# MEER CONTROLE DOOR BURGERS

## OVER HUN PERSOONSGEGEVENS

Rapport voor het Bureau Verkenningen en Onderzoek

Ministerie van Binnenlandse Zaken

Den Haag, maart 2015

**Mw. Prof. Dr. E.A. van Zoonen**

**Mw. H. van der Meulen (BA)**

## Contact:

Prof. Dr. E.A. van Zoonen

Afdeling Sociologie
Faculteit der Sociale Wetenschappen
Burgemeester Oudlaan 50
3062 PA Rotterdam

Email: vanzoonen@fsw.eur.nl

# INHOUDSOPGAVE

# MANAGEMENTSAMENVATTING EN AANBEVELINGEN

## 1. INLEIDING

Het Bureau Verkenningen en Onderzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is geïnteresseerd in de volgende vraag:

*Wat is vanuit een sociaal psychologisch perspectief de betekenis van meer controle door de burger (inzicht, toestemming verlenen, beheer) over zijn persoonsgegevens bij de overheid voor de steun van integrale persoonsverwerkende datasystemen van de overheid van de burger?*

Deze vraag wordt gesteld in de context van een sterke wens vanuit overheid en bedrijfsleven om meer, efficiënter en doelgerichter van allerlei soorten data gebruik te maken, en een sterke zorg van burgers over hun privacy ten opzichte van beide partijen.

De rapportage is gebaseerd op literatuurstudie, secundaire analyse van survey-gegevens uit 2010, en expertgesprekken.

## 2. OMGEVING

Recente ontwikkelingen maken het mogelijk om van een zich snel ontwikkelend 'data-veld' te spreken waarin talloze commerciële partijen met wisselend success proberen nieuwe manieren en technologieën te ontwikkelen die de privacy beschermen en burgers controle geven over hun eigen data. Het is in dit veld vaak onduidelijk wat een hype is en wat een reële ontwikkeling.

***De overheid dient zich in dit veld afwachtend op te stellen en zich te concentreren op het definiëren van kaders. Als de overheid zich als speler opstelt die meedoet aan het ontwikkelen en implementeren van nieuwe oplossingen, is het risico te groot dat ze meegesleurd wordt in de afwisseling van succes en mislukking die dit veld kenmerkt. Dit zal potentieel tot een afname van vertrouwen in de overheid leiden.***

## 3. BESTAAND ONDERZOEK

Onderzoek naar zorgen om verwerking van persoonsgegevens laat een aantal terugkerende patronen aan de kant van gebruikers zien die enigszins los staan van de specifieke technische vormgeving van dataverwerking en bescherming. Deze betreffen zowel de algemene sociaal-culturele omgeving waarin dataverwerking betekenis krijgt, als de specifieke context waarin om dataverwerking gevraagd wordt; eveneens gaat het om persoonskenmerken van gebruikers en hun vertrouwen in overheids- en commerciële instanties die met hun data omgaan.

a.

Er zijn nauwelijks positieve verhalen over dataverzameling en verwerking. Misbruik en manipulatie voeren de boventoon in het publieke discours, en het culturele klimaat rond deze vraagstukken kunnen we benoemen als een van zorg en gebrek aan vertrouwen.

***Het is zaak om meer, zorgvuldig en evenwichtig aandacht te besteden aan de voordelen die dataverzameling en datakoppeling kunnen bieden aan individuele burgers en maatschappelijke groeperingen.***

b.

Burgers zijn in te delen als zorgeloos, oplettend, voorzichtig en verontrust ten opzichte van dataverwerking. Hoe deze groepen op intensievere vormen van dataverwerking door de overheid zullen reageren hangt af van het type data waar het om gaat en de wijze waarop deze verzameld en verwerkt worden; het doel waarvoor en de context waarin dit gebeurt; de mate van vertrouwen die men in de data-verwerkende instantie heeft.

***De overheid moet erop voorbereid zijn dat elke vorm van dataverzameling en verwerking, ongeacht de zorgvuldigheid van de procedures, op relatief onvoorspelbare wijze tot privacy-onrust onder verschillende groepen mensen kan leiden.***

c.

Het bestaande onderzoek geeft geen uitsluitsel of en hoe demografische dan wel persoonlijkheidskenmerken de zorgen van burgers over dataverwerking en privacy beïnvloeden.

***In afwezigheid van voorspellende factoren over privacy-bezorgdheid, dient de overheid ervan uit te gaan dat privacy voor iedereen een kwestie van belang is.***

d.

Voor al deze burgers geldt dat intensievere vormen van dataverwerking door de overheid (bijvoorbeeld koppeling of datamining) twee specifieke irritatiefactoren herbergen. Door een combinatie van verschillende relatief onschuldige gegevens kunnen zeer persoonlijke en gevoelige profielen gemaakt worden. Datakoppeling gebeurt bovendien relatief onzichtbaar voor burgers; men weet in de regel niet wat er precies gebeurt, noch hoe het precies gebeurt.

***De overheid moet ervan uitgaan dat data-koppeling gevoelige persoonlijke gegevens oplevert, waarvan burgers graag precies willen kunnen zien hoe ze ontstaan zijn.***

e.

Onderzoek met gegevens van de Eurobarometer suggereert dat in Nederland daadwerkelijk privacybeschermend gedrag niet afhangt van sociale of psychologische factoren, maar bepaald wordt door de mate waarin men gebruik maakt van internet en online overheidsdiensten, en de mate waarin men zich zorgen maakt over 'function creep' en het afgeven van informatie.

***De overheid dient ervan uit te gaan dat intensieve internetgebruikers en afnemers van online overheidsdiensten er veel aan gelegen is om hun data af te schermen.***

f.

Nederlanders hebben een relatief groot vertrouwen in de overheid als het om de verwerking van persoonlijke data gaat. Echter, het blijkt ook dat naarmate diverse soorten zorgen en ervaringen met inbreuk op privacy toenemen, ongeacht in welke context dit gebeurt, het vertrouwen in Nederlandse overheidsinstanties om zorgvuldig met persoonlijke data om te gaan afneemt.

***De overheid dient zich ervan bewust te zijn dat het bestaande vertrouwen in de Nederlandse overheid makkelijk ondermijnd kan worden door gevallen van datamisbruik, mislukte initiatieven en slechte ervaringen.***

## 4. CONTROLESCENARIO'S

Het feit dat voor de meeste mensen hun houding en gedrag ten opzichte van de bescherming van hun persoonsgegevens afhangt van contextuele factoren, doet de aandacht verschuiven naar die verschillende contexten en met name de verschillende manieren waarop privacy vorm gegeven wordt. Het gaat dan om de mate van controle die mensen kunnen uitoefenen over hun eigen gegevens, ook wel 'informationele zelfbeschikking' genoemd'. Hierin zijn vier scenario's te onderscheiden.

a. Klassiek

Het gaat hier om een opvatting over privacy in de zin van afscherming van een steeds breder palet aan persoonsgegevens. Deze heeft online vorm gekregen in het privacystatement. Uit onderzoek en expertgesprekken blijkt dat het print-privacystatement in de regel niet gelezen of begrepen wordt, maar desalniettemin tot een gevoel van zekerheid bij gebruikers leidt.

***De overheid dient bij te dragen aan een betere invulling van privacy-informatie en de bestaande initiatieven op dit gebied te verkennen, ondersteunen en waar mogelijk te implementeren.***

b. Transparant

Transparantie heeft betrekking op nieuwe technieken om privacybeleid beter uit te leggen aan gebruikers (Transparancy Enhancing Technologies, TET), en op inzicht verlenen in de gegevens die instanties over gebruikers hebben opgeslagen (zoals MijnOverheid.nl). Voor gebruikers leidt dat laatste tot de nog niet beantwoorde vraag bij wie de verantwoordelijkheid voor administratieve fouten ligt, en door wie de correctie uitgevoerd moet worden.

***De overheid dient te streven naar maximale transparantie van haar eigen dataverzameling en koppeling, en de modaliteiten ter correctie te versnellen en vereenvoudigen.***

c. Keuze

Het betreft hier de vraag of gebruikers actief toestemming moeten verlenen om data te laten verwerken, of passief geen bezwaar kunnen maken. Dat laatste leidt tot grotere deelname. Voor gebruikers is er echter vaak geen echte keuze en is het meestal onduidelijk waar ze precies toestemming voor geven. Een meer fundamenteel bezwaar is dat privacy hiermee wordt gereduceerd tot een individuele beslissing in plaats van een maatschappelijke waarde.

***Hoewel burgers keuze moeten kunnen hebben in de manier waarop ze hun data willen laten gebruiken, dient privacy niet tot een individuele verantwoordelijkheid worden gereduceerd.***

d. Controle

Gebruikers lijken behoefte aan controle over hun eigen gegevens te hebben, maar hier is sprake van een controleparadox: het gevoel van controle leidt tot onveiliger omgang met de eigen persoonsgegevens. Bovendien is onduidelijk hoe gebruikers dergelijke controle zouden willen uitoefenen.

***De controleparadox suggereert dat de verantwoordelijkheid over persoonlijke data niet uitsluitend bij burgers zelf gelegd kan worden.***

e. Het begrip van de gebruiker

In alle scenario's geldt dat er impliciet van uit wordt gegaan dat de gebruiker rationeel en competent oordeelt over de privacyscenario's die hem of haar aangeboden worden, en vervolgens tot een daarop aansluitende handeling overgaat. Al het onderzoek laat echter zien dat het overgrote deel van gebruikers rommelig opereert. Waarschijnlijk voldoet alleen de kleine groep verontruste gebruikers aan het ideaalbeeld.

***De overheid dient haar systemen maximaal gebruiksvriendelijk in te richten en dient maximale gebruiksondersteuning te bieden.***

## 5. ANTWOORD OP DE ONDERZOEKSVRAAG

Zowel de vigerende scenario's van dataverwerking als de onderzoeksvraag van het onderhavige onderzoek, hebben een radicale wijziging van het perspectief op databescherming nodig die start vanuit de alledaagse realiteit van burgers. Dat impliceert ten eerste 'privacy-by-design', en ten tweede een sterkere nadruk op data- herstel achteraf, ongeacht of dataproblemen door fraude, bureaucratisch onvermogen of onoplettendheid van de burger zijn ontstaan.

***Vanuit de zorgen en het alledaagse handelen van burgers geredeneerd, ligt de meest dringende opdracht van de overheid niet bij het vooraf in controle brengen van de burger, maar in het mogelijk maken en garanderen van gebruiksvriendelijke, snelle en efficiënte mechanismen van correctie, intrekken of vernietiging van gegevens als achteraf blijkt dat er iets mis is gegaan.***

## INLEIDING

In het licht van recente en te verwachten ontwikkelingen rond de verwerking van persoonlijke data, is het Bureau Verkenningen en Onderzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties geïnteresseerd in de volgende vraag:

*Wat is vanuit een sociaal psychologisch perspectief de betekenis van meer controle door de burger (inzicht, toestemming verlenen, beheer) over zijn persoonsgegevens bij de overheid voor de steun van integrale persoonsverwerkende datasystemen van de overheid van de burger?*

Daarbij komen tevens vragen aan de orde over een eventueel verschil tussen bedrijfsleven en overheid op dit punt; over veranderde verhoudingen tussen burgers en overheid; en of burgers meer legitimiteit aan dataverwerking toekennen als zij een sterkere controlepositie hebben.

