersteunend is het concept van Privacy by Design: het zorgwekkende effect van Privacy-Invasive Technologies moet worden opgeheven door een intense combinatie van Privacy-Enhancing Technologies, regelgeving, beleid, procedures en verantwoordelijk gedrag van alle partijen.

Op die manier moet ook Big Data een win-winsituatie kunnen worden voor iedereen. Die ambitie en belofte willen overal ter wereld de politiek, bedrijven, overheden en individuen gerealiseerd zien.

Privacy, technologie en de wet

Het is de bedoeling dat de relatie tussen het trio privacybescherming, digitale technologie en regelgeving de komende jaren overal ter wereld sterk ten goede zal veranderen. Dat is belangrijk voor de ontwikkeling van de economie en van de sociaalmaatschappelijke verhoudingen. In 2011 installeerde het 112^{de} Amerikaanse Congres (de regering-Obama I) voor het eerst een aparte senaatscommissie met deze duidelijke naam: *Privacy, Technology and the Law*. De commissie heeft de volgende vier hoofdtaken in haar portefeuille:

- *Toezicht op regelgeving en beleid inzake de verzameling, de bescherming, het gebruik en de verspreiding van commerciële informatie door de private sector, waaronder behavioral advertising, privacy in sociale netwerken en andere online privacy-issues.*
- *Handhaving en implementatie van commerciële informatieprivacyregeling en -beleid.*
- *Gebruik van technologie door de private sector om de privacy te beschermen, de transparantie te vergroten en innovatie aan te moedigen.*
- *Privacystandaarden voor de verzameling, de opslag en het beheer, het gebruik en de verspreiding van commerciële Personally Identifiable Information (PII).*
- *Privacy-implicaties van nieuwe of opkomende technologieën.*

In onze Big Data-businessrealiteit gaan we nu wereldwijd de kant op van een principiële nadruk op transparantie en keuze, op 'informed consent' en duidelijke 'opt out'-mogelijkheden voor individuen. Daarbij lijkt een balans tussen PIT's en PET's, gekoppeld aan heldere regels en procedures via Privacy by Design, de beste want meest integrale oplossing. Daarover gaat hoofdstuk 3.

2.10 Een game om privacy te oefenen

Tot Privacy by Design behoort ook het aankweken van awareness en eigen verantwoordelijkheid. Op <http://www.open.edu/openlearn/privacy> is sinds kort een privacyspel beschikbaar om te oefenen in de nieuwe normen en waarden op sociale netwerken. Via 'Secret or sharing? Play our Privacy Game' kunt u bepalen welke informatie u bereid bent te delen en wat u beter voor uzelf kunt houden. Het spel biedt de gelegenheid om op een veilige manier een leerzaam gokje te wagen met uw persoonlijke data. Via OpenLearn speelt u alleen tegen de computer, maar u kunt ook uw Facebook-vrienden uitdagen in een multiplayer-versie van het privacyspel, dat dan natuurlijk nog steeds een besloten karakter heeft.



Count not him among your friends who will retail your privacies to the world.

Publilius Syrus, ca. 50 v. Chr.

3 Privacy by Design en de balans tussen PIT's en PET's

(Privacy-Invasive versus Privacy-Enhancing Technologies)

3.1	Een nieuwe privacytaxonomie	36
3.2	Personally Identifiable Information en PET's	37
3.3	Privacy volgens TNO en TILT	40
3.4	E-privacygerelateerde uitdagingen	42
3.5	Verantwoordelijk gedrag als kern	43

3.1 Een nieuwe privacytaxonomie

In januari 2006 publiceerde de *University of Pennsylvania Law Review* een 84 pagina's tellend artikel van Daniel Solove, momenteel hoogleraar aan de George Washington University Law School. In het artikel, waaraan nog 25 andere deskundigen bijdroegen, presenteert Solove een nieuwe *Taxonomy of Privacy*, zoals de titel kort en krachtig luidt, gerelateerd aan technologie en informatie.

Digitale vernieuwingen zijn hand over hand toegenomen maar het abstracte juridische privacybegrip was en is daar onvoldoende op aangepast, om een understatement te gebruiken. Solove en de zijnen zijn snoeihard in hun oordeel:

Privacy is a concept in disarray. Nobody can articulate what it means. [...] Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of "privacy" do not fare well when pitted against more concretely stated countervailing interests. [...] This Article develops a taxonomy to identify privacy problems in a comprehensive and concrete manner.

De notie van privacy moet veel beter handen en voeten worden gegeven, zeker om privacy helder te kunnen gebruiken in de context van regelgeving. Begin 2006 waren we al ver in het digitale tijdperk voortgeschreden, maar concrete nieuwe privacy-issues werden verre van adequaat geadresseerd. Het was hoog tijd voor een alomvattende en duidelijke indeling die vooral zou aangrijpen op de activiteiten die mensen, organisaties en overheden aan de dag leggen:

Technology is involved in various privacy problems, as it facilitates the gathering, processing, and dissemination of information. Privacy problems, however, are caused not by technology alone, but primarily through activities of people, businesses, and the government. The way to address privacy problems is to regulate these activities.

Vanuit deze interessante observatie uit 2006 zijn we zeven jaar later op een punt aanbeland waar de aandacht voor activiteiten begint te worden gecombineerd met de ontwikkeling en handhaving van een goede balans: tussen Privacy-Invasive Technologies (PIT's) enerzijds en Privacy-Enhancing Technologies (PET's) anderzijds. Deze fundamentele en integrale aanpak staat bekend als Privacy by Design. Als klankbord daarvoor fungeert de volgende privacytaxonomie van Solove en de zijnen uit 2006, die een duidelijke technologie- en informatiefocus heeft:

Information Collection

- Surveillance
- Interrogation

Information Processing

- Aggregation
- Identification
- Insecurity
- Secondary Use
- Exclusion

Information Dissemination

- Breach of Confidentiality
- Disclosure
- Exposure
- Increased Accessibility
- Blackmail
- Appropriation
- Distortion

Invasion

- Intrusion
- Decisional Interference



PbD-vraag 5

Denkt u er bij databescherming ook aan dat informatie op een bepaald tijdstip veilig moet kunnen worden vernietigd?

<http://bit.ly/vintR3Q5>

3.2 Personally Identifiable Information en PET's

Om verschillende redenen en op verschillende manieren beschikken organisaties over de Personally Identifiable Information (PII) van medewerkers, klanten en andere

partijen. Daarbij moeten privacy- en databescherming goed in acht worden genomen. Goed ontworpen en geïmplementeerde Privacy-Enhancing Technologies (PET's) zijn het tegenovergestelde van Privacy-Invasive Technologies (PIT's). Ze helpen om bescherming en controle te realiseren in combinatie met regelgeving, richtlijnen, processen, training enzovoort.

Idealiter hebben PET's een duidelijke relatie met wat wetten en regels inzake privacy voorschrijven en beogen. Het Britse Information Commissioner's Office omschrijft PET's dan ook als:

any technologies that protect or enhance an individual's privacy, including facilitating access to their rights under the Data Protection Act.

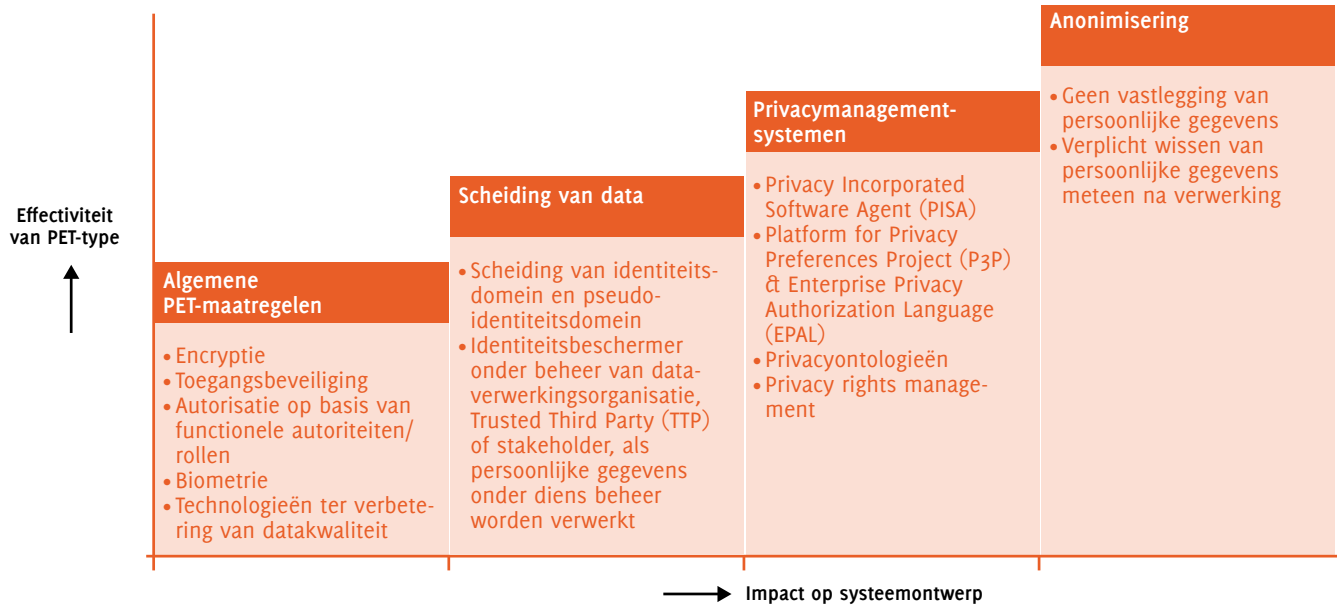
De Europese Unie benadrukt bovendien de rol van PET's in het ontwerp van informatie- en communicatiesystemen, zodanig dat regelgeving vanuit de technologie handen en voeten krijgt:

The use of PETS can help design information and communication systems and services in a way that minimises the collection and use of personal data and facilitates compliance with data protection rules making breaches more difficult and/or helping to detect them.