Hoewel de vraag complex gesteld is, sluit zij direct aan bij een reeks van verschillende ontwikkelingen rond persoonsgegevens en andere soorten data. “Data is het nieuwe goud”, zei voormalig Eurocommissaris Neelie Kroes, bijvoorbeeld, toen ze in 2011 het open data beleid van de EU lanceerde.[1] “Big Data is een van de grootste buzzwoorden in de technologiesector”, aldus *Business Insider* in augustus 2014.[2] Technology start-ups die betere databescherming bieden, behoren tot de snelst groeiende bedrijven in de digitale sector, volgens de gezaghebbende blog *TechCrunch*.[3] De één na de andere internationale consultant brengt een rapport uit over digitale identiteiten, databescherming en databeverwerking[4], en in Nederland volgen de bijeenkomsten waarin nieuwe technologieën, diensten en systemen voor dataverwerking, privacy en ‘identity-management’ gepresenteerd worden elkaar in hoog tempo op. Het nieuw te lanceren E-ID stelsel van de Nederlandse overheid is daarin een favoriet onderwerp.[5] De EU kwam onlangs, na jaren grondige voorbereiding, met een nieuwe richtlijn voor de bescherming van persoonsgegevens die naar verwacht tot harmonisatie binnen de unie zal leiden. Al dergelijke uitspraken en activiteiten laten zien dat er zowel een duidelijk sociaal en economisch ‘data-veld’ is ontstaan als een breed gedragen beleidsdiscours waarin data, hun verzameling, verwerking, opslag en toepassing centraal staan.

Enigszins buiten dat data-veld staan burgers en consumenten, die zich in toenemende mate zorgen maken over wat er met hun data gebeurt. In de politieke barometer van IPSOS zijn sinds 2013 vragen over privacy opgenomen, en uit de twee tot nu toe gehouden metingen blijkt dat het aantal mensen dat zegt zich *geen* zorgen te maken over privacy in rap tempo afneemt (van 44 % in 2013 naar 32 % in 2014) waarbij online winkels, sociale media en de Amerikaanse geheime dienst het minst vertrouwd worden, en de Nederlandse belastingdienst het meest. Uit ander onderzoek blijkt dat 65 % van de Nederlandse burgers vindt dat de overheid ‘meer en meer’ persoonlijke informatie van hen vraagt (Eurobarometer, 2011). In het TNO rapport *i-Overheid, de burger in beeld* uit 2012, wordt aangegeven dat koppeling tussen uitkeringsgegevens en woongegevens, of tussen gemeentelijke gegevens en die van zorginstellingen snel tot een gevoel van onbehagen bij burgers over de overheid kan leiden (Cuipers, e.a., 2012). In een recente enquête werd aan Britse burgers de volgende stelling

[1] http://ec.europa.eu/digital-agenda/en/news/data-new-gold
[2] http://www.businessinsider.com/companies-not-embracing-big-data-2014-8?IR=T
[3] http://techcrunch.com/2014/12/08/another-data-breach-another-dollar/
[4] Bv. Boston Consultancy Group (20120
[5] Zie voor actuele overzichten http://www.pimn.nl/

over de toekomst voorgelegd: “Ik vrees dat in de toekomst de overheid verschillende van mijn persoonlijke gegevens zal kunnen koppelen, zoals mijn bankrekening, arbeidsgeschiedenis, persoonlijke bezittingen en belastingdata. Zijn ze daartoe in staat in 2030?”. 61 % van de mannen en 55 % van de vrouwen deelden die angst (Van Zoonen e.a., 2014). Hoewel in het data-veld voortdurend over dergelijke zorgen, wensen en belangen van gebruikers gesproken wordt, vormen dezelfde gebruikers nauwelijks een concrete gesprekspartner in de ontwikkeling van nieuwe systemen, producten of diensten.

De volgende rapportage van bestaand onderzoek en expert-opinies vindt plaats in deze context van een sterke wens vanuit overheid en bedrijfsleven om meer, efficiënter en doelgerichter van allerlei soorten data gebruik te maken, en een sterke zorg van burgers over hun privacy ten opzichte van beide partijen. Er is gebruik gemaakt van gepubliceerd wetenschappelijk onderzoek, van surveydata over het gebruik van persoonsgegevens uit een Eurobarometer peiling en van expert-visies (een precieze uitleg van de methode staat in bijlage 1). Hierbij moet worden aangetekend dat waar het de praktijken, meningen en verwachtingen van burgers en consumenten betreft, het bestaande wetenschappelijke onderzoek achterloopt op nieuwe technologische ontwikkelingen en beleidsmatige ontwikkelingen; er is bijvoorbeeld nog nauwelijks onderzoek over gebruikerservaringen- en verwachtingen ten aanzien van cloud-diensten of digitale kluizen. Anderzijds laat gebruikersonderzoek echter een aantal terugkerende patronen over sociaal psychologische processen aan de kant van gebruikers zien die enigszins los staan van de specifieke technische vormgeving van dataverwerking en bescherming. Deze betreffen zowel de algemene sociaal-culturele omgeving waarin dataverwerking betekenis krijgt, als de specifieke context waarin om dataverwerking gevraagd wordt; eveneens gaat het om persoonskenmerken van gebruikers en hun vertrouwen in overheids- en commerciële instanties die met hun data omgaan. In deel 1 van het rapport zullen deze uitkomsten nader besproken worden.

Deze algemene patronen laten zien dat de handelingsvrijheid die burgers hebben in specifieke situaties van dataverwerking van cruciaal belang is voor hun gevoel daarover. Daarbij gaat het om situaties waarin burgers geen andere keuze hebben dan zich te onderwerpen aan de eisen van controlerende instanties. Een andere mate van handelingsvrijheid is aanwezig in transacties waarin men in ruil voor specifieke data een dienst of product terugkrijgt, zoals bijvoorbeeld bij online winkelen, online gamen of participatie in specifieke gemeenschappen. Hierbij is met name de balans tussen wat gevraagd wordt aan data en wat men ervoor terugkrijgt van belang voor hoe handelingsvrijheid ervaren wordt. Weer een ander voorbeeld bieden met name sociale media die de illusie van totale handelingsvrijheid geven over hoe en met wie men persoonlijke en alledaagse gegevens deelt. Vanuit dat perspectief van handelingsvrijheid zijn 4 scenario’s te ontwikkelen voor de controle van burgers over hun eigen data: een klassiek, transparant, keuze en controle scenario. In deel 2 van het rapport zullen we bespreken wat het bestaande onderzoek en de expert-opinies aangeven over de sociaal psychologische betekenis van deze scenario’s voor burgers.

## DEEL 1. CULTUUR, CONTEXT EN GEBRUIKERS

Onderzoek naar gebruikers van diverse nieuwe identificatiemiddelen en naar zorgen om privacy laat een aantal terugkerende patronen over sociaal psychologische processen aan de kant van gebruikers zien die enigszins los staan van de specifieke technische vormgeving van dataverwerking en bescherming. Deze betreffen zowel de algemene sociaal-culturele omgeving waarin dataverwerking betekenis krijgt, als de specifieke context waarin om dataverwerking gevraagd wordt; eveneens gaat het om persoonskenmerken van gebruikers en hun vertrouwen in overheids- en commerciële instanties die met hun data omgaan.

### Cultuur

De huidige discussies over de controle van burgers en consumenten over hun persoonsgegevens vinden niet plaats in een isolement, maar krijgen betekenis tegen de achtergrond van zowel historische als actuele verhalen over persoonsgegevens, identiteiten en privacy. Die verhalen schetsen vrijwel zonder uitzondering een duistere culturele 'horizon'. Enkele voorbeelden uit actualiteit en populaire cultuur:

Op 1 oktober 2014 publiceerde de Volkskrant het volgende bericht: "Burger wordt straks doorgelicht zoals profiel van crimineel wordt opgesteld". In het artikel werd melding gemaakt van de plannen van de Nederlandse overheid om persoonsgegevens uit verschillende databestanden te koppelen, teneinde uitkerings- en belastingfraude tegen te gaan. Al had de Tweede Kamer unaniem met het voorstel ingestemd, en lag een controverse dus niet voor de hand, toch deed het bericht onmiddellijk alarmbellen rinkelen. Andere media pikten het snel op, onder andere met de kop "Crimineel profiel van elke burger"[6], en diverse commentatoren spraken hun bezorgdheid uit over de verregaande interventie van de staat in het privéleven van mensen. Minister Asscher voelde zich gedwongen om binnen een dag tekst en uitleg te geven via de site van de Rijksoverheid, en liet weten dat de koppeling 'niet zomaar' plaats zou vinden, dat de adviezen van het College Bescherming Persoonsgegevens en de Raad van State waren meegenomen en dat de Tweede Kamer uitgebreid naar het voorstel had gekeken en het unaniem had goedgekeurd.

Dat het koppelen en delen van persoonsgegevens ontzettend gevoelig ligt, was al bekend uit de heftige discussies rond de invoering van het landelijke Elektronisch Patiëntendossier (zie voor een analyse (Boonstra, Boddy & Bell, 2008). De ING werd met die gevoeligheid geconfronteerd toen de bank begin 2014 bekend maakte een proef te willen doen met het doorgeven van betalingsgedrag van hun klanten aan commerciële partijen, zodat deze gerichte persoonlijke advertenties kunnen aanbieden. "Een tuincentrum wil graag weten dat je elk jaar in maart 150 euro uitgeeft aan tuinspullen. Hij kan dan op het juiste moment een scherp aanbod doen," aldus de bank. Ook in dit geval brak een storm van kritiek los, en volgens een snel uitgevoerde studie van het TV programma Radar, zorgde het plan ervoor dat bijna 80 % van de ING klanten minder vertrouwen in de bank hadden gekregen. Een derde van de ondervraagden zei te overwegen naar een andere bank over te stappen.[7] De ING probeerde de schade nog te herstellen met extra informatie, en stuurde een open

[6] http://www.crimesite.nl/crimineel-profiel-van-elke-burger/
[7] http://www.radartv.nl/nieuws/archief/detail/article/30-ing-klanten-overweegt-overstap-1/

brief naar haar klanten. Het mocht niet baten; het tumult ging pas liggen toen ING bekend maakte voorlopig van de proef af te zien.

In de regel identificeren en kritiseren specifieke consumenten- en privacy-organisaties dergelijke gevallen. *Bits of Freedom*, bijvoorbeeld, maakt regelmatig privacy-schendingen openbaar en reikt sinds 2002 elk jaar de Big Brother award uit aan de organisatie die zich naar hun idee het meeste misdragen heeft. Vrijwel altijd zit daar een geval van ongeoorloofde datakoppeling bij. Zo kreeg de Belastingdienst de prijs in 2013 voor "het stofzuigen van parkeer- en kentekendata die door anderen is verzameld en eigenlijk gewist had moeten worden."[8] (Overigens heeft de rechter in 2014 besloten dat dergelijk gebruik toegestaan is). De Nationale Ombudsman is een andere instantie die gevallen van onrechtmatige datakoppeling en -deling in de gaten houdt: ook bij hem kwam de Belastingdienst in opspraak door overdragen van inkomensgegevens aan verhuurders in de vrije sector.[9] In het brede veld van privacybescherming zijn diverse andere organisaties en partijen actief, waaronder burgerinitiatieven zoals *Privacy First*, de *Privacy Barometer*, *VrijBit, Platform Bescherming Burgerrechten*, of *Stichting KDVP* (speciaal voor privacy in de medische sector), en bedrijfsinitiatieven zoals *Privacy Waarborg* dat een keurmerk voor het zorgvuldig gebruik van klantgegevens uitgeeft.