De hierboven aangehaalde *Taxonomy of Privacy* van Daniel Solove kan goed dienen als een *Privacy Impact Assessment*-raamwerk (zie paragraaf 4.8) voor PET's die privacygerelateerde schade moeten voorkomen. In het geding is wat bekendstaat als *Fair Information Practices*, het fundament van een vertrouwenswaardige digitale economie, zeker als daarbinnen met Big Data wordt gewerkt. In het geding zijn onze persoonsgegevens, onze PII of simpelweg onze contextuele ID. Met dank aan Alexander Alvaro, vicepresident van het Europese parlement, hebben we de beschrijving van zijn PII-pictogrammen teruggebracht tot de praktische set van FIP's (*Fair Information Practice Principles*) hiernaast.

Een concreet overzicht van PET's geeft de desbetreffende wiki van het Center for Information and Society: <http://cyberlaw.stanford.edu/wiki/index.php/PET>. De volgende illustratie van Koorn en Ter Hart (2011) geeft een overzicht van de effectiviteit van verschillende PET-typen, afgezet tegen de impact op het systeemontwerp.

	verzamelen	
	bewaren	
	verwerken	
	verspreiden	
	verkopen	
	versleutelen	



Technologie is een noodzakelijk hulpmiddel, maar het succes hangt altijd af van implementatie – zie Koorn en Ter Hart (2011) voor een overzicht – en adoptie. In *Privacy Enhancing Technologies: A Review* uit 2011 doen Yun Shen en Siani Pearson van HP Laboratories de aanbeveling om te focussen op de volgende terreinen:

- Usability
- Privacy by Design
- Economics of Privacy

Wat dat laatste betreft vinden we de kosten van een afgewogen privacykeuze, hoe klein ook, tegenwoordig meestal niet de moeite waard. De zogeheten *Willingness to Pay* legt het in de praktijk duidelijk af tegen de *Willingness to Accept*. Een goed voorbeeld is het klakkeloos akkoord gaan met pagina's lange voorwaarden online.

Differential Privacy

In de context van het nog steeds zeer relevante thema databaseprivacy moet hier het relatief onbekende *Differential Privacy* aan worden toegevoegd. De individuele bescherming van privacy in databases is heel moeilijk te garanderen, ook als PII is geminimaliseerd. Met de nodige moeite blijkt het toch vaak mogelijk om vanuit andere databases informatie aan te vullen en die zo te herleiden tot het individuele niveau. Differential Privacy neutraliseert onder meer dit re-identificatieprobleem door ruis toe te voegen aan de verder correcte database-inhoud. De kwaliteit van de geaggregeerde resultaten komt door een Differential Privacy-aanpak niet in het geding.

3.3 Privacy volgens TNO en TILT

In december 2011 publiceerden TNO en TILT het rapport *Trusted Technology: een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid*. Het concept van Privacy by Design vertrekt expliciet vanuit Privacy-Enhancing Technologies (PET's). Zie bijvoorbeeld het 350 pagina's tellende *Handbook of Privacy and Privacy-Enhancing Technologies* uit 2003 op de website van het College bescherming persoonsgegevens: http://www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf. Die publicatie is gewijd aan intelligente software agents.

Het PET-spectrum is enorm breed. Een basale PET-toepassing op computer-niveau is deze beveiligingstool voor onder meer beveiligde wachtwoorden, bestandsversleuteling, een beveiligd dagboek en een optie om bestanden definitief te verwijderen:

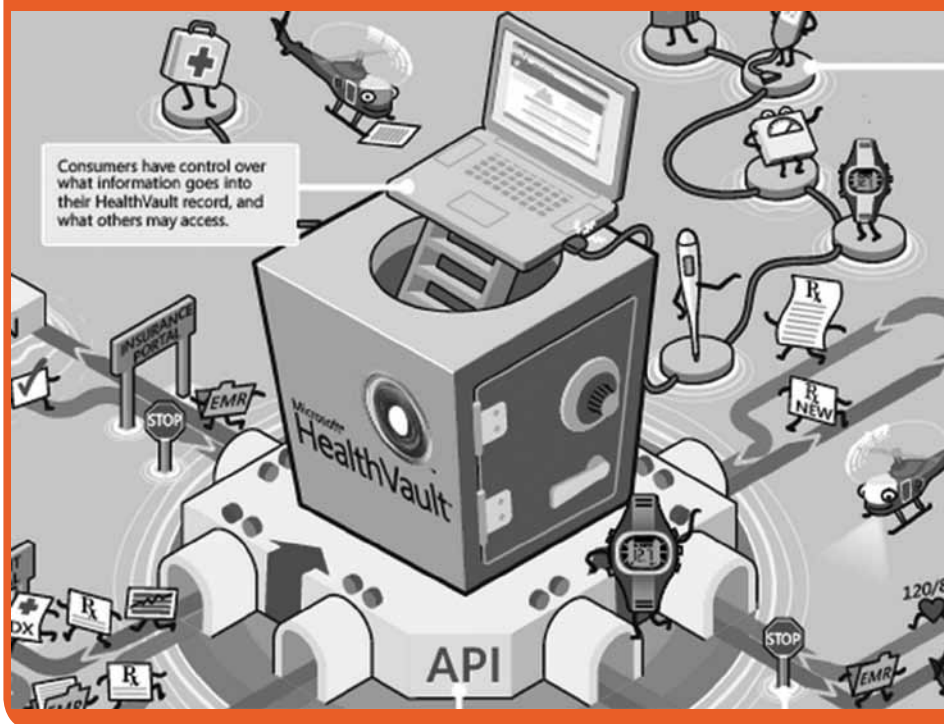


Een overzicht van een ICT-specifieke *Top Ten Big Data Security and Privacy Challenges* geeft het gelijknamige rapport van de Cloud Security Alliance – onder meer Fujitsu en HP Labs – uit november 2012.

Een andere focus is die van de digitale kluis (Digital Vault). Dat soort kluisen is er in soorten en maten, van eenvoudige consumententoepassingen, zoals

van British Telecom, tot aan de gepatenteerde kluistechnologie van leveranciers als CyberArk, die speciaal is ontwikkeld om het niveau van de best beveiligde bankkluisen te evenaren.

Een concrete toepassing, in lijn met het nieuwe Elektronisch PatiëntenDossier, is Microsoft HealthVault. In zo'n persoonlijke kluis kunnen individuen hun gezondheidsinformatie opslaan, updaten, koppelen aan devices en makkelijk delen met medisch personeel, de apotheek, verzekeraars en andere partijen.



Privacy by Design is het toepassen van technische en organisatorische maatregelen bij informatiesystemen om inbreuken op de persoonlijke levenssfeer te vermijden. Als informatiesystemen inherent privacyvriendelijk zijn, draagt dat substantieel bij tot een duurzame informatiesamenleving. (TNO is de organisatie voor Toegepast Natuurwetenschappelijk Onderzoek en TILT het Tilburg Institute for Law, Technology and Society.)

Maar in zijn algemeenheid, zo legt het rapport van TNO en TILT uit, omvat de bescherming van privacy alle activiteiten en maatregelen, gericht op de regulering van de toegang tot het individu in ruimtelijke, relationele en informationele zin. Dat gaat dus verder dan de bescherming van persoonsgegevens ofwel dataprotectie.

Bescherming van privacy heeft uiteindelijk als doel om de persoonlijke autonomie van mensen te beschermen of te vergroten en hun kwetsbaarheid – bijvoorbeeld voor materiële schade, discriminatie, stigmatisering – te verminderen of althans niet verder te vergroten. Privacy is bovendien niet alleen bedoeld om individuen te beschermen. De waarden achter privacy hebben ook belangrijke sociale dimensies en vrijheidsdimensies.

Privacy geeft mensen de mogelijkheid om zonder controle van buitenaf tot eigen meningen en voorkeuren te komen. Zo draagt privacy bij tot de pluriformiteit en creativiteit in de samenleving en tot de bescherming en handhaving van de democratische rechtsstaat. Tot zover TNO en TILT.

3.4 E-privacygerelateerde uitdagingen

De zienswijze van TNO en TILT is een legitieme maar erg ideële kijk op de e-privacy-discussie. Een concretere nadruk op *Trustworthy Social eCommerce* vinden we bij Philippe Coueignoux van Eprivacy.com. In zijn analyse 'ePrivacy, What's at Stake?' maakt Coueignoux duidelijk dat ICT- en internetgerelateerde interne fraude, externe fraude en expliciete privacy-issues allemaal vertrouwensbreuken veroorzaken die direct *Economic Activity & Individual Business Valuation* in de wielen rijden, zoals hij dat noemt. Coueignoux geeft de volgende handige vijfdeling van aan e-privacy gerelateerde thema's die hij schaaft onder *Liabilities and Vulnerabilities in the Information Age*.

Overzicht van online-privacy-issues

1. *Identiteit*: diefstal van persoonsgegevens, kredietfraude, ambush marketing
2. *Eigendom*: medische data, marketingcampagnes, internationale data & safe harbor (zie paragraaf 4.7), bewaking, virale marketing
3. *Locatie*: gegevens zoeken en matchen
4. *Verdediging (de goede kant)*: beveliging, opslag, gebruik, verspreiding en aanbeveling van digitale informatie
5. *Aanval (de donkere kant)*:
 - tijd stelen van ontvangers: spam, zoekresultaten manipuleren
 - de toegang blokkeren: denial of service, censuur
 - de context vervalsen: kopiëren, plagiaat en bedrog, advertentiefraude

Een recente suggestie van Coueignoux aan de presidenten Barack Obama en Herman van Rompuy is om economisch gebruik van privacy financieel progressief te belasten naast de handhaving van e-privacy-wetgeving. De deels technologische Privacy & Security by Design-oplossing van Coueignoux sluit aan bij de economische waarde die persoonlijke data in het internettijdperk hebben.

3.5 Verantwoordelijk gedrag via Privacy & Security by Design

De kern van alle ethisch-juridische thema's is verantwoordelijk gedrag. Voor de bescherming van persoonlijke digitale data annex privacy op internet geldt dat zeker vanwege de fluïditeit. Een niet-limitatieve generieke opsomming van verantwoordelijk gedrag van verschillende stakeholders, met in het midden wet- en regelgeving, rechtspraak en jurisprudentie – het liefst dus internationaal goed geharmoniseerd of geüniformeerd – is de volgende:



Wat Vrouwe Justitia in haar wetgevende, uitvoerende/handhavende en rechtsprekende capaciteit allemaal aan mogelijkheden en middelen ten dienste staat is indrukwekkend, maar in de praktijk moet het allemaal wel nog even gebeuren. In de context van privacy en security liggen Privacy & Security by Design idealiter aan de basis van alle inspanningen.

In de eerste plaats zijn Privacy & Security by Design het van systeemontwerp af aan inbouwen van privacybescherming door middel van Privacy-Enhancing Technologies (PET's). Behalve op het technische microniveau moet het principe ook doorwerken op het organisatorische meso- en het wettelijke macro-niveau. Het doel van Privacy & Security by Design is tweërlei: veilige privacyvriendelijke systeemontwerpen en een duurzame informatiemaatschappij in de dagelijkse praktijk.

Bij herhaling en in verschillende contexten hebben het Nederlandse parlement en de senaat aangedrongen op Privacy by Design. Zo dienden de Tweede Kamerleden Elissen, Gesthuizen en Hennis-Plasschaert in oktober 2011 de volgende motie in:

*De Kamer,
gehoord de beraadslaging,*

overwegende, dat er bij ICT-projecten van de overheid te weinig aandacht is voor de bescherming van privacy en er te weinig aandacht is voor het voorkomen van misbruik van deze systemen;

overwegende, dat privacy van burgers niet verder aangetast dient te worden dan strikt noodzakelijk is en dat onveilige systemen privacy in gevaar brengen;

overwegende, dat systemen die gemakkelijk gekraakt kunnen worden het aanzien van de overheid ernstig aantasten;

overwegende, dat achteraf systemen aanpassen om privacy te waarborgen en veiligheid te verhogen in de regel duurder is en vaak tot een lager beschermingsniveau leidt dan wanneer privacy en veiligheid aan het begin van een project randvoorwaarden zijn;

*verzoekt de regering om bij de ontwikkeling van alle nieuw te starten ICT-projecten **Privacy by Design** en **Security by Design** toe te passen zodat nieuwe ICT-systemen veiliger zijn en beter berekend op misbruik en slechts privacygevoelige gegevens bevatten als dat strikt noodzakelijk is,*

en gaat over tot de orde van de dag.

Meer informatie is te vinden in het recente rapport *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* van de Canadese Information and Privacy Commissioner Ann Cavoukian, dat ook in de conclusie van deze notitie wordt behandeld.

4 Regelgeving in beweging

4.1	De vijand van privacy zijn we zelf	45
4.2	Voor 50 cent verpats ik mijn privacy	45
4.3	Privacy niet langer de sociale norm	43
4.4	Wat mag wel en wat niet?	43
4.5	Privacy & Security: New Drivers of Brand, Reputation and Action	43
4.6	Plannen goed formuleren en beredeneren	49
4.7	Richtlijnen van de OESO e.a.	50
4.8	Privacy Impact Assessment (PIA)	52
4.9	Privacy Quick Scan	52

4.1 De vijand van privacy zijn we zelf

De Amerikaanse opperrechter Alex Kozinski heeft weinig op met de schuld van verlies van privacy buiten onszelf leggen. Wat kun je anderen verwijten als we zelf een loopje met onze eigen privacy nemen? Het exhibitionistische onlinegedrag van vandaag maakt het Amerikaanse rechters steeds moeilijker om een lans te breken voor privacy. De praktijk bepaalt mede hoe de overheid en de rechtsprekende macht daarmee omgaan en als dat open en bloot is, dan is die normverandering een feitelijk gegeven.

In een Twitter-wereld waar de politie ons zomaar even pingt op de smartphone, beschouwen steeds meer mensen dat doodleuk alleen als meer volgers, aldus een ironische Kozinski op het Stanford Law Enforcement Symposium 2012 over 'privacy and its conflicting values':

The idea that law enforcement can now ping your cell phone and find out exactly where you are at any time, with no probable cause and no judicial supervision, is greeted with a big collective yawn. In a Twitter world where people clamor for attention, having the police know your whereabouts just increases your fan base.

4.2 Voor 50 cent verpats ik mijn privacy

Wat is onze privacy ons eigenlijk waard? Vijftig cent korting op een bioscoopkaartje van 7,50 is online een prima ruil voor ons telefoonnummer of e-mailadres. Dat blijkt uit de begin 2012 gepubliceerde *Study on Monetizing Privacy* van ENISA, het European Network and Information Security Agency.

Zo verschrikkelijk vinden we het in de praktijk kennelijk niet om persoonlijke informatie prijs te geven. Driekwart van de Europeanen beschouwt het in toenemende mate als een fact-of-life. Ruim 40 procent van de Europese internetgebruikers zegt



PbD-vraag 6

Is het voor stakeholders duidelijk wat u ten aanzien van privacy allemaal heeft geregeld en wat er precies in concrete gevallen gebeurt?

<http://bit.ly/vintR3Q6>

online vaak meer gegevens dan nodig te moeten vermelden en doet dat gewoon. Dat onthulde het onderzoek *Attitudes on Data Protection and Electronic Identity in the European Union* van eind 2010.

Het jaar daarop verdubbelde Facebook zijn inkomsten uit advertenties tot bijna 4 miljard dollar. Dan gaat het om 1st, 2nd en 3rd party cookies, die ons onlinegedrag op de voet volgen en waaruit munt wordt geslagen. Bewust informatie verstrekken is één, maar zonder het volledig te beseffen worden gevolgd is een vele malen groter deel van de persoonlijke-datakoek. In juni 2012 werd daarom in Nederland een strenge opt-in-cookiewet ingevoerd, om vlak voor het einde van het jaar te worden versoepeld conform de beoogde Europese norm. Want behalve privacy staan ook ondernemerschap en innovatie hoog in het vaandel. Zeker in economisch mindere tijden.

Geregeld gaan er stemmen op die zeggen dat we onze privacy maar moeten vergeten, want net als intellectueel eigendom bestaat privacy in het internettijdperk in feite niet meer. Misschien is het allemaal inderdaad niet zo belangrijk, want parallel hieraan zijn de meeste bedrijven als de dood voor reputatieschade die ontstaat als duidelijk zou worden dat ze klanten buiten hun medeweten om onder een vergrootglas houden, alleen maar om het eigen gewin te optimaliseren.

Grof gegevensmisbruik op basis van een paar simpele cookies wordt bijvoorbeeld schromelijk overdreven en een strenge opt-in-regeling is funest voor ondernemerschap. De klant is mondig genoeg, zo is nu de heersende gedachte, en als hij maar goed wordt geïnformeerd en gewezen op de opt-out-mogelijkheden, dan is dat in economisch opzicht voor iedereen het meest aantrekkelijk.

rtlnederland

RTL Nederland gebruikt cookies om haar websites te kunnen onderhouden, te ontwikkelen en te verbeteren. Cookies zijn nuttige technieken in websites die het gemak voor u als gebruiker vergroten. Wij vinden het van groot belang dat u weet welke cookies onze websites inzetten en voor welke doeleinden ze worden gebruikt. Ons doel met de cookies is het bewaken van uw privacy, het verbeteren van de gebruiksvriendelijkheid en de financiering van onze websites.

Door cookies te accepteren, krijgt u toegang tot alle websites van RTL Nederland. Klik hier voor meer informatie over de cookies die gebruikt worden door en via onze websites en voor welke doeleinden.

Ik accepteer de cookies

Ik accepteer geen cookies

[Meer weten over cookies?](#)

[Uitleg over de op de sites van RTL Nederland gebruikte cookies.](#)

4.3 Privacy niet langer de sociale norm

De eerste ontkenning van de relevantie van de digitale-privacydiscussie kwam van Scott McNealy, indertijd CEO van Sun Microsystems. ‘You already have zero privacy – get over it’, zei hij in 1999 bij de introductie van Jini, software bedoeld om een groot aantal verschillende devices aan elkaar te koppelen. Dus bijvoorbeeld, zoals tegenwoordig heel normaal is, een foto schieten die automatisch via internet wordt geüpload naar een krant om nog dezelfde dag overal ter wereld in de kiosk te liggen.