In deze en aanverwante discussies vallen onvermijdelijk de termen Big Brother, Orwell en soms 'panopticum', die alle verwijzen naar strakke surveillance van onschuldige burgers door de staat. Nadat Edward Snowden had onthuld hoever het afluisterprogramma PRISM van de Amerikaanse overheid reikte, zag Amazon de verkoop van Orwell's *1984* met 7000 % stijgen.[10] In extreme discussies wordt een vergelijking met het Naziregime gemaakt, en daar wordt dan aan toegevoegd dat de huidige systemen geavanceerder en dus nog gevaarlijker zijn.[11] Publieke weerstand tegen persoonsregistratie dateert echter al van veel eerder: toen in Engeland in 1837 een landelijke burgerlijke stand werd ingevoerd, protesteerden de tegenstanders dat 'de Engelsman' zo zijn recht op vrijheid en privacy kwijtraakte, en dat de registratie een voorbode zou zijn van hogere belastingen.[12]

De collectieve angst voor de overheid en haar registratie- en surveillancepraktijken uit zich ook in een niet aflatende stroom populaire films en TV-series die alle suggereren dat het staatsvermogen om burgers te identificeren, op te sporen en te volgen volledig en oneindig is. Een recente loot aan deze stam van 'surveillance cinema' is de Amerikaanse TV-serie 'Person of Interest, waarin een alwetende 'Machine' in staat is terrorisme en misdaad te voorspellen op basis van een combinatie van telefoongesprekken, CCTV beelden, banktransacties en emailverkeer. Tijdens het PRISM schandaal werd de serie alom genoemd als levensecht voorbeeld van hoe de permanente monitoring van burgers plaatsvindt. "Dit komt allemaal niet als een verrassing", schreef een Amerikaanse journalist, "als je een beetje regelmatig naar spionnenseries of films kijkt".[13] We kunnen dan denken aan *Spooks*, *24*, *Homeland*, *Intelligence*, *The Bourne Identity*, *The Last Enemy, The Net* en nog vele andere titels (zie voor een compleet overzicht: Turner, Van Zoonen & Harvey, 2014).

[8] https://bba2013.bof.nl/2013/08/dit-zijn-de-winnaars-minister-opstelten-en-de-belastingdienst/index.html
[9] https://www.nationaleombudsman.nl/nieuws/2013/belastingdienst-mag-inkomensgegevens-van
[10] http://www.theguardian.com/books/booksblog/2013/jun/11/george-orwell-prism-big-brother-1984
[11] http://www.gewoon-nieuws.nl/2013/06/overheid-beschouwt-eigen-burger-als-vijand/
[12] http://www.genuki.org.uk/big/eng/LIN/civilreg.html
[13] http://entertainment.time.com/2013/06/07/prism-of-interest-how-tv-drama-anticipated-the-data-mining-news/

Dergelijke beelden functioneren ook regelmatig in de campagnes van privacy-organisaties en bezorgde burgers om op de bezwaren van data-verwerking te wijzen. Zo circuleert op YouTube een scene uit de Britse serie *The Last Enemy* waarin de overheid de hoofdpersoon zijn identiteit heeft ontnomen; het fragment eindigt met een tekst-over 'Couldn't happen in Britain, could it?'.[14] De American Civil Liberties Union die zich al sinds 1920 inzet voor vrijheid en gelijkheid van Amerikaanse burgers, maakte een YouTube filmpje over pizza bestellen in de toekomst. Het filmpje is inmiddels is al talloze malen gedeeld en ook door diverse andere partijen omgebouwd tot een eigen versie, vaak om een punt te maken in een actuele privacy discussie. Die filmpjes volgen een identiek scenario: klant belt een pizzeria, moet zijn klantnummer doorgeven en krijgt dan, onder meer, te horen dat a) zijn bestelling ongezond is gegeven zijn medische dossier; b) dat zijn kredietlimiet is bereikt en hij cash moet betalen; c) dat hij geen cash geld meer kan opnemen omdat zijn dagelijkse limiet al is bereikt; d) dat hij niet boos moet worden omdat hij zijn cursus woedebeheersing nog niet heeft afgerond. Halverwege de bestelling vraagt de klant dan wanhopig: "Hoe weten jullie dit allemaal?".

De conclusie van deze korte rondgang door de actualiteit en de populaire cultuur kan niet anders zijn dan dat er nauwelijks positieve verhalen over dataverzameling en verwerking bestaan. Misbruik en manipulatie voeren de boventoon en het culturele klimaat rond deze vraagstukken is er vaak een van zorg en gebrek aan vertrouwen. De Amerikaanse onderzoekster Robbin sprak in 2001 in dit verband al van een 'hostile political environment'.

**Context**

Desondanks zijn mensen wel degelijk bereid om hun persoonsgegevens over te dragen en te delen. Daarbij is de context waarin hen dat gevraagd wordt cruciaal. Hoewel het landelijk Elektronisch Patiëntendossier op veel verzet uit het privacy-veld kon rekenen, suggereert divers onderzoek dat er ook een brede bereidheid bestaat om medische gegevens te delen. Een in 2009 uitgevoerde opiniepeiling in opdracht van de Nederlandse Patiënten Consumentenfederatie (NPCF) liet zien dat 95 % van de ondervraagden er geen bezwaar tegen had als hun gegevens zouden worden gedeeld via een EPD. Sommige respondenten gaven ook risico's van privacy en beveiliging aan, maar ook voor hen wogen de voordelen zwaarder dan de nadelen (Van Thiel, 2009). Het rapport kreeg onmiddellijke kritiek van privacy-watchers die het als een propaganda-instrument bestempelden, en de methodologie bekritiseerden.[15] Recenter onderzoek van het NIVEL laat echter eenzelfde bereidheid zien, en ook een brede erkenning van het nut van de uitwisseling van medische gegevens tussen verschillende zorginstellingen (Jansen et al, 2015). Ook buitenlandse onderzoeksgegevens wijzen in dezelfde richting van publieke acceptatie van het koppelen van medische gegevens. Diverse studies die rond 2010 in de staat New York zijn uitgevoerd, laten zien dat de meerderheid van de onderzochte personen positief stond tegenover de uitwisseling van hun persoonlijke data tussen medische professionals (bv. Ancker e.a., 2012).

Voor andersoortige gegevens is het echter minder duidelijk hoe mensen tegenover de brede uitwisseling daarvan met derde partijen staan. Het weinige onderzoek dat er is, suggereert dat

[14] https://www.youtube.com/watch?v=1XsMsWsaoHQ
[15] http://www.nrc.nl/opklaringen/2009/05/25/94-voor-epd-actievoeren-met-een-opiniepeiling/ http://www.spaink.net/2009/05/26/propagandapeiling/

mensen vaak niet goed weten waarom dat voor henzelf of voor een breder maatschappelijk doel nuttig zou zijn. De Engelse overheid heeft het bijvoorbeeld mogelijk gemaakt dat erkende sociaalwetenschappelijke onderzoekers toegang kunnen krijgen tot een brede verzameling administratieve gegevens van Britse burgers die los van elkaar of in koppeling geanalyseerd mogen worden. Een begeleidend onderzoek naar de visies van het publiek op dergelijke uitwisseling liet zien dat het allereerst bijzonder tijdrovend bleek om mensen uit te leggen hoe dergelijke datakoppeling plaats zou vinden en dat er behoorlijke scepsis was over het nut van sociaalwetenschappelijk onderzoek. Na uitleg hoe het onderzoek zou bijdragen aan verbeterde gezondheidszorg of verbetering van de openbare dienstverlening (openbaar vervoer, misdaadbestrijding) zag men echter veel minder problemen. Het profileren van bepaalde individuen of bevolkingsgroepen op basis van postcode of andere gegevens vond men onacceptabel, evenals het doorverkopen van hun administratieve gegevens aan derde commerciële partijen (Cameron, Pope & Clemence, 2014). Die laatste weerzin wordt ook onderschreven door het feit dat een uitbreiding van de koppeling van medische gegevens op grote weerstand in Engeland stuitte, omdat het voornemen was om ook de verzekeringsmaatschappijen toegang tot de nieuwe dataset te verlenen.[16]

Dergelijke uitkomsten geven het belang aan van de *context* waarin gegevens gedeeld worden. Van Zoonen e.a., (2014) noemen op basis van een internationaal literatuur- en onderzoeksoverzicht de volgende factoren:

*Om welke data gaat het?*

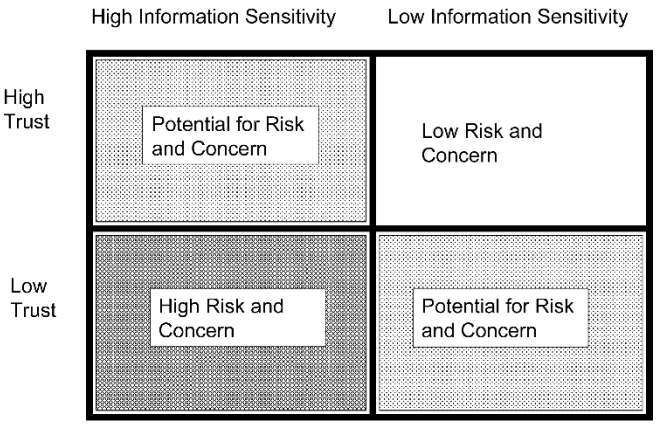
Al het onderzoek op dit gebied wijst in dezelfde richting: mensen beschouwen medische, financiële en civiele data (BSN, ID of paspoortnummer) als hoogst gevoelig, terwijl ze hun sekse, nationaliteit, of leeftijd minder privé vinden. Er is meer variatie in opvatting met betrekking tot biometrische data, foto's, naam en adres, koopgedrag, (sociale) mediagebruik: sommige mensen vinden dit alles hoogst persoonlijk, anderen niet (BCG, 2013; Cranor et al., 2000; Eurobarometer, 2011; InfoSys, 2013).

*Wat voor partij verzamelt de data?*

Eveneens is van belang *met wie* de burger data deelt. Rohm en Milne (2004) maakten een handige indeling van soorten gegevens en soorten instellingen om meer inzicht te krijgen in de zorgen die mensen over hun privacy kunnen hebben. 'Vertrouwen' is daarbij de sleutelfactor, hoewel hun schema ook laat zien dat mensen ook bezorgd kunnen worden als het om instellingen gaat die ze zeer vertrouwen.

[16] http://www.theguardian.com/commentisfree/2014/feb/28/care-data-is-in-chaos

Figuur 1. Schema van Rohm & Milne (2004)




Als het om de behandeling van persoonlijke data gaat, blijkt dat 84 % van de Nederlanders de overheid daarin vertrouwt. Ook is er veel vertrouwen in medische instanties (83 %), banken en financiële instituties (79%) en meer dan gemiddeld vertrouwen in Europese instanties (64%). Er is veel minder vertrouwen in de commerciële bedrijven met wel 75% die absoluut geen vertrouwen heeft in internetbedrijven (Eurobarometer, 2011). De Nederlandse overheid bevindt zich dus in de bovenste twee cellen van het schema van Rohm en Milne, en heeft met een laag tot mogelijk risico te maken, afhankelijk van het soort gegevens dat wordt verzameld.

*Wat is het doel van dataverwerking?*

Zoals gezegd zijn mensen in de regel zeer bereid hun data te delen voor medische doeleinden. Het is eveneens bekend dat in de onmiddellijke nasleep van terroristische aanslagen, mensen het geen probleem vinden om de overheid verdere controle over persoonlijke data te geven. Die bereidheid neemt na ongeveer een half jaar weer af (Sanquist et al., 2008; Smith and Lyon, 2013). Uit het Engelse onderzoek naar datakoppeling bleek eveneens dat mensen dat acceptabel vinden als het om specifieke medische of maatschappelijke doeleinden gaat, maar weinig andere doelen zinvol genoeg vonden om datakoppeling toe te staan.

*Hoe worden data verzameld?*

Staat men vrijwillig of verplicht data af en is men zich ervan bewust dat er data verzameld worden? Met name allerlei relatief onzichtbare vormen van data-tracking en data-mining veroorzaken een gevoel van ongemak (BCG, 2013). In de nasleep van de Snowden onthullingen over de grootschalige en geheime aftapoperaties van de Amerikaanse overheid, is transparantie over dataverzameling steeds hoger op de agenda van zowel aanbieders als gebruikers van online diensten komen te staan.[17]

*In welke sector worden data verzameld?*

Ook telt mee in welke sector van de samenleving men zijn data deelt. De Nederlandse scholen, bijvoorbeeld, kregen in 2014 de jaarlijkse Big Brother Award vanwege de onduidelijke manier waarop

[17] http://www.theguardian.com/commentisfree/2014/jun/05/what-snowden-revealed-changed-nsa-reform

ze gegevens van scholieren deelden met educatieve uitgevers.[18] Ook in de UK ontstaat regelmatig onrust over de manier waarop nieuwe identificatietechnologieën, met name biometrie, in het onderwijs gebruikt worden (Big Brother Watch, 2014). Een vergelijkbare zorg bestaat over privacy op de werkplek of andere semi-privé locaties zoals restaurants of clubs, terwijl men zich weer minder opwindt over (het gebrek aan) privacy in publieke ruimtes zoals de stad of het vliegveld. Bij dit laatste zien we ook weer terug dat men voor veiligheidsdoeleinden bereid is om enige privacy op te geven.

*Privacy paradox*

Dergelijke uitkomsten laten zien dat mensen zich in verschillende contexten andere zorgen over hun data maken. Het is op dit moment goed om even pas op de plaats te maken en stil te staan bij wat wel de 'privacy paradox' genoemd wordt: het gegeven dat mensen zeggen zich zorgen maken over hun privacy maar daar in concrete online situaties niet naar handelen. De grote Amerikaanse opiniepeiler Pew, bijvoorbeeld, vond bijvoorbeeld dat ruim 80 % van de ondervraagden zich niet erg zeker van hun privacy voelt als ze gegevens over zichzelf via sociale media delen; desalniettemin leidt die onrust niet tot minder gebruik. Dat wordt met enige regelmaat als hypocriet bestempeld.[19] Het recente wetenschappelijk onderzoek biedt echter wel degelijk genuanceerde inzichten in deze paradox, die onder andere te maken hebben met het gevoel van en de daadwerkelijke controle die mensen over hun gegevens hebben, en de mate waarin privacybeschermend gedrag mogelijk is. We komen daar later op terug.

Uit dit korte overzicht wordt duidelijk dat datakoppeling door de overheid een paar specifieke irritatiefactoren in zich herbergt. Ten eerste kunnen door een combinatie van verschillende relatief onschuldige gegevens zeer persoonlijke en gevoelige profielen gemaakt worden. Zo bleek uit een geruchtmakend onderzoek uit 2013 dat het relatief eenvoudig is om op basis van Facebook 'likes' iemands politieke, seksuele en religieuze voorkeur, gevoelens van geluk of depressie, leeftijd, sekse en andere persoonlijke gegevens vrij precies te voorspellen (Kosinski, Stillwell & Graepel, 2013). In de context van deze onderzoeksrapportage is het daarom verstandig om datakoppeling in het domein van privacygevoelige data te plaatsen. Ten tweede is datakoppeling relatief onzichtbaar voor burgers; men weet in de regel niet wat er precies gebeurt, noch hoe het precies gebeurt. Uit een dergelijk gebrek aan transparantie ontstaan eveneens regelmatig ergernis en wantrouwen. Ook al wordt datakoppeling door de overheid uitgevoerd, en wordt deze relatief vertrouwd, een combinatie van gevoelige gegevens en onduidelijke procedures kan tot een snelle afname van dat vertrouwen leiden.

**Gebruikers**

Tenslotte suggereert veel onderzoek dat *mensen* zelf ook sterk variëren in de mate waarin ze zich zorgen maken over hun privacy. Sheehan (2002) constateert dat internetgebruikers in vier groepen ingedeeld kunnen worden:

[18] http://www.volkskrant.nl/binnenland/opstelten-en-nederlandse-scholen-winnaars-big-brother-awards~a3812722/

[19] http://www.theguardian.com/technology/2014/nov/16/why-internet-has-turned-us-into-hypocrites

1. Onbezorgd. Deze gebruikers maken zich enkel zorgen wanneer er gevraagd werd om een burgerservice nummer bij het registreren voor een website; iets waar iedere respondent zich ernstig zorgen over maakte. Onbezorgde internetgebruikers klagen zelden bij hun internetproviders over bijvoorbeeld ongewenste email, registreren zich vaker voor websites en geven daarbij zelden onjuiste informatie op (16 % van de respondenten van Sheehan).
2. Oplettend. Deze internetgebruikers zijn weinig of matig bezorgd in de meeste situaties. Ze geven vaker onjuiste informatie op dan onbezorgde internetgebruikers bij het registreren voor websites. Verder verschilt hun gedrag niet van de minst bezorgde groep (38 %).
3. Voorzichtig. Deze internetgebruikers voelen middelmatige bezorgdheid in de meeste situaties. Voorzichtige internetgebruikers klagen zo nu en dan over ongewenste email en registreren zich maar af en toe voor websites. Hierbij geven ze vaker onjuiste informatie op dan de oplettende internetgebruikers (43 %).
4. Verontrust. Deze kleine groep internetgebruikers (3%) is erg bezorgd over hun online privacy. Ze klagen het meest over ongewenste email en registreren zich amper voor websites. Wanneer zij zich wel registreren geven ze vaak incomplete in onjuiste informatie op.

Een dergelijke indeling is ook in andere studies gevonden. Zo vindt Norval (2012) vier houdingen ten opzichte van biometrische gegevens: 'privacy advocates' (zeer bezorgd over privacy), conservative techies (bezorgd maar enthousiast over biometrie), safety champions (pragmatisch maar oplettend) en 'casual adopters' (onbezorgd).

Vaak wordt verondersteld dat er tussen deze groepen specifieke demografische verschillen bestaan, waarbij ouderen en hoger opgeleiden meer privacyzorgen zouden hebben en jongeren en lager opgeleiden minder. Ook is er onderzoek dat erop wijst dat vrouwen zich meer zorgen zouden maken dan mannen. Desalniettemin blijkt uit een overzicht van Van Zoonen et al. (2014) en van Segers en Van Zoonen (2014) dat er nog geen consistente patronen zijn gevonden met betrekking tot sociaal-demografische voorspellers van privacy-concerns:

*Leeftijd*

Er wordt vaak gedacht dat jongeren zich minder zorgen maken dan ouderen over hun privacy. Er is ook divers onderzoek dat deze gedachte onderbouwt (bv. Young &Quan-Haasse, 2013), maar er is eveneens onderzoek dat erop wijst dat leeftijd niet veel uitmaakt (Van Zoonen & Turner, 2013) of dat juist oudere groepen zich zorgeloos gedragen (Sheehan, 2002).

*Sekse*

Ook wat betreft sekse zijn de uitkomsten van het onderzoek divers met resultaten die laten zien dat meisjes beter hun privacy beschermen dan jongens (Hoy and Milne, 2010; Rowan en Dehlinger, 2014), dat mannen dat meer doen dan vrouwen (Sheehan, 1999), of dat er geen verschil is (Kolsaker and Payne, 2002). In een studie van UK surveygegevens, vinden Segers en Van Zoonen (under review) ook geen verschillen van belang met betrekking tot zorgen over privacy. Wel blijkt dat meer vrouwen zeggen behoefte aan controle over hun eigen data te hebben dan mannen.

*Opleiding*

Ook hier zijn de resultaten van het onderzoek tegenstrijdig en afhankelijk van de specifieke context waarin naar privacy gevraagd is. Zo is er bijvoorbeeld onderzoek dat laat zien dat privacy zorgen over mobiele communicatie groter zijn onder hoog opgeleiden (Zhang, Chen and Lee, 2013), evenals

onderzoek dat laat zien dat privacy zorgen over internet groter zijn onder laag opgeleiden (Zukowski and Brown, 2007).

*Nationaliteit*

Er is tevens onderzoek gedaan naar de invloed van nationale cultuur op de privacy concerns van burgers, waarbij veelvuldig gebruik is gemaakt van de culturele waarden index van Geert Hofstede. Zo vonden Cho, Rivera-Sánchez & Lim (2009) dat internetgebruikers uit Aziatische landen die hoog scoren op de waarde collectiviteit zich minder zorgen maakten over hun online privacy dan internetgebruikers uit westerse landen die hoog scoren op de waarde individualiteit. Daartegenover staan bevindingen van Bellman, Johnson, Kobrin en Lohse (2004) die uitwijzen uit dat verschillende culturele waarden wel een effect kunnen hebben op sommige dimensies van privacy concerns, maar ze vinden daarbij geen coherente patronen.

Dergelijke tegenstrijdigheden komen voort uit de verschillende designs en meetinstrumenten van studies naar privacyzorgen, maar wijzen er ook op dat mensen verschillende interpretaties van privacy hebben en dat ze bij de beantwoording van vragen aan verschillende contexten denken. Daarnaast zijn er onderzoekers die stellen dat demografische variabelen geen zinvolle voorspellers meer zijn (zoals ze ook veel zeggingskracht in marketingonderzoek hebben verloren) en dat persoonlijkheidskenmerken, lifestyle en ervaring met inbreuk in privacy of identiteitsfraude betere resultaten opleveren (Bansal et al.,2010). Het onderzoek hierover is echter beperkt en toont voorlopig eveneens tegenstrijdige resultaten. Junglas et al. (2008), bijvoorbeeld, gebruikten the 'big five' van persoonlijkheidskenmerken in hun survey over privacyzorgen en vinden dat mildheid, ordelijkheid en autonomie alle de zorgen over privacy doen toenemen. Korzaan & Boswell (2008) vinden echter alleen een invloed van mildheid.