Een decennium later, aan het begin van 2010, nam Mark Zuckerberg, de CEO van Facebook, een vergelijkbare positie in door in een interview met TechCrunch te stellen dat privacy niet langer de sociale norm was. ‘Toen we zeven jaar terug begonnen met Facebook op mijn kamer in Harvard,’ zei Zuckerberg, ‘vroegen we ons af of mensen wel informatie op internet zouden gaan zetten. Maar in een paar jaar tijd zijn de normen rondom privacy compleet veranderd. En wij gaan gewoon met onze tijd mee.’

Kozinski, ENISA, McNealy en Zuckerberg komen vanuit verschillende optiek tot dezelfde slotsom: de privacyopvattingen zijn de afgelopen decennia en zelfs jaren enorm veranderd, en daarom gaat behalve de normen en waarden ook de regelgeving met die tijdgeest mee.

4.4 Wat mag wel en wat niet?

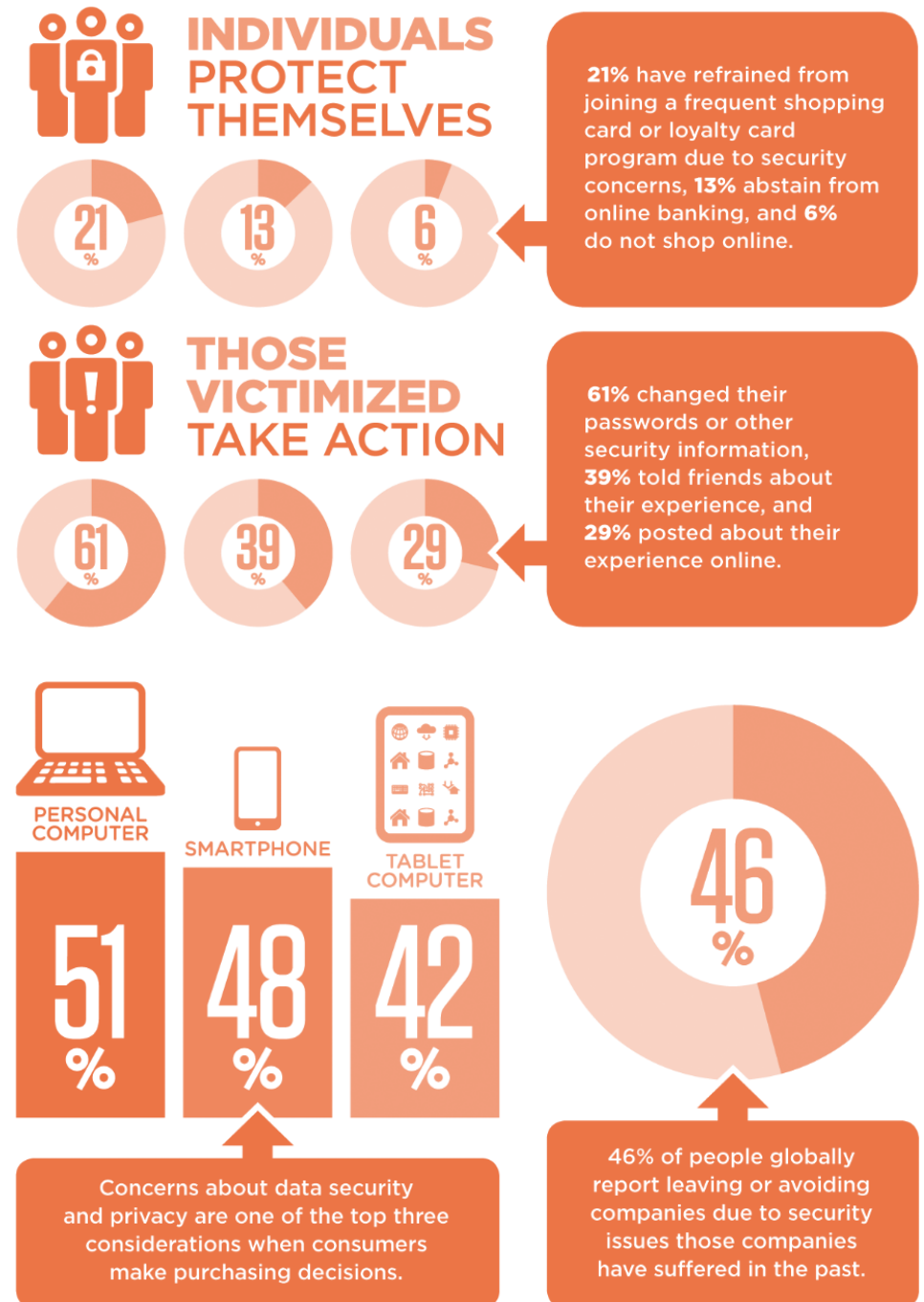
De meest praktische vraag die vanuit organisaties inzake privacy kan worden gesteld, is wat er wel en niet mag. Met allerlei waarborgen omgeven is er voor marketingdoel-einden veel toegestaan, want inperking van vrij ondernemerschap is niet het doel van privacybescherming. Mailings per post kunnen we laten stopzetten (*opt out*) en voor ongewenste telefoonmarketing is er in Nederland het wettelijke Bel-me-niet Register. Voor een beter gebruiksgemak zijn er per 1 november 2012 twee aparte websites: één voor consumenten (www.bel-me-niet.nl) en één voor adverteerders, callcenters en databewerkers (www.bedrijven-bmnr.nl).

Malafide privacypraktijken door serieuze organisaties komen in het economische verkeer eigenlijk niet voor. Dat is om te beginnen een tautologie, maar inderdaad beseffen steeds meer organisaties dit: reputatieschade loop je makkelijk op en is moeilijk te repareren. Bovendien wordt het publiek vanuit het hiervoor geschetste negatieve sentiment steeds onzekerder en handelt het bij het minste of geringste naar dat gevoel met duidelijke afweerreacties.

4.5 Privacy & Security: the New Drivers of Brand, Reputation and Action

Dat laatste blijkt zonneklaar uit de volgende infografiek van Edelman, samengesteld op basis van een survey uit 2012 onder 4050 mensen uit 7 verschillende landen. Edelman noemt privacy en security de nieuwe drivers van het merk. Privacy moet een kerncompetentie worden voor elke organisatie. Bijna de helft van alle ondervraagde

consumenten zegt bedrijven te mijden die niet goed zijn omgegaan met het beschermen van data. Het feit dat bijvoorbeeld veiligheidslekken nu heel snel viraal kunnen gaan en een berg aan negatieve publiciteit kunnen veroorzaken, is er mede debet aan dat organisaties hard aan deze nieuwe competenties moeten gaan werken.



Als er al ophef ontstaat over inbreuk op de privacy, heeft de organisatie in kwestie vrijwel altijd een verklaring paraat die zij in lijn acht met regelgeving en goede normen. Door de bank genomen wordt er in het economische verkeer heel goed nagedacht over privacyzaken. Maar tegelijkertijd is privacy vanwege high-profile Big Brother-issues een gebied van toenemende onenigheid en (over)gevoeligheid en zijn er veel 'luizen in de pels' die maar wat graag de noodklok luiden.

Zwakke beveiliging van systemen, verregaande bevoegdheden van overheden, een lappendeken van verouderde wetten en regels, acties van groepen als WikiLeaks en Anonymous, cybercrime en cyberwarfare enzovoort bepalen ontegenzeggelijk een groot deel van het sentiment rondom e-privacy en databescherming. Het is echter onterecht om dit negatieve sentiment klakkeloos door te trekken naar de dagelijkse privacypraktijk van organisaties in het economische verkeer.

In de context van onder meer de informatiemaatschappij, de Surveillance Society en Big Data is al wat raakt aan privacy momenteel sterk in beweging en worden maatregelen aangescherpt en beter gefocust. Zo is het de bedoeling dat de Europese Richtlijn, waar nationale overheden nu hun eigen privacywet- en regelgeving op baseren, in 2015 is vervangen door een harde verordening. Een algemeen geldende Europese wet kortom. Zulke uniformering is wenselijk om een economisch *level playing field* te creëren.

Echter, zonder een concrete casus is de vraag wat er op privacygebied mag en niet mag nauwelijks naar tevredenheid te beantwoorden. Ook met een casus zijn er vele afwegingen en voors en tegens in de argumentatie. Bovendien valt de huidige regelgeving niet goed uit te leggen en bevat ze gaten. Dat is het afzonderlijke oordeel van verschillende experts die we voor deze onderzoeksnotitie consulteerden.

4.6 Plannen goed formuleren en beredeneren

Wie commerciële plannen heeft, moet die om te beginnen:

1. zo precies mogelijk formuleren en idealiter ook kunnen aangeven waar men in die context over bijvoorbeeld vijf jaar wil staan.
2. Daarnaast moet worden beredeneerd waarom de beoogde acties netjes zijn en maatschappelijk verantwoord ten opzichte van de doelgroep van bijvoorbeeld klanten, personeel, prospects en suspects.
3. Vervolgens kan in samenspraak worden bekeken of er een acceptabele juridische vorm te vinden is. De doelgroep moet ten minste op de hoogte worden gebracht van de plannen (informatieplicht) en men moet doen wat er is gezegd.
4. Transparantie is dus erg belangrijk en alles wat lijkt op discriminatie en met twee maten meten, zoals *dual pricing*, moet worden vermeden.

5. Expliciet om toestemming vragen is alleen vereist in onder meer de sfeer van gezondheid en strafrecht.
6. Big Data-praktijken, zoals persoonlijke informatie bijeenbrengen vanuit allerlei verschillende bronnen en daar conclusies aan verbinden, bijvoorbeeld segmentering, moeten in elk geval goed worden uitgelegd.
7. *Straight-through processing* – gegevens verwerken zonder menselijke tussenkomst – is in het algemeen niet geoorloofd.