**Gebruikers en de Nederlandse overheid**

Aan de Universiteit van Twente zijn in de afgelopen jaren een aantal gebruikersonderzoeken uitgevoerd die zich specifiek richtten op de houding van Nederlandse burgers ten opzichte van de overheid als het gaat om de verwerking van persoonlijke gegevens (zie Beldad, 2011). Daaruit komen een aantal specifieke factoren naar voren die bijdragen aan de bereidheid van mensen om persoonlijke data met de overheid te delen: het vertrouwen dat mensen hebben in de betreffende overheidsinstelling, en de aanwezigheid en vindbaarheid van het privacystatement van die instelling; de inschatting van voordelen, effectiviteit en risico van de interactie. Met name de perceptie van risico bleek samen te hangen met de gevoeligheid van gegevens, en met het (gebrek aan) vertrouwen dat men in een specifieke instantie had. Daarnaast bleek dat positieve ervaringen met de overheid, en de reputatie van de betreffende instelling ook positief bijdragen.

Enkele van deze bevindingen worden ondersteund door gegevens uit een in 2010 uitgevoerde survey in 27 EU landen onder toezicht van de Eurobarometer waarin vragen werden gesteld over databescherming en elektronische identiteit (Eurobarometer, 2011). In de survey zijn twee vragen gesteld die van direct belang zijn voor de onderhavige onderzoeksvraag. Om te beginnen gaat het om een vraag naar vertrouwen in publieke instanties (bv. belastingdienst of sociale verzekeringsinstanties) om met persoonlijke data om te gaan. De Nederlandse data zijn ten behoeve van dit onderzoek opnieuw geanalyseerd (zie Bijlage 1 voor detail).

Het bleek dat de overgrote meerderheid van de Nederlandse bevolking (84,5%) vertrouwen heeft in overheidsinstanties met betrekking tot het beschermen van persoonlijke data. Meer dan een derde (35,8%) is daar zelfs zeer gerust over. Onder jonge respondenten lag dit percentage beduidend hoger. Het vertrouwen was ook groter in de groepen mensen met veel vertrouwen in andere instanties, die zich weinig zorgen maakten over privacy en het gevoel hadden controle te hebben over hun eigen data. Bij de groepen die bezorgd zeiden te zijn over function creep, surveillance of webtracking, of die ervaring hadden met identiteitsfraude en die actief hun eigen privacy beschermen lag dit percentage lager. Er bleek geen verband met andere demografische variabelen, noch met het al of niet gebruiken van online overheidsdiensten. In tabel 1 worden de relaties in tabelvorm weergegeven.

Tabel 1. Vertrouwen in dataverwerking door Nederlandse overheidsinstanties

| **Onder deze groep ….** | **…. zijn er meer of minder mensen die overheidsinstanties vertrouwen met hun persoonlijke data** |
|---|---|
| Jongeren | Meer |
| Vertrouwen in meerdere instanties (Europese instanties, financiële instellingen, internetbedrijven etc.) | Meer |
| Weinig moeite met verstrekken van persoonlijke data | Meer |
| (Van mening dat) verstrekken van persoonlijke data behoort tot het moderne leven | Meer |
| Persoonlijke data verstrekken in ruil voor gratis online diensten | Meer |
| Gevoel van controle over eigen data | Meer |
| Zorgen over function creep, surveillance of webtracking | Minder |
| Ervaring met identiteitsfraude | Minder |
| (Van mening dat) de overheid steeds meer om persoonlijke data vraagt | Minder |
| Weinig internetactiviteiten (online winkelen, sociale media, foto’s/video’s delen) | Minder |
| Actief beschermen van online identiteit | Minder |

We zouden uit het onderzoek van Beldad (2011) en de Eurobarometer in algemene termen kunnen concluderen dat naarmate diverse soorten zorgen en ervaringen met inbreuk op privacy toenemen, ongeacht in welke context dit gebeurt, het vertrouwen in Nederlandse overheidsinstanties om zorgvuldig met persoonlijke data om te gaan, afneemt. Als we daarbij nemen dat de uitkomsten van het eerder besproken onderzoek over antecedenten van privacy weinig systematiek laten zien, moeten we er vooralsnog van uitgaan dat dit proces van verlies aan vertrouwen zich onder alle bevolkingsgroepen en onder alle typen mensen afspeelt.

*Privacygedrag*

Een tweede opvallende uitkomst uit het Eurobarometer onderzoek betreft in hoeverre mensen daadwerkelijk hun privacy beschermen als ze op internet actief zijn, en van welke factoren dit afhangt. De vraag die gesteld werd, luidde: " Wat doet u specifiek op het internet om uw identiteit te beschermen? Daarbij werden 10 keuzemogelijkheden gegeven die varieerden van nep-email accounts gebruiken tot spyware downloaden of privacysettings aanscherpen (zie appendix # voor detail). Op basis van de secundaire analyses die we ten behoeve van de onderhavige onderzoeksvraag hebben uitgevoerd konden we niet vast stellen dat enige demografische variabele van invloed was op privacybeschermend gedrag. Wel bleken twee specifieke opvattingen over privacy van belang: mensen die zich zorgen maakten over function creep deden ook meer om hun privacy te beschermen terwijl mensen die het blootgeven van persoonlijke informatie op internet geen probleem vinden minder deden. Daarnaast liet de analyse zien dat naarmate men meer gebruik van internet maakt (waaronder meer gebruik van online overheidsdiensten) en zegt de privacystatements te lezen, de hoeveelheid manieren die men gebruikt om privacy te beschermen, toeneemt.

Dat het hier geen voor de hand liggende verbanden betreft blijkt uit een vergelijking van de Nederlandse bevindingen met twee landen die wat betreft culture waarden en internetgebruik respectievelijk op Nederland lijken en van Nederland verschillen: de factoren die privacybeschermend gedrag voorspellen zijn anders, maar in beide landen speelt het gebruik van online overheidsdiensten daar geen rol in. Dat lijkt een typisch Nederlandse samenhang.

## Samenvatting deel I en vooruitblik deel II

De rapportage in deel I werd ingegeven door het feit dat er nog geen goed wetenschappelijk onderzoek is naar wat gebruikers vinden van nieuwe technieken om de eigen data te beschermen en beheren, maar dat er op basis van bestaand onderzoek wel een aantal algemene patronen te identificeren zijn.

1. Er zijn nauwelijks positieve verhalen over dataverzameling en verwerking. Misbruik en manipulatie voeren de boventoon in het publieke discours, en het culturele klimaat rond deze vraagstukken kunnen we benoemen als een van zorg en gebrek aan vertrouwen. Er lijkt sprake van een 'hostile political environment'.

2. Intensievere vormen van dataverwerking door de overheid (bijvoorbeeld koppeling of datamining) herbergen twee specifieke irritatiefactoren voor burgers. Ten eerste kunnen door een combinatie van verschillende relatief onschuldige gegevens zeer persoonlijke en gevoelige profielen gemaakt worden. Ten tweede is datakoppeling relatief onzichtbaar voor burgers; men weet in de regel niet wat er precies gebeurt, noch hoe het precies gebeurt. Uit een dergelijk gebrek aan transparantie ontstaan eveneens regelmatig ergernis en wantrouwen.

3. Er zijn globaal vier posities van burgers ten opzichte van dataverwerking en privacy te identificeren: zorgeloos, oplettend, voorzichtig en verontrust, waarbij de grootste groep zich in de twee midden categorieën bevindt. Hoe deze groepen op intensievere vormen van dataverwerking door de overheid zullen reageren hangt af van het type data waar het om gaat en de wijze waarop ze verzameld en verwerkt worden; het doel waarvoor en de context waarin dit gebeurt; de mate van vertrouwen die men in de data-verwerkende instantie heeft. Het bestaande onderzoek geeft geen uitsluitsel of en hoe

demografische dan wel persoonlijkheidskenmerken de houdingen van burgers tegenover dataverwerking en privacy beïnvloeden.

4. Wat betreft de relatie van Nederlandse burgers met de overheid blijkt uit onderzoek dat men een relatief groot vertrouwen heeft in de overheid als het om de verwerking van persoonlijke data gaat. Echter, het blijkt ook dat naarmate diverse soorten zorgen en ervaringen met inbreuk op privacy toenemen, ongeacht in welke context dit gebeurt, het vertrouwen in Nederlandse overheidsinstanties om zorgvuldig met persoonlijke data om te gaan, afneemt. Teruggrijpend op het negatieve culturele klimaat, zien we dus hoe dit een rol kan spelen bij het vertrouwen wat men in de overheid op dit punt heeft.

5. Eveneens blijkt, relatief uniek voor Nederland, dat het gebruik van online overheidsdiensten samenhangt met een hoge mate van privacybeschermend gedrag. Ongeacht de causaliteit van dit verband, is deze samenhang een indicator van het feit dat mensen die online overheidsdiensten gebruiken voorzichtiger zijn met hun persoonlijke data dan mensen die dat niet doen. Dat kan als een goed teken beschouwd worden en roept de vraag op of en hoe de overheid specifiekere vormen van privacybescherming en controle over de eigen gegevens moet realiseren in de interactie met haar burgers; niet alleen voor het gevoel wat ze bij online transacties met de overheid hebben, maar ook voor de daadwerkelijke uitoefening van die bescherming en controle. Om die vraag te beantwoorden, worden in het volgende deel vier mogelijke scenario's van databescherming beschreven; een klassiek, transparant, keuze en controlescenario.

## DEEL II. SCENARIO'S VOOR DATACONTROLE

De afwezigheid van duidelijke demografische en persoonlijke kenmerken die de houding van mensen tegenover dataverwerking en privacy voorspellen en het feit dat voor de meeste mensen (met uitzondering van de zorgelozen en de verontrusten) die houding afhangt van een aantal contextuele factoren, doen de aandacht verschuiven naar die verschillende contexten en met name de verschillende manieren waarop privacy vorm gegeven wordt. Het gaat dan om de mate van vrijheid en controle die mensen kunnen uitoefenen over hun eigen gegevens, ook wel 'informationele zelfbeschikking' genoemd'. In de volgende bespreking van de vier scenario's wordt ook duidelijk dat opvattingen over privacy en dataverwerking door de tijd heen sterk veranderd zijn.

### Klassiek

Vraagstukken over privacy hebben zich in het verleden vooral gericht op tot het recht om het eigen privéleven af te schermen tegen de buitenwereld, en in het bijzonder tegen de overheid (cf. DeCew, 2013). Aan het einde van de 19e eeuw zorgde de opkomst van de massapers ervoor dat deze discussies over privacy uitgebreid werden met de vraag of en in hoeverre de journalistiek mocht berichten over privéhandelingen, gedachten en emoties van burgers. Dit kwam in de jaren daarna steeds sterker naar voren ten gevolge van een de opkomst van gespecialiseerde celebrity-media die berichten over het privéleven van sterren uit de sfeer van entertainment, sport en politiek. De meest recente aflevering van dit privacy discours betreft het *News of the World* schandaal in Engeland; de tabloid-krant van die naam moest sluiten vanwege het afluisteren van politici, royalty, slachtoffers van misdaad en andere nieuwswaardige figuren. Het leidde eveneens tot een onderzoek naar de

praktijken van andere tabloids en een heftig openbaar debat over persvrijheid versus privacy (cf. Van Zoonen, 1998).