4.7 Richtlijnen van de OESO e.a.

Een goed universeel eerste aanknopingspunt voor de bescherming van privacy en data zijn de OESO-richtlijnen uit 1980, die kort beschreven staan op <http://oecdprivacy.org>. Deze in totaal acht *OECD Privacy Principles* betreffen achtereenvolgens:

- *Collection Limitation*: er mag niet zomaar in het wilde weg data worden verzameld, gegevens moeten rechtmatig worden verkregen, indien van toepassing met kennis of instemming van de betrokkene.
- *Data Quality*: de juistheid van de gegevens moet gegarandeerd zijn.
- *Purpose Specification*: het moet duidelijk zijn waarvoor de gegevens worden gebruikt.
- *Use Limitation*: het gebruik van de gegevens moet worden beperkt.
- *Security Safeguards*: de veiligheid van de gegevens moet zijn gegarandeerd.
- *Openness*: het moet volstrekt helder zijn welke gegevens worden verzameld en wat ermee gebeurt.
- *Individual Participation*: bij het hele proces rondom de verzameling, het gebruik enzovoort van persoonsgegevens moet het individu actief en laagdrempelig worden betrokken, opdat de betrokkene goed is geïnformeerd en kan ingrijpen.
- *Accountability*: de 'data controller' is verantwoordelijk voor de naleving van deze acht Fair Information Practice Principles (FIP'S).

In detail en in hun context zijn deze principes te raadplegen op de IT Law Wiki (http://itlaw.wikia.com/wiki/The_IT_Law_Wiki).

Samen sluit dit goed aan bij de Europese kijk op privacy. De Amerikaanse *Consumer Privacy Bill of Rights* van februari 2012 (officieel: *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*) bevat een bijlage die de eigen Fair Information Practice Principles (FIP's) vergelijkt met onder meer die van de OESO.

Een document van 119 pagina's van de Europese Commissie uit januari 2012 presenteert het zogeheten 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'. Het is de bedoeling dat dit voorstel in 2015 kracht van wet krijgt.

Op de jaarlijkse European Data Protection and Privacy Conference in 2012 zei de Amerikaanse ambassadeur William Kennard overigens dat de nieuwe databeschermingsregels van de EU de samenwerking bedreigen tussen de Europese en Amerikaanse politie en justitie, omdat honderden goed werkende opsporingsregelingen zouden moeten worden herzien.

Op de website OECDprivacy.org worden nog drie andere privacyframeworks genoemd dan de hiervoor genoemde OESO-richtlijnen, namelijk het *Asia-Pacific Economic Cooperation (APEC) Privacy Framework*, de *United States Department of Commerce Safe harbor* (zie par. 4.7) *Privacy Principles* en de *Generally Accepted Privacy Principles (GAPP)*. De wereldwijde trend inzake privacy- en securityregelgeving is die van harmonisering, uniformering en standaardisering.

Het **US-EU Safe Harbor-verdrag** is bedoeld om Amerikaanse organisaties te helpen voldoen aan de EU-regels inzake de bescherming van persoonlijke data. Het bevat onder meer checklists, zelf-certificatie en een werkboek. De kern zijn de volgende zeven Safe Harbor-principes:

- *Notice*: individuen moet worden verteld dat hun gegevens worden verzameld en hoe die worden gebruikt.
- *Choice*: individuen moeten de gelegenheid hebben de verzameling van hun gegevens en de overdracht daarvan aan derde partijen te blokkeren.
- *Onward Transfer*: de overdracht van gegevens aan derde partijen mag alleen plaatsvinden als die de data goed beveiligen.
- *Security*: verlies van verzamelde informatie moet worden voorkomen door deugdelijke maatregelen.
- *Data Integrity*: de gegevens moeten relevant zijn en betrouwbaar in relatie tot waarvoor ze worden gebruikt.
- *Access*: individuen moeten toegang kunnen hebben tot de verzamelde informatie en foutieve gegevens kunnen corrigeren of verwijderen.
- *Enforcement*: deze regels moeten effectief worden gehandhaafd.

Dat ziet er mooi uit maar na twee negatieve reviews door de Europese Unie in 2002 en 2004 oordeelde Galexia in 2008 zelfs het volgende:

The growing number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers.

De genoemde OESO-richtlijnen heten officieel de *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. De complete tekst staat in de documenten onder het kopje 'Information security and privacy', een onderwerp in de sectie 'Internet economy' op de website.

4.8 Privacy Impact Assessment (PIA)

Om het thema privacy en security praktisch te houden kan er een *Privacy Impact Assessment* (PIA) worden gehouden om vooraf de risico's van plannen bij uitvoering duidelijk te maken. Onder meer het Britse Information Commissioner's Office heeft een *PIA Handbook* en onderscheidt de volgende negen stappen:

- ◆ belanghebbenden in kaart brengen;
- ◆ initiële beoordeling privacyrisico's;
- ◆ besluit over de diepgang van de PIA;
- ◆ privacyrisico's in kaart brengen;
- ◆ overleggen met belanghebbenden;
- ◆ voorstellen doen voor acceptatie;
- ◆ risico's verzachten of vermijden;
- ◆ compliance nalopen;
- ◆ een review plannen.

De review bekijkt de genomen acties en de effecten, wat kan leiden tot een uitgebreidere of nieuwe PIA.



PbD-vraag 7
Vertrouwen staat bij privacyvraagstukken voorop. Stelt u de interactie met individuen voldoende centraal?

<http://bit.ly/vintR3Q7>

4.9 Privacy Quick Scan

VNO-NCW en MKB-Nederland vinden een PIA vaak een te zwaar en onwerkbaar instrument. Die ervaring deed men op bij het opstellen van een PIA door het College bescherming persoonsgegevens (Cbp). In een brief, begin september 2011, aan de Vaste Tweede Kamer-commissie voor Veiligheid en Justitie stellen VNO-NCW en MKB-Nederland dat het bedrijfsleven het meeste baat heeft bij een handzame *Privacy Quick Scan*. Daarmee kunnen bedrijven een eerste inschatting maken van de privacy-effecten van een dienst of product voor hun bedrijf en klanten of werknemers. Ook zo'n Privacy Quick Scan heeft kennelijk flink wat voeten in de aarde. Op de website <http://privacyimpactassessment.nl/QuickScan.html> ('Doe hier gratis een Quick Scan van uw privacyrisico's') staat namelijk nu nog het volgende:

Wij zijn momenteel nog druk bezig om de Privacy Quick Scan te bouwen, dus wij vragen nog even uw geduld.

Inmiddels is er een Nederlandse privacy-checker online, die op verschillende vraagstukken antwoord geeft, zie paragraaf 1.1.

Conclusie

Privacy is een begrip uit de vijftiende eeuw, maar in de eerste eeuw voor Christus zei Publilius Syrus al dat we ons niet moeten afgeven met 'vrienden' die onze privé-zaken aan de grote klok hangen. Dat is een mooie boodschap in deze tijd van sociale media. Het toont aan dat privacy van alle tijden is en verbonden is met de individualiteit die elk mens als redenerend wezen eigen is.

Iedereen is kieskeurig als het om zijn of haar privacy gaat. Van oudsher is dan het mijn, het dijn en ons privé-terrein in het geding, maar digitale privacy is wel een bijzonder ambivalente zaak. Als we bijvoorbeeld door informatiesystemen zijn geormerkt als minder kredietwaardig, dan kan dat heel langdurige gevolgen hebben, zo heeft de praktijk keer op keer uitgewezen. Het concept van digitaal DNA krijgt daarmee een wrange bijmaak.

Privacyschandalen hebben een lange halfwaardetijd: we blijven achterdochtig. Want te vaak is het toch weer op de een of andere manier fout gegaan. Statistisch gezien is het misschien als met de wijzen die alle vragen van één gek niet kunnen beantwoorden of zijn fundamentele wantrouwen kunnen wegnemen. Maar wat de aandacht heeft, beklijft, zeker bij gebrek aan systematische duidelijkheid.

Iedereen is zich er momenteel zeer van bewust dat privacy, technologie en regelgeving de drie-eenheid zijn die voldoende duidelijkheid en zekerheid zou moeten kunnen verschaffen om een betere sociale en economische digitale wereld te bewerkstelligen. Een integrale benadering van Privacy by Design zal uiteindelijk het vertrouwen moeten winnen op basis waarvan de vruchten van een digitale economie kunnen worden geoogst.

De ontwikkeling van Big Data en haar toepassingen zet de urgentie hiervan op scherp, zowel aan de kant van de angst als die van de hoop, de ambitie. Bij alle complexiteit en twijfel wordt steeds duidelijker dat alleen een concrete en integrale Privacy by Design-aanpak soelaas kan bieden. Maar vanwege de onophoudelijke reeks van privacy-inbreuken zullen zorg en wantrouwen de boventoon blijven voeren.

Dat is een existentieel gegeven, want privacy is geworteld in de eenzaamheid van het individu. Rationeel culmineert zij in de methodische twijfel van de verlichtingsfilosoof Descartes: wantrouwen is onze levenshouding. Big Data-gewin voor iedereen veronderstelt in feite een mathematische bewijsvoering, maar die kan er niet komen en zo ze er zou zijn, zou slechts een minderheid haar begrijpen.