In deze gevallen is de privacy-discussie gebouwd op een scherp onderscheid tussen de intimiteit van het huiselijke, privéleven en de openbaarheid van ofwel de staat ofwel de massamedia. Met de opkomst van het internet bleek dat relatief simpele privacy paradigma niet meer te handhaven. Een opvatting over privacy die betrekking heeft op de afscherming van privégegevens en de handhaving van een zekere mate van anonimiteit  is in de context van online transacties steeds minder zinvol. Mensen blijken via hun persoonlijke blogs en sociale media hun privéleven vaak met plezier vrij te geven aan vrienden en familie, maar ook vaak aan een groter publiek van onbekenden (bv. Marwick, 2013). Daarnaast worden persoonlijke gegevens relatief makkelijk gedeeld met commerciële partijen als daar voordelen van gemak, kostenbesparing of efficiëntie tegenover staan, zo blijkt, onder meer, uit recent onderzoek van het Nederlandse platform voor de Informatiesamenleving (ECP, 2014; zie ook Acquisti, John & Loewenstein, 2013).

Diverse auteurs hebben dientengevolge geprobeerd om het privacybegrip op te rekken en inclusiever te maken dan voorheen, toen het alleen op de afscherming van de privésfeer gestoeld was. Clarke maakte in 1997 bijvoorbeeld een veel gebruikt onderscheid naar privacy van de persoon (in het bijzonder kenmerken van het lichaam), gedrag, communicatie en data (dat laatste staat ook wel bekend als information privacy). In 2013 voegde hij daar nog de privacy van ervaringen aan toe, waarmee hij doelt op de kleine en grote dingen die mensen met elkaar delen via de diversiteit aan communicatiemiddelen. Finn, Wright en Friedewald (2013) bouwen op deze indeling voort en voegen nog de privacy van locatie en van vereniging toe en komen zo op zeven dimensies van privacy.

De concrete vorm die dit klassieke scenario aanneemt is die van het privacystatement, dat als bescherming van de eigen gegevens in zijn meest voorkomende geschreven vorm, eigenlijk niet voldoet. Dat is in het algemeen de mening van de experts die we gesproken hebben en is eveneens bekend uit wetenschappelijk onderzoek. Privacystatements zijn vaak lang, ingewikkeld en moeilijk vindbaar (Van Alsenoy et al., 2014). Daarnaast geven ze meestal wel informatie over wat er met persoonlijke data gebeurt, maar zelden wat de risico's van misbruik of fraude zijn (Adjerid e.a., 2013). Hoewel dergelijke analyses vooral voor commerciële contexten zijn gedaan, suggereert het enkele onderzoek dat de privacy statements van overheidssites heeft bekeken dat het daar niet veel beter is gesteld: Beldad en collega's (2011) vonden bijvoorbeeld dat sommige gemeentelijke websites in Nederland geen privacystatement bevatten, en andere ze niet makkelijk vindbaar presenteren. Daarnaast varieerde de kwaliteit van de informatie aanzienlijk. Wat betreft het gebruik van privacy-statements blijkt ook regelmatig dat mensen deze nauwelijks lezen, laat staan grondig bestuderen om op basis daarvan een geïnformeerde afweging te maken. Desalniettemin hebben privacystatements wel effect op het vertrouwen dat gebruikers in de betreffende site hebben; Arcand e.a.., (2007) vond bijvoorbeeld dat de pure aanwezigheid van een privacystatement het vertrouwen van gebruikers over hun data-controle vergroot. Wordt het privacy-statement echter wel gelezen, dan blijkt vertrouwen vooral af te hangen van de manier waarop informatie gepresenteerd wordt en minder van de daadwerkelijke vormen van data-bescherming (ibid; also Adjerid e.a., 2013)

**Transparantie**

Privacystatements in hun huidige vorm lijken dus hun doel voorbij te schieten of perverse effecten te hebben.[20] Er wordt daarom steeds meer gezocht naar Transparency Enhancing Technology (TET). Janic, Wijbinga en Veugen (2013, zonder pagina) definiëren deze als volgt: "Als we transparantie definiëren als inzicht in hoe data worden verzameld, opgeslagen, verwerkt en toegankelijk gemaakt, dan zijn TETs alle middelen die dat inzicht nauwkeurig en begrijpelijk presenteren". Dergelijke TETS worden bijvoorbeeld ontworpen in de vormen van iconen, scores, zogenaamde add-ons voor browsers, quizjes, enzovoort. Zo zijn er sinds kort diverse visuele instrumenten (o.a. Lightbeam, Disconnect) in omloop die je aan je browser kunt koppelen en die laten zien of er derde partijen betrokken zijn bij je bezoek aan een website. Takano et al (2014) deden een proefonderzoek onder een kleine groep gebruikers en vonden dat een visualisering van web-tracking bijdroeg aan hun privacybewustzijn. Een ander visueel middel werd ontwikkeld door Vaniea et al (2012) die constateerden dat zo'n beeld wel dicht bij de online plaats van data-handeling moest staan, om gebruikers attent te maken op privacy-beslissingen. Een ander voorbeeld komt van Mazurek en collega's (2011) die een methode ontwikkelden en toetsten waarmee gebruikers verzoeken om datagebruik reactief kunnen honoreren of niet. Hun pilotgroep waardeerde de flexibiliteit van het systeem en de manier waarop het ze zelf controle gaf over hun data. Een laatste voorbeeld komt van Tsai en haar collega's (2009) die een systeem ontwikkelden waarmee gebruikers van een mobiele toepassing konden zien wie hun locatie had opgevraagd. Na vier weken bleek dat de groep die het middel gebruikte hun privacy-settings preciezer konden instellen en zich ook minder bezorgd voelden over het delen van hun locatie, dan de groep die het middel niet gebruikte.

Transparantie gaat echter veel verder dan een aantal technologieën die de begrijpelijkheid van privacystatements vergroten en de wijze van dataverwerking inzichtelijk maken. Dergelijke verfijningen laten de kern van privacy als bescherming en afscherming van persoonlijke data en levenssfeer ongemoeid. De Leidse jurist Bart Schermer legde in 2011 al uit dat een dergelijk afschermingsprincipe om verschillende redenen niet meer houdbaar is: er zijn legitieme redenen voor overheids-, commerciële en andere instellingen om persoonlijke data te registreren en te bewaren; het is zelfs met minimale gegevens al mogelijk om individuen te identificeren en te profileren; ook onpersoonlijke gegevens als IP-adres en cookies maken het mogelijk om personen te identificeren. 'Privacy als afscherming' geeft in al deze gevallen een vals gevoel van zekerheid. Bovendien, stelt Schermer, is afscherming een principe dat vooraf ingevuld wordt, maar de gevoelige persoonsinformatie die ontstaat door koppeling van onschuldige gegevens is juist gebaat bij een mechanisme om achteraf vast te stellen of privacy geschonden is.

Dergelijke argumentatie heeft sterk aan politieke kracht gewonnen. De Europese Unie heeft hierin het voortouw, en is in 2014 met voorstellen voor een nieuwe Algemene Verordening Gegevensbescherming (AVG) gekomen.[21] Hoewel het nog enkele jaren zal duren voordat de volledige AVG geïmplementeerd is en nationaal specifieke invullingen heeft gekregen, heeft de Nederlandse overheid een deel van de verordening al toegepast op haar eigen dataverzameling. Via de website Mijn Overheid.nl kunnen burgers zien welke persoonlijke gegevens de overheid van iemand heeft

[20] Van Alsenoy et al (2014) geven bovendien een aantal fundamentele en politieke misvattingen over het huidige type privacy statement aan.
[21] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf

vastgelegd. Eveneens kunnen mensen hun gegevens online controleren en wordt vermeld waar men terecht kan voor correctie. Ook andere instanties verschaffen steeds vaker inzicht in de gegevens die zij van mensen beheren.

In onze expertgesprekken werden twee belangrijke kanttekeningen bij deze vormen van transparantie gemaakt; de eerste betrof de correctiemogelijkheden wanneer incorrecte gegevens worden aangetroffen, de tweede betrof de verantwoordelijkheid voor de correcte gegevens. Wanneer men bijvoorbeeld een incorrecte registratie van arbeidshistorie bij het UWV aantreft, dan ligt de bewijslast en het werk ter correctie bij de burger die moet zorgen dat de juiste documenten aangeleverd worden; er zijn allerlei gevallen denkbaar waarin die gegevens niet eenvoudig te verkrijgen zijn (bedrijf failliet, verstreken tijd, enzovoort). Daarnaast moet de burger blijven toezien op de uitvoering van de correctie en zijn juist grote bureaucratieën als het UWV niet altijd in staat om snel en adequaat te reageren. Zo wordt misschien door transparantie een schijn van controle gegeven die in werkelijkheid moeizaam te realiseren is.[22] Ten tweede werd de vraag gesteld wie er uiteindelijk verantwoordelijk is voor administratieve fouten in de registratie van gegevens, de overheid of de burger? Met transparantie komt controle, maar betekent dat ook totale verantwoordelijkheid voor de burger?

**Keuze**

In hoeverre hebben mensen keuze om in specifieke situaties hun persoonlijke gegevens wel of niet vrij te geven, of om toestemming te geven om hun gegevens te laten koppelen? Het onderzoek hierover betreft vooral de vraag naar de effecten van opt-out of opt-in strategieën. Vanuit privacy en controle perspectief is een opt-in strategie waarin mensen expliciet toestemming moeten geven om hun data te gebruiken en te delen het meest wenselijk, zo stelt onder meer de Europese richtlijn over gegevensbescherming. Bij gevoelige data, en in het bijzonder medische data, raden ethische commissies eveneens een opt-in strategie aan. Anderzijds leiden opt-in keuzes ertoe dat minder mensen aangeven dat hun data gebruikt en gedeeld kunnen worden, hetgeen voor marketing organisaties, maar ook voor medische onderzoekers soms reden is om the pleiten voor opt-out (cf. Lai & Hui, 2006). Diverse organisaties van medische onderzoekers hebben bijvoorbeeld aangegeven dat de huidige voorstellen van de EU voor aangescherpte wetgeving ter bescherming van persoonsgegevens, ertoe leiden dat bijvoorbeeld epidemiologisch en kankeronderzoek in kwaliteit achteruit zouden gaan.[23] Daarnaast vergt opt-in een ingewikkelder administratie dan opt-out (Das & Couper, 2014). De standaard optie die daarom meestal aan burgers en consumenten wordt gegeven is dat ze actief moeten aangeven dat NIET te willen.

Daarnaast maakt uit via welk communicatiemiddel en met welke formulering de opt-in of opt-out keuze wordt gepresenteerd. Onderzoek van Milne & Rohm (2000) en van Das en Couper (2014) wijst erop dat uitgebreide en/of schriftelijke uitleg meer bereidheid oplevert tot data delen dan korte emails. De laatste auteurs vinden in hun onderzoek echter ook dat mensen vaak niet goed overzien wat er precies met hun data gebeurt. Het ging in hun onderzoek speciaal over het koppelen van bevolkingsstatistieken met survey-gegevens. Ook het Engelse Office of National Statistics vond dat

[22] Het betreft hier een algemene kanttekening als wel een persoonlijke ervaring van een van de experts.
[23] http://www.bmj.com/content/346/bmj.f3534?ijkey=zvI2K7lzHjKRr5E&keytype=ref

mensen vaak niet goed begrijpen wat de koppeling van bevolkingsstatistieken met administratieve gegevens precies inhoudt. Ander onderzoek suggereert eveneens dat mensen vaak niet precies weten waar ze toestemming voor geven (e.g. Kelly et al., 2012).