Het fundamentele trade-offkarakter van privacy maakt consensus onmogelijk. Maar precies daar begint het eerlijke spel van de economische potentie voor iedereen. Zoals aan het begin van deze notitie gezegd, is digitale privacy namelijk het vermogen om

sociaal-economische relaties uit te onderhandelen op basis van controle over de eigen persoonlijke informatie.

In toenemende mate geven regelgeving, beleid en technologie vorm aan de relaties die individuen hebben met organisaties, met overheden en met elkaar. Inzake privacy biedt dit nieuwe uitdagingen maar ook kansen. Daarom moet er een nieuw conceptueel raamwerk komen voor enerzijds de analyse van het privacybeleid en anderzijds het ontwerp en de ontwikkeling van dataverwerkende systemen.

In dat verband is de redenering als volgt: Big Data is een realiteit, daar zit bijzonder veel waarde in, maar Big Data voedt ook het onbehagen inzake privacy. Tussen organisaties en individuen moeten we hier een goede balans in zien te creëren. Privacy by Design, Privacy-Enhancing Technologies, gestandaardiseerde regelgeving plus het bijbehorende verantwoordelijke gedrag zijn de integrale aanpak die Big Data-gewin voor iedereen mogelijk moet maken.

De inleiding van deze notitie schetst al hoe de economie van persoonlijke informatie werkt. Over ons allemaal worden door uiteenlopende organisaties gegevens verzameld die via verschillende typen informatiemakelaars overal en nergens terechtkomen, zoals bij banken, marketeers, media, overheden, juridische organisaties, individuen, wetshandhavers en werkgevers. Alleen organisaties die uitsluitend privacyneutrale informatie verzamelen van minder dan vijfduizend mensen per jaar en die data op geen enkele manier delen met derden, vallen buiten dit ecosysteem, aldus de Amerikaanse Federal Trade Commission. Alle andere partijen moeten serieus aandacht besteden aan de implementatie van Privacy by Design en aan simpele keuzemogelijkheden voor consumenten en moeten blijven werken aan hun transparantie naar de markt.

Omdat privacy, databescherming en persoonlijke informatie zo'n grote economische en relationele waarde vertegenwoordigen, moeten organisaties Privacy by Design operationaliseren vanuit de volgende zeven basisprincipes:

1 Privacy by Design betekent dat u proactief en preventief te werk gaat: niet reactief, niet repareren achteraf

Probeer dus zoveel mogelijk te anticiperen op zogeheten *privacy-invasive* gebeurtenissen en voorkom ze vooral. Wacht niet totdat een privacy-inbreuk zich voordoet.

2 Privacygarantie moet de defaultinstelling zijn

U wilt voor individuen de maximale privacy garanderen en zorgen dat persoonlijke informatie automatisch veilig is in elk ICT-systeem en elke business-

praktijk. Individuen moeten zich hier niet om hoeven te bekommeren of actie te hoeven ondernemen.

3 Privacy moet ingebakken zijn in het ontwerp

Privacy-requirements moeten vanaf het begin integraal deel uitmaken van het ontwerp en de architectuur van ICT-systemen en businesspraktijken. Privacy is een essentiële component van de functionaliteit die wordt geleverd.

4 Ga voor volledige functionaliteit: geen magere trade-off maar een duidelijk positieve balans

Pak de legitieme privacybelangen en -doelstellingen op als een win-winsituatie. Vermijd valse tegenstellingen als privacy versus security en toon aan dat ze allebei tegelijk mogelijk zijn.

5 Oplossingen moeten helemaal dichtgetimmerd zijn: end-to-end security door de tijd heen

Security is een centraal element. Tot databescherming behoort ook dat aan het einde van een proces of andere levenscyclus alle gegevens veilig en op het gewenste tijdstip kunnen worden vernietigd.

6 Zorg voor zichtbaarheid en transparantie: openheid is uw leidmotief

Ten aanzien van alle businesspraktijken en ICT-oplossingen moet het voor stakeholders duidelijk zijn wat er precies gebeurt. Wie dat wil controleren moet dat te allen tijde kunnen doen.

7 Ga respectvol om met privacy: stel dus vooral het individu centraal

Sterke privacy-defaults, op het juiste moment duidelijk maken wat er gebeurt en gebruiksvriendelijke keuzemogelijkheden voor individuen zijn onontbeerlijk voor een goede vertrouwensrelatie. De interactie is daarbij doorslaggevend.

Deze principes betreffen de kern van elke organisatie, namelijk digitale technologie, ontwerp en infrastructuur plus de operatie zelf. In het rapport *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* uit december 2012 zijn ze verder toegelicht en uitgewerkt, compleet met acties en verantwoordelijkheden in de organisatie voor directie, softwarearchitecten, developers, business-line-eigenaren en eigenaren van applicaties. Ook vindt u er specifieke voorbeelden, onder meer voor de zorg en de energiesector, plus voor technologieën als camerabewaking en near-fieldcommunicatie (tap & go).

Literatuur en afbeeldingen

- Agre, P.E. & M. Rotenberg (1997): *Technology and Privacy: The New Landscape*, <http://polaris.gseis.ucla.edu/pagre/landscape.html>
- Alessandro Acquisti, A. (2010): 'The Economics of Personal Data and The Economics of Privacy', <http://www.oecd.org/sti/interneteconomy/46968784.pdf>, http://www.heinz.cmu.edu/~acquisti/papers/acquisti_privacy_economics.ppt
- Alvaro, A. (2012): *Lifecycle Data Protection Management: A contribution on how to adjust European data protection to the needs of the 21st century*, <http://www.alexander-alvaro.de/wp-content/uploads/2012/10/Alexander-Alvaro-LIFECYCLE-DATA-PROTECTION-MANAGEMENT.pdf>
- Asimov, I. (1951): *Foundations*
- Berin Szoka (2009): *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, <http://ftc.gov/os/comments/privacyroundtable/544506-00035.pdf>
- Bradbury, R. (1951): *Fahrenheit 451*
- Burkert, H. (1997): 'Privacy-Enhancing Technologies: Typology, Vision, Critique', <http://books.google.nl/books?id=H2KB2DK4W78C&pg=PA125>
- Bygrave, L.A. (2002): 'Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place', http://folk.uio.no/lee/publications/PETS_speech.pdf
- Cavoukian, A. (2009): 'Privacy by Design: The 7 Foundational Principles', <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>
- Cavoukian, A. (2012): *Operationalizing Privacy by Design. A Guide to Implementing Strong Privacy Practices*, <http://privacybydesign.ca/content/uploads/2012/12/operationalizing-pbd-guide.pdf>
- Cavoukian, A. & J. Jonas (2012): *Privacy by Design in the Age of Big Data*, http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf
- Center for Internet and Society PET wiki: <http://cyberlaw.stanford.edu/wiki/index.php/PET>
- Clarke, R. (1995-2013): *Dataveillance & Information Privacy*, <http://www.rogerclarke.com/DV>
- Clarke, R. (2001): 'Introducing PITS and PETS: Technologies Affecting Privacy', <http://www.rogerclarke.com/DV/PITSPETS.html>
- Clinton, W.J. & A. Gore (1997): 'A Framework voor Global Electronic Commerce', <http://clinton4.nara.gov/WH/New/Commerce/read.html>
- Cloud Security Alliance (2012): *Top Ten Big Data Security and Privacy Challenges*, https://downloads.cloudsecurityalliance.org/initiatives/bdvwg/Big_Data_Top_Ten_v1.pdf
- Computers, Privacy & Data Protection (2013): 'Reloading Data Protection', <http://www.cdpconferences.org/sponsors.html>
- Considerati (2013): *Privacychecker*, <http://privacychecker.nl>
- Coueignoux, P. (2006): 'Liabilities and Vulnerabilities in the Information Age', <http://www.eprivacy.com/lectures/toc.html>

- Coueignoux, P. (2012): 'The Privacy Tax. Open letter to Barack Obama and Herman van Rompuy', <http://www.cawa.fr/the-privacy-tax-article005879.html>
- Coueignoux, P. (2013): ePrio, trustworthy social eCommerce, <http://eprivacy.com>
- Cyberspace Law and Policy Centre (2008): *Distinguishing PETS from PITS: Developing technology with privacy in mind*, http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_DP72_Technology_final.pdf
- Daniel P. (2013): 'Abine's DeleteMe app review: deal with personal info databases from the comfort of your phone', http://www.phonearena.com/news/Abines-DeleteMe-app-review-deal-with-personal-info-databases-from-the-comfort-of-your-phone_id38722
- De Wereld Draait Door (2012): 'Doorstart EPD: Wilna Wind en Alexander Klöpping', <http://dewerelddraaitdoor.vara.nl/media/197890>
- Department of Defense (2013): Personally Identifiable Information Course Module, http://iase.disa.mil/eta/pii/pii_module/pii_module/index.html
- Department of Health, Education and Welfare (1973): 'The Code of Fair Information Practices', http://epic.org/privacy/consumer/code_fair_info.html
- Department of Homeland Security (2011): *Handbook for Safeguarding Sensitive Personally Identifiable Information At The DHS*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_sp11_handbook.pdf
- Diploma of Information Technology, Knowledge Management (2012): 'Types of Privacy', http://toolboxes.flexiblelearning.net.au/demosites/series4/411/content/privacy/types_of_privacy.htm
- Duhigg, C. (2012): 'How Companies Learn Your Secrets', <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>
- Edelman (2012): 'Privacy & Security: The New Drivers of Brand, Reputation and Action. Global Insights 2012', http://edelmaneditions.com/wp-content/uploads/2012/03/Data-Security-Privacy-Infographic_Final.png
- Electronics Weekly (2010): 'Electroon #9 - "Computer says No" (1960)', <http://www.electronics-weekly.com/blogs/electronics-weekly-blog/2010/09/electroon-9---computer-says-no.html>
- Elissen, A. et al. (2011): 'Gewijzigde motie Elissen c.s. over privacy van design en safety by design (ter vervanging van 26643, nr. 203) - Informatie- en communicatietechnologie (ICT)', http://www.europa-nu.nl/id/vitwlyaaklx7/gewijzigde_motie_elissen_c_s_over
- Ellis Smith, R. (2004): *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, http://www.privacyjournal.net/_center_ben_franklin_s_web_site__privacy_and_curiosity_from_plymouth_rock_to_the_3087.htm
- ENISA (2012): *Study on monetising privacy: An economic model for pricing personal information*, <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy>
- European Commission (2010,2011): *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
- Europese Commissie (2012): *Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming)*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:>