Van Alsenoy, Kosta en Dumortier (2014 vatten de skepsis over keuzescenarios samen en stellen in navolging van Calo (2012, in Van Alsenoy et al, 2014 dat ze ten eerste op een verkeerd idee van een ideale gebruiker gebaseerd zijn: 'de rationele consument met grenzeloze aandacht' (p.189). De moeite om zich in datakeuzes te verdiepen is soms te groot voor de opbrengst die men ervan verwacht; daarnaast is de veronderstelling dat iedereen precies begrijpt waartoe men kiest onhoudbaar en treedt ook snel keuzevermoeidheid op. Daarnaast, en dat geldt voor talloze data-interacties die men met de overheid aangaat, is in veel gevallen geen keuze mogelijk en betekent afzien van dataverwerking ook dat de betreffende dienst niet gebruikt kan worden. Het resultaat van dit alles is dat er soms geen echte keuze is, of dat men toestemming geeft of weerhoudt zonder dat men precies weet waartoe of waarover. Ten tweede snijden Van Alsenoy en zijn collega's een principiëler punt aan dat te maken heeft met de manier waarop privacy tot een individueel en onderhandelbaar product wordt gemaakt dat alleen gedefinieerd wordt door de keuzes van individuen om wel of niet mee te doen met dataverwerking. Privacy wordt zo tot een individuele verantwoordelijkheid gemaakt, terwijl het een maatschappelijke waarde is, aldus de auteurs (zie ook Hildebrandt en Koops, 2010). Dat betekent zowel dat er een bredere dan een individuele verantwoordelijkheid is om privacy te beschermen, als dat er een maatschappelijke reden kan zijn om privacy in te perken, in bijvoorbeeld de context van misdaad- of ziektebestrijding.

We hebben in de gesprekken met de experts het keuzescenario verder uitgebreid naar de manier waarop mensen over dataverwerking geïnformeerd willen worden. Omdat het bestaande onderzoek consequent een drie à vierdeling van privacy-types laat zien van zeer bezorgd, pragmatisch en onbezorgd, die op wisselende manieren afhankelijk is van persoonskenmerken en context, is het misschien wenselijk om daarmee rekening te houden in de keuzemogelijkheden en informatie. In hun interacties met de overheid zouden mensen daarom zelf via – bijvoorbeeld – een keuzemenu moeten kunnen aangeven hoeveel ze willen weten en controleren over het gebruik van hun data. Mensen met weinig zorgen en veel vertrouwen volgen zo een andere 'route' naar toestemming dan mensen met veel zorgen. In verschillende contexten kan men verschillende routes kiezen, en op elk gewenst moment kan men van route veranderen. De experts vonden het de moeite waard om over de praktische vormgeving daarvan verder na te denken, maar vroegen zich eveneens af of dat een juridisch houdbare procedure zou kunnen zijn.

**Controle**

De onderzoeksvraag van de overheid voor de onderhavige reportage betreft met nadruk de vraag rond het in controle brengen van de burger, in het bijzonder door "te komen tot een stelsel van afspraken rond digitale datakluizen die zowel door de overheid als door het bedrijfsleven worden

ontwikkeld. Daarnaast zou de overheid het voortouw moeten nemen in een aantal proefimplementaties."[24]

Deze vraag komt voort uit een steeds intensiever wordende discussie over het persoonlijk eigenaarschap en beheer van online gegevens, onder meer naar aanleiding van een gedachte dat consumenten zelf ook financieel zouden moeten kunnen profiteren van hun datagedrag. De bedragen die hierover genoemd worden variëren nogal: Shawn Buckles, een Groningse student, verkocht zijn persoonlijke data aan de hoogste bieder en verkreeg er 350 euro voor.[25] De Financial Times biedt een online instrument aan waarmee je de waarde van je persoonlijke data kunt berekenen, en komt voor een dataprofiel van een gemiddelde huizenbezitter met thuiswonende kinderen op 35 cent uit.[26] Ook zijn er start-ups geweest die het mogelijk maakten dat je zelf je data direct aanbiedt aan geïnteresseerde partijen maar geen van deze heeft een succesvol kostenplaatje weten te ontwikkelen. Een nieuwe social media site (Teckler) die beloofde 70% van hun data-inkomsten te delen met zijn gebruikers, heeft het ook niet gehaald.[27] Vooralsnog lijkt er aan data-eigendom voor een individu dus weinig winst te behalen.

Een geheel andere reden dat persoonlijk eigenaarschap en databeheer op de agenda is komen te staan, heeft te maken met de vraag wat er met iemands online bestaan dient te gebeuren na overlijden (bv. Moreman & Lewis, 2014). Het gaat hier om het afsluiten van email accounts, sociale media profielen, klantenkaarten en de onuitputtelijke hoeveelheid andere gevallen waarin de overledene een digitale nalatenschap achterlaat die voor de nabestaanden soms moeilijk te beheren is. Er worden hier inmiddels talloze diensten voor ontwikkeld met aansprekende namen als Death Switch, Suicide Machine of Accountkiller, en – iets minder spectaculair – Digizeker, een dienst van de Nederlandse notarissen waarmee 'nabestaanden jouw profielen van internet kunnen verwijderen'.[28] Het betreft een digitale kluis waarin alle digitale gegevens van de gebruiker opgeslagen kunnen worden, en waarvan de notaris een 'reservesleutel' bezit die de erfgenamen kunnen gebruiken om de digitale nalatenschap af te ronden. Overigens zijn er ook diverse diensten die het mogelijk maken een digitaal level na de dood te leiden.[29]

Wij hebben geen wetenschappelijk of marketing onderzoek kunnen vinden naar gebruikersbehoeften aan en –ervaringen met digitale kluizen. Het gebruik van meer algemene cloud-diensten lijkt vooralsnog vrijwel beperkt tot bedrijfsmatige of professionele contexten.[30] Het is echter belangrijker om na te gaan wat de behoefte van gebruikers aan controle over hun data is, en hoe ze met die controlemogelijkheden omgaan, dan de gebruiksgegevens van een specifieke technologie te weten. Er zijn rond die vraag inmiddels een aantal studies gedaan die in analogie met de privacy paradox, wijzen op een controle paradox. Dit laat zich het beste uitleggen aan de hand van Facebook.

---

[24] Uit Beieidsverkenning Digitalisering, zoals weergegeven in Offerteverzoek onderzoek eigenaarschap van gegegevens, DG Bestuur en Koninkrijksrelaties, 15 april 2014.
[25] http://www.shawnbuckles.nl/dataforsale/
[26] http://www.ft.com/intl/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz2z2agBB6R
[27] Alle voorbeelden afkomstig uit The Guardian, How much is personal data worth? http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth
[28] http://www.digizeker.nl/hoe-werkt-het/digizeker.html
[29] Zie bijvoorbeeld http://www.thedigitalbeyond.com/online-services-list/
[30] http://www.rightscale.com/lp/2015-state-of-the-cloud-report?campaign=701700000012UP1

Tot 2006 waren de status-updates van Facebookgebruikers alleen zichtbaar voor degenen die ernaar op zoek gingen. Via de in 2006 gelanceerde 'news feed' werden status updates automatisch aan het hele vriendennetwerk aangeboden. De daarop volgende controverse dwong Facebook snel excuus aan te bieden en zijn privacysettings uit te breiden. Er zijn een paar studies over deze affaire verricht en ze tonen alle dat gebruikers het gevoel hadden dat de controle over hun data hen afgenomen was, al veranderde er strikt genomen niets aan de toegankelijkheid (o.a. Boyd, 2008; Hoadley et al., 2010). Brandimarte en collega's (2013) deden naar aanleiding van de Facebook controverses een aantal survey-experimenten. Daarin varieerden ze hoeveel controle mensen hadden over het vrijgeven van gegevens terwijl ze de toegang tot en het gebruik van die gegevens door anderen constant hielden. Hun data suggereren dat mensen meer waarde hechten aan controle over het vrijgeven van hun gegevens, dan over wie toegang hebben tot die gegevens en ze kunnen gebruiken. Dat komt misschien, aldus de onderzoekers, omdat vrijgeven iets is wat je zelf doet, en zichtbaar voor je is, terwijl toegang en gebruik later plaatsvinden en ook niet merkbaar zijn. Daarnaast bleek dat de respondenten zich meer zorgen over hun privacy gingen maken, als ze minder controle over het vrijgeven van informatie kregen, ongeacht wat er met toegang en gebruik gebeurde. De auteurs stellen daarom dat controle over data vrijgeven een illusie van privacy kan geven die niet gebaseerd is op daadwerkelijke afscherming tegenover toegang en gebruik door anderen. Controle over je eigen data, kan dus – net als de TETs hierboven besproken – tot een perverse effect leiden: een groter gevoel van veiligheid dat tot onveiliger gedrag leidt.

Ook onze experts waren van mening dat gebruikers niet altijd de rationele wezens zijn die specifieke privacytechnologieën veronderstellen. Het fenomeen 'digitale kluis' vereist dezelfde inzet en vaardigheden als het lezen van een privacystatement of een opt-in/opt-out keuze. Er is geen reden te denken dat gebruikers door een andere technologie zich plotseling anders gaan gedragen. Bovendien suggereert het onderzoek over de controleparadox dat het discours (beheer je eigen data) en de specifieke terminologie ('kluis') een vals gevoel van zekerheid en zelfbeschikking geven. In een discussie die in 2012 op de site van Bits of Freedom werd gevoerd werden daarnaast nog andere argumenten gegeven; de toegevoegde waarde is klein omdat mensen zeiden hun eigen email al als 'kluis' gebruiken of altijd een datastick bij zich hebben; je persoonlijke data staan opnieuw bij een commercieel bedrijf. Daar kunnen we anno 2015 volgens onze experts aan toevoegen dat er ongeveer maandelijks nieuwe, en naar eigen zeggen betere technieken worden ontwikkeld waarvan men nog maar moet afwachten of het een hype of realiteit is.[31]

## ANTWOORD OP DE ONDERZOEKSVRAAG EN DISCUSSIE

Het probleem van de bovengenoemde scenario's is dat ze alle uitgaan van de behoeften van instanties. Voor privacystatements geldt bijvoorbeeld dat ze zowel dienen om gebruikers te informeren als om aanbieders te vrijwaren van juridische claims (Van Alsenoy e.a. 2014. Ook de aanleiding voor het onderhavige onderzoek ligt in te ontwikkelen beleidskaders en politieke druk. Daarnaast heeft het door overheid en bedrijfsleven bevolkte 'dataveld' zoals in de inleiding geschetst, de neiging achter elke nieuwe privacytechnologie aan te rennen en het als een one-size-

[31] Zie bijvoorbeeld het recente seminar van het Platform Identity Management Nederland over de FIDO Alliance (Fast Identity Online).

fits-all oplossing te zien. Momenteel zijn dat de datakluizen. Dat betekent niet dat er geen rekening met gebruikers wordt gehouden, integendeel: onophoudelijk wordt in het dataveld de vraag gesteld welke gevolgen een privacydienst of –vereiste voor gebruikers heeft (zoals in het onderhavige onderzoek) en hoe deze het beste vormgegeven en uitgelegd kan worden. Daarbij wordt vaak impliciet een rationele gebruiker verondersteld die zowel in staat als bereid is om zich te verdiepen in de verwerking van persoonsgegevens, en daar tijd en inspanning in wenst te investeren. Bestaand onderzoek levert echter geen gegevens op die kunnen voorspellen welke gebruikers dat precies zullen gaan doen, en welke dat zullen gaan laten. Alles blijkt van context afhankelijk (om welke data gaat het, hoe verzameld, met welk doel, in welke sector enzovoort) en noch demografische, noch persoonlijkheids- of lifestyle kenmerken geven daar consistente indicaties voor.