- 2012:0011:FIN:NL:PDF http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- Export.gov (2012): U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, <http://export.gov/safeharbor>
- Fair Information Practice Principles, FIPs (1973, 1980), http://simson.net/ref/2004/csg357/handouts/o1_fips.pdf
- Federal Trade Commission (2012): Fair Information Practice Principles, <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>
- Federal Trade Commission (2012): *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers*, <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>
- Fielder, A. (2013): 'European Parliament committees threaten wholesale destruction of privacy and data protection rights', <https://www.privacyinternational.org/blog/european-parliament-committees-threaten-wholesale-destruction-of-privacy-and-data-protection>
- Foremski, T. (2011): 'SFCurators: Our Public, Private, And Secret Lives...'; http://www.siliconvalleywatcher.com/mt/archives/2011/07/sfcurators_our.php
- Frankfurter Allgemeine (2011): 'Der deutsche Staatstrojaner wurde geknackt', <http://www.faz.net/aktuell/chaos-computer-club-der-deutsche-staatstrojaner-wurde-geknackt-11486538.html>
- Galexia (2008): 'The US Safe Harbor – Fact or Fiction?', http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction-Recommend.html
- Garfinkel, S. (2001): *Database Nation. The End of Privacy in the 21st Century*
- Gerber, B. (2009, 2010): OECD Privacy Principles, <http://oecdprivacy.org>
- Gorodyansky, D. (2013): 'It's Data Privacy Day: 3 Things You Must Do', <http://www.inc.com/david-gorodyansky/3-ways-to-go-all-out-this-data-privacy-day.html>
- Greenberg, A. (2008): 'The Privacy Paradox', http://www.forbes.com/2008/02/15/search-privacy-ask-tech-security-cx_ag_0215search.html
- Hagel, J. (2012): 'The Rise of Vendor Relationship Management', http://edgeperspectives.typepad.com/edge_perspectives/2012/06/the-rise-of-vendor-relationship-management.html
- Hamlin, K. (2012): 'Personal Data List in Mind Map Form', <http://www.identitywoman.net/personal-data-list-in-mind-map-form>
- Hirschleifer, J. (1979): *Privacy: Its Origin, Function, and Future*, <http://www.econ.ucla.edu/workingpapers/wp166.pdf>
- HP Laboratories (2011): *Privacy-Enhancing Technologies: A Review*, <http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf>
- Huffington Post (2010): 'Facebook's Zuckerberg Says Privacy No Longer A "Social Norm"' (video), http://www.huffingtonpost.com/2010/01/11/facebooks-zuckerberg-the_n_417969.html

- Human Rights Council (2012): Resolution A/HRC/20/L.13: The promotion, protection and enjoyment of human rights on the Internet, <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf>
- Huxley, A. (1932): *Brave New World*
- ICT Issues, een Business Issues-kennisbank (2013): Quickscan Wet bescherming persoonsgegevens, <http://www.ictforyourbusiness.nl/?ContentId=2279>
- Information Commissioner's Office (1998): 'Data protection principles', http://www.ico.gov.uk/for_organisations/data_protection/the_guide/the_principles.aspx
- Information Commissioner's Office (2013): 'Privacy impact assessment (PIA)', http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx
- Internationaal privacykader (2013): http://www.cbpweb.nl/Pages/ind_wetten_int.aspx
- IT Law Wiki (2013): 'Privacy-Enhancing Technologies' [incl. UK ICO & EU], http://itlaw.wikia.com/wiki/Privacy%E2%80%90enhancing_technologies
- IT Law Wiki (2013): 'The IT Law Wiki', http://itlaw.wikia.com/wiki/The_IT_Law_Wiki
- Johnson, H. (2013): 'The Application Privacy, Protection, and Security (APPS) Act of 2013', <http://apprights-hankjohnson.house.gov/2013/01/apps-act.shtml>
- Kennard, W.E. (2012): 'Remarks by U.S. Ambassador to the EU, William E. Kennard, at Forum Europe's 3rd Annual European Data Protection and Privacy Conference', http://useu.usmission.gov/kennard_120412.html
- Koorn, R.F. & J. ter Hart (2011): 'Privacy by Design: From privacy policy to privacy-enhancing technologies', <http://www.compact.nl/artikelen/C-2011-o-Koorn.htm>
- Kozinski, A. (2012): 'The Dead Past', <http://www.stanfordlawreview.org/online/privacy-paradox/dead-past>
- Kuner, C. et al. (2012): 'The Challenge of Big Data for Data Protection', <http://idpl.oxfordjournals.org/content/2/2/47.extract>
- Kuneva, M. (2009): Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling, http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm
- Lee, F. (2006): *An Investigation of Privacy Tradeoff on the Internet*, http://citebm.business.illinois.edu/twc%20class/project_reports_spring2006/privacy%20issues/lee/internet_privacy_fei.pdf
- Lynley, N. (2013): 'A Palantir Founder Suggests His Startup Is Worth About \$8 Billion', <http://blogs.wsj.com/digits/2013/01/16/a-palantir-founder-suggests-his-startup-is-worth-about-8-billion>
- Mackay, S. (2012): "'Apps" and Big Data and Privacy – An Oxymoron?', <http://ediscoverytalk.blogs.xerox.com/2012/12/10/apps-and-big-data-and-privacy-an-oxymoron>
- Magenta Advisory (2012): 'Wise use of consumer data enables to improve companies' performance and creates possibilities for new services and solutions', <http://www.magentaadvisory.com/2012/09/12/wise-use-of-consumer-data-enables-to-improve-companies-performance-and-creates-possibilities-for-new-services-and-solutions/>
- Microsoft (2012): *Differential Privacy for Everyone*, <http://www.microsoft.com/en-us/download/details.aspx?id=35409>

- Microsoft HealthVault: <http://www.healthvault.me/>, <https://www.healthvault.com/nl/nl>, <http://www.microsoft.com/health/en-us/products/Pages/healthvault.aspx>
- Microsoft HealthVault Ecosystem: http://www.netsoft-usa.com/images/img_medtracker_HealthVaultFuture.png
- MozillaWiki (2011): Privacy Icons project (beta release), https://wiki.mozilla.org/Privacy_Icons
- Mulligan, D. (2012): 'Bridging the Gap between Privacy and Design', <http://www.law.berkeley.edu/14542.htm>
- Nader, R. (1965): 'Unsafe at Any Speed', <http://www.nndb.com/people/788/000023719/>
- National Institute of Standards and Technology (2010): *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
- OECD (2013): 'Information security and privacy', <http://www.oecd.org/sti/interneteconomy/informationsecurityandprivacy.htm>
- Olsson, M. (2012): 'NSA Building A \$2 Billion Quantum Computer Artificial Intelligence Spy Center', <http://mind-computer.com/2012/05/13/nsa-building-a-2-billion-quantum-computer-artificial-intelligence-spy-center>
- Öman, S. (2004): *Implementing Data Protection in Law*, <http://www.scandinavianlaw.se/pdf/47-18.pdf>
- OpenLearn (2012): 'Secret or sharing? Play our Privacy Game', <http://www.open.edu/openlearn/privacy>
- Orwell, G. (1948): *1984*
- Out-law.com (2012): 'Smart meter technology is privacy intrusive', <http://www.out-law.com/en/articles/2012/january-/smart-meter-technology-is-privacy-intrusive-researchers-claim>
- Packard, V. (1964): *The Naked Society*, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=3842&context=fss_papers
- PISA Consortium (2003): *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*, http://www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf
- Pratt, W.F. (1979): *Privacy in Britain*, <http://books.google.nl/books?id=GDjNgEgw2fgC>
- 'Privacy & Free Speech: It's Good for Business', <http://www.dotrights.org/business/primer>
- Privacy by Design (2013), <http://www.privacybydesign.ca>
- Privacy Impact Assessment .nl (2013): Privacy Quick Scan, <http://privacyimpactassessment.nl/QuickScan.html>
- Privacy, Technology and the Law, <http://www.judiciary.senate.gov/about/subcommittees/privacytechnology.cfm>
- Rand, A. (1943): *The Fountainhead*
- Reyburn, S. (2012): 'ACT debuts the App Privacy Icons', <http://www.insidemobileapps.com/2012/10/04/act-debuts-the-app-privacy-icons/>
- Rosen, J. (2012): 'The Right to Be Forgotten', <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>

- Rousseau, J.-J. (1754): *Discourse on the Origin and Basis of Inequality among Men*
- RT, Russia Today (2012): 'NSA refuses to disclose its links with Google', <http://rt.com/usa/nsa-epic-foia-court-413>
- RTL Z (2013): 'Privacy op internet niet goed beschermd', <http://www.rtl.nl/components/financien/rtlz/nieuws/2013/03/privacy-op-internet-niet-goed-beschermd.xml>
- Rubinstein, I. (2011): *Regulating Privacy By Design*, https://www.privacyassociation.org/media/pdf/knowledge_center/Regulating_privacy_by_design.pdf
- Rubinstein, I. (2012, 2013): *Big Data: The End of Privacy or a New Beginning?*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659
- Schoen, S. (2009): 'What Information is "Personally Identifiable"?' <https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable>
- Searls, D. (2010): 'Do we have to "trade off" privacy?', <http://blogs.law.harvard.edu/vrm/2010/09/19/do-we-have-to-trade-off-privacy>
- Sengupta, S. (2012): 'Building an Iconography for Digital Privacy', <http://bits.blogs.nytimes.com/2012/11/19/building-an-iconography-for-digital-privacy>
- Smith (2012): 'Digital privacy in the big data era: Microsoft's data protection keynote', <http://www.networkworld.com/community/blog/digital-privacy-big-data-era-microsofts-data-protection-keynote>
- Sogeti VINT (2012, 2013): vier Big Data-onderzoeksnotities, <http://vint.sogeti.com/bigdata>
- Solove, D.J. (2006): *A Taxonomy of Privacy*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622
- Solove, D.J. (2011): *Nothing to Hide: the False Trade-off between Privacy and Security*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1827982
- Solove, D.J. & P.M. Schwartz. (2011): *Privacy Law Fundamentals*, https://www.privacyassociation.org/media/pdf/publications/PLF_TOC.pdf, 'Chapter 1: An Overview of Privacy Law in all its varied types and forms and a timeline with key points in the development of privacy law', https://www.privacyassociation.org/media/pdf/publications/PLF_Chap_1.pdf
- South Australian Law Reform Institute (2012): *Computer says no. Modernisation of South Australian evidence law to deal with new technologies*, <http://www.law.adelaide.edu.au/reform/downloads/issues-paper-1-computer-says-no.pdf>
- Spiegel, Der (2012): 'Surfing for Details: German Agency to Mine Facebook to Assess Credit-worthiness', <http://www.spiegel.de/international/germany/german-credit-agency-plans-to-analyze-individual-facebook-pages-a-837539.html>
- Strahilevitz, L.J. (2004): *A Social Networks Theory of Privacy*, <http://www.law.uchicago.edu/files/files/230-ljs-privacy.pdf>
- Surveillance Studies Network (2006): *A Report on the Surveillance Society for the Information Commissioner*, http://www.surveillance-studies.net/?page_id=3
- Tavani, H. & D. Vance (1996): 'Chapter 4.3 Computers and Privacy', <http://home.aisnet.org/displaycommon.cfm?an=1&subarticlenbr=633>
- Tene, O. & J. Polonetsky (2012): *Big Data for All: Privacy and User Control in the Age of Analytics*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364

- Tene, O. & J. Polonetsky (2012): 'Privacy in the Age of Big Data: A Time for Big Decisions', <http://www.stanfordlawreview.org/online/privacy-paradox/big-data>
- TNO, TILT (2011): *Trusted Technology. Een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid*, <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/12/05/trusted-technology-een-onderzoek-naar-de-toepassingsvoorwaarden-voor-privacy-by-design-in-de-elektronische-dienstverlening-van-de-overheid.html>
- Tompor, S. (1994): 'The Credit Report from Hell', http://www.recordnet.com/apps/pbcs.dll/article?AID=/19940801/A_NEWS/308019321
- TrendLabs (2012): *Be Privy to Online Privacy*, <http://about-threats.trendmicro.com/ebooks/be-privy-to-online-privacy/files/assets/downloads/publication.pdf>
- Upshure, R.E.G. et al. (2001): 'The privacy paradox: laying Orwell's ghost to rest', <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC81333>
- Verenigde Naties (1948): Universele Verklaring van de Rechten van de Mens, artikel 12, <http://www.un.org/en/documents/udhr/index.shtml#a12>
- Vitaliev, D. (2011): 'Data Protection and Privacy', <http://dmitri.vitaliev.info/data-protection-and-privacy>
- VNO NCW (2011): Brief: Kabinetsnotitie Privacy met o.m. Privacy Quick Scan (PIA), <http://www.vno-ncw.nl/SiteCollectionDocuments/Brieven/brief11-11507.pdf>
- Warren, S. & L. Brandeis (1890): 'The Right to Privacy', http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
- Westin, A.F. (1967): 'Privacy and Freedom', <http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlur>
- Westin, A.F. & M.A. Baker (1972): *Databanks in a Free Society. Computers, Record-keeping, and Privacy*
- Wet bescherming persoonsgegevens (2013), http://www.cbpreweb.nl/pages/ind_wetten_wbp.aspx
- White House, The (2012): *Consumer Data Privacy in a Networked World. A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>
- Wolfensberger, D.R. (2006): 'Congress and the Right to Privacy', <http://www.wilsoncenter.org/sites/default/files/privacy-essay-drw4.pdf>
- World Economic Forum (2011): *Personal Data: The Emergence of a New Asset Class*, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf
- World Economic Forum, Boston Consulting Group (2013): *Unlocking the Value of Personal Data: From Collection to Usage*, <http://www.weforum.org/issues/rethinking-personal-data>
- Zamyatin, Y. (1924): *We*

Privacy prima, en wat nu ...?

- Voor een overall beeld van digitale privacy voor uw business kunt u op onder meer de twee volgende plekken online informatie inwinnen: op www.privacychecker.nl en op www.ictforyourbusiness.nl/?ContentId=2279. De privacychecker betreft consequenties vanuit de huidige Wet bescherming persoonsgegevens én vanuit de beoogde algemene Europese privacyverordening. Die wordt mogelijk al in 2015 van kracht. Op de website www.ictforyourbusiness.nl treft u op de genoemde pagina een specifieke ICT-quickscan aan op basis van dertien vragen, gerelateerd aan de Wet bescherming persoonsgegevens.
- In deze onderzoeksnotitie treft u in hoofdstuk 4 onder meer de suggestie aan om een *Privacy Impact Assessment* (PIA) te houden.
- De structurele ontwikkeling van omgaan met privacy als economische katalysator heet *Privacy by Design* (PbD). Over het nut van deze oplossingsrichting bestaat een hoge mate van consensus. Privacy by Design is in de conclusie van deze notitie geoperationaliseerd aan de hand van zeven aanbevelingen. Om u door de onderzoeksnotitie heen alvast in die richting te leiden zijn de zeven aanbevelingen voor Privacy by Design ook opgenomen als vragen in de kantlijn.

(NB: lees verder op de achterzijde.)

Over Sogeti

Sogeti is een toonaangevende speler op het gebied van professionele ICT-dienstverlening, gespecialiseerd in applicatiemanagement, infrastructuurmanagement, high-tech engineering en testen. Sogeti werkt nauw samen met haar opdrachtgevers en maakt technologische innovatie mogelijk dankzij maximale resultaten. Bij Sogeti werken meer dan 20.000 professionals, verspreid over ruim 15 landen en meer dan 100 locaties in Europa, de VS en India.

Over VINT

Alle ontwikkelingen volgen op ICT-gebied is voor veel organisaties een zware opgave. Vaak staan nieuwe ICT-mogelijkheden immers ver af van het primaire bedrijfsproces. Bronnen die deze ontwikkelingen inzichtelijk en pragmatisch benaderen, door ook het mogelijke gebruik te belichten, zijn dun gezaaid. VINT, het Verkenningsinstituut Nieuwe Technologie van Sogeti, geeft invulling aan die koppeling tussen bedrijfsprocessen en nieuwe ICT.

In elke rapportage over een verkenning die het instituut heeft uitgevoerd, zoekt VINT het juiste midden tussen feitelijke beschrijving en beoogde toepassing. Op die manier inspireert VINT organisaties om nieuwe technologie in beschouwing te nemen of zelfs te gaan gebruiken.

Privacy prima, en wat nu ...?

(Privacy by Design (PbD) – vervolg van de vorige pagina)

<http://bit.ly/vintR3Q1>

PbD-vraag 1

Heeft u wel eens te maken gehad met privacy-issues? Een Privacy by Design-aanpak (PbD) is nadrukkelijk bedoeld om dat te voorkomen.

<http://bit.ly/vintR3Q2>

PbD-vraag 2

Is persoonlijke informatie in uw ICT-systemen automatisch veilig, zodat niemand zich daarom hoeft te bekommeren?

<http://bit.ly/vintR3Q3>

PbD-vraag 3

Maken privacy-requirements integraal deel uit van het ontwerp en de architectuur van uw ICT-systemen en businesspraktijken?

<http://bit.ly/vintR3Q4>

PbD-vraag 4

Hoe gaat u om met privacy versus security? Denkt u dat ze allebei in harmonie gerealiseerd kunnen worden?

<http://bit.ly/vintR3Q5>

PbD-vraag 5

Denkt u er bij databescherming ook aan dat informatie op een bepaald tijdstip veilig moet kunnen worden vernietigd?

<http://bit.ly/vintR3Q6>

PbD-vraag 6

Is het voor stakeholders duidelijk wat u ten aanzien van privacy allemaal heeft geregeld en wat er precies in concrete gevallen gebeurt?

<http://bit.ly/vintR3Q7>

PbD-vraag 7

Vertrouwen staat bij privacyvraagstukken voorop. Stelt u de interactie met individuen voldoende centraal?

Doe mee aan onze Big Data-discussie op www.sogeti.com/vint/bigdata/questions