Vanuit het dataveld wordt het perspectief echter zelden zó radicaal omgedraaid dat de problemen die burgers zelf ervaren met hun gegevens en hun privacy het startpunt van de discussie vormen. Overigens blijkt telkens uit het Continu Onderzoek Publieksperspectieven van het SCP dat dataverwerking en privacy niet spontaan opkomen als mensen gevraagd wordt wat precies de grote sociale problemen zijn die opgelost moeten worden.[32] Ook wetenschappers nemen privacy en dataverwerking niet in hun lijstjes op, zo bleek uit een inventarisatie van De Groene in 2011.[33] Als je mensen echter expliciet vraagt naar hun zorgen op dit gebied, dan blijken deze er wel degelijk te zijn. Het gaat dan zowel om algemene gevoelens van privacyverlies, als om concrete bezorgdheid over datakoppeling, function creep en identiteitsfraude. Daarbij geldt dat men lang niet altijd concrete gedragsverandering aan die zorgen koppelt (de beruchte privacyparadox), maar dat is alleen maar onbegrijpelijk als men van übercompetente en rationeel handelende mensen uitgaat. Voor de meesten van ons is het onduidelijk waar we precies toestemming voor geven als we onze data delen, en is ons alledaagse handelen zo rommelig of inconsequent dat we ook geen tijd of zin hebben om daar lang over na te denken. Die dagelijkse praktijk is niet afhankelijk van een specifieke privacy of administratietechnologie en wordt niet opgelost door een digitale kluis of welke andere vorm van controle vooraf.

De tweede consequentie van radicaal omdraaien van het perspectief is dan ook dat men van een slordige en opportunistische burger moet uitgaan. Tellen we daar nog bij op dat in het publieke domein vooral duistere verhalen over identiteitsfraude, datachaos of administratieve fouten circuleren, dan dient een alternatief scenario voor de overheid zich aan waarin men ervan uit gaat dat er iets mis zal gaan met de verwerking van persoonsgegevens en dat men dus over gebruiksvriendelijke, snelle en efficiënte mechanismen moet beschikken om de narigheid die daarmee ontstaat te herstellen; of dat nu in het eigen domein van de overheid is of in een andere context. Juist bij de nieuwe vormen van datakoppeling en datamining die in deze onderzoeksvraag centraal staan, zijn niet alleen transparantie maar ook de mogelijkheden om achteraf in te grijpen en te corrigeren cruciaal voor het gevoel van en de daadwerkelijke controle die gebruikers hebben. Het gaat dan om meer dan alleen herstel van administratieve fouten (zie daarvoor de rapporten van de Nationale Ombudsman maar ook Genova, 2014 en Novay, 2013), maar ook om de ontdekking dat door datakoppeling plotseling gegevens zijn ontstaan die men helemaal niet met de overheid wil

[32] http://www.scp.nl/Onderzoek/Bronnen/Beknopte_onderzoeksbeschrijvingen/Continu_onderzoek_burgerperspectieven_COB

[33] https://www.groene.nl/dossier/350

delen. Vanuit de onvolkomenheden van de burger geredeneerd, en vanuit zijn of haar zorgen is een grotere beleidsinspanning met betrekking tot controle en correctie achteraf misschien wel belangrijker dan het voortouw nemen in digitale kluizen, of welke nieuwe techniek dan ook die zich in 2015 en later zal aandienen. Dat is misschien minder geavanceerd en spectaculair, maar wel meer dienstverlenend.

## GEBRUIKTE LITERATUUR


Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth?. *The Journal of Legal Studies*, *42*(2), 249-274.

Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013, July). Sleights of privacy: Framing, disclosures, and the limits of transparency. In Proceedings of the Ninth Symposium on Usable Privacy and Security (p. 9). ACM.

Ancker, J. S., Silver, M., Miller, M. C., & Kaushal, R. (2012). Consumer experience with and attitudes toward health information technology: a nationwide survey. *Journal of the American Medical Informatics Association*, amiajnl-2012.

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, *31*(5), 661-681.

Bansal, G., Zahedi, F. M., Gefen, D. (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, *Decision Support Systems* 49: 138-150, doi: 10.1016/j.dss.2010.01.010.

BCG (2013). *The value of our digital identity*. Boston Consultancy Group, Liberty Global Policy Series.

Beldad, A. (2011). *Trust and information privacy concerns in electronic government* [Dissertation]. Enschede, NL: University of Twente.

Beldad, A., de Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. *The information society, 27*(4), 220-232.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313-324.

Big Brother Watch (2014). Defending civil liberties, protecting privacy. Annual Review. http://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/02/annual-review.pdf, last accessed March 30, 2015.

Boonstra, A., Boddy, D. and Bell, S. (2008). Stakeholder management in IOS projects: analysis of an attempt to implement an electronic patient file. *European Journal of Information Systems, 17*(2), 100-111.

Boyd, D. (2008). Facebook\'s Privacy Trainwreck. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13-20.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science,* 4(3), 340-347.

Cameron, D., Pope, S. & M Clemence (2014). Dialogue on data. Exploring the public's views on using administrative data for research purposes. IPSOS MORI, Officie of National Statistics, Economic and Social Research Council, UK. http://www.esrc.ac.uk/_images/Dialogue_on_Data_report_tcm8-30270.pdf, per 20 februari 2015.

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *New Media & Society*, *11*(3), 395-416.

Clarke, R. (1999). Introduction to dataveillance and information privacy, and definitions of terms. Roger Clarke's Dataveillance and Information Privacy Pages., http://www.rogerclarke.com/DV/

Cranor, L. F., Reagle, J. and Ackerman, M. S. (2000). *Beyond concern: Understanding net users' attitudes about online privacy* (pp. 47-70). Cambridge, MA: MIT Press.

Cuijpers, C. M. K. C., van Veenstra, A. F., Roosendaal, A. P. C., & Bakker, T. (2012). *I-overheid, burgers in beeld*. TNO Rapport.

Das, M., & Couper, M. P. (2014). Optimizing Opt-Out Consent for Record Linkage. *Journal of Official Statistics*, *30*(3), 479-497.

DeCew, Judith, "Privacy", *The Stanford Encyclopedia of Philosophy* (Fall 2013 Edition), Edward N. Zalta (ed.), URL = <http://plato.stanford.edu/archives/fall2013/entries/privacy/>.

ECP (2014). Online gemak belangrijker dan privacy. Onderzoeksrapport Platform voor de Informatiesamenleving. http://ecp.nl/actueel/4288/online-gemak-belangrijker-dan-privacy.html.

*Eurobarometer, S. (2011). Attitudes on data protection and electronic identity in the European Union."* Brussels: European Commission, Directorate-General for Communication. Special Barometer 359.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European data protection: coming of age* (pp. 3-32). Springer Netherlands.

Genova, M. (2014). *Komt een vrouw bij de hacker. Hoe je identiteit gestolen kan worden*. Veltman Uitgevers.

Hildebrandt, M., & Koops, B. J. (2010). The challenges of ambient law and legal protection in the profiling era. *The Modern Law Review*, *73*(3), 428-460.

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications, 9*(1), 50-60.

Hoy, M. G. and Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45.

Infosys (2013). Engaging with digital consumers. They are ready, are you? http://www.infosys.com/marcom/digital-consumer-study/default.asp, last accessed July 14, 2014.

Janic, M., Wijbenga, J. P., & Veugen, T. (2013, June). Transparency enhancing tools (TETs): an overview. In Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on (pp. 18-25). IEEE.

Jansen, T., Koppes, L.L., Reitsma-van Rooijen, M., Verheij, R. (2015). *Elektronische gegevensuitwisseling in de zorg: ervaringen en opvattingen van zorgverleners en zorggebruikers***.** Utrecht: NIVEL, 2015. 56 p.

Junglas, I. A., Johnson, N. A. and Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.

Kolsaker, A. and Payne, C. (2002). Engendering trust in e-commerce: a study of gender-based concerns. Marketing Intelligence & Planning, 20(4), 206-214.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), 15-24.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802-5805.

Lai, Y. L., & Hui, K. L. (2006, April). Internet opt-in and opt-out: investigating the roles of frames, defaults and privacy concerns. In *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research: Forty four years of computer personnel research: achievements, challenges & the future* (pp. 253-263). ACM.

Marwick, A.E. (2013). *Status Update: Celebrity, Publicity, and Branding in the Social Media Age*. New Haven: Yale University Press.

Mazurek, M. L., Klemperer, P. F., Shay, R., Takabi, H., Bauer, L., & Cranor, L. F. (2011, May). Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2085-2094). ACM.

Milne, G. R., & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing, 19*(2), 238-249.

Moreman, C. M., & Lewis, A. D. (Eds.). (2014). *Digital Death: Mortality and Beyond in the Online Age*. ABC-CLIO.

Norval, A.J. and Prasopoulou, E. (2012). Living in the biometric state: Examining citizen engagement with new identification technologies. 7th International Conference in Interpretive Policy Analysis (IPA 2012). Understanding the drama of democracy: Policy work, power and transformation, 5th - 7th July, Tilburg, Netherlands.

Novay (2013). *Correctie van persoonsgegevens*. Organisatieoverschrijdende aanpak van probleemgevallen. Onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Centraal Meldpunt Identiteitsfraude en –fouten.

O'Donnell, H. C., Patel, V., Kern, L. M., Barrón, Y., Teixeira, P., Dhopeshwarkar, R., & Kaushal, R. (2011). Healthcare consumers' attitudes towards physician and personal use of health information exchange. *Journal of general internal medicine, 26*(9), 1019-1026.

Robbin, A. (2001). The loss of personal privacy and its consequences for social research. *Journal of Government Information*, *28*(5), 493-527.

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research, 57*(9), 1000-1011.

Rowan, M., & Dehlinger, J. (2014). Observed Gender Differences in Privacy Concerns and Behaviors of Mobile Device End Users. *Procedia Computer Science*, *37*, 340-347.

Sanquist, T. F., Mahy, H. and Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk analysis*, *28*(4), 1125-1133.

Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, *27*(1), 45-52.

Sheehan, K.B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. Journal of Interactive Marketing, 13(4), 24-38.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*(1), 21-32.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, *19*(1), 62-73.

Smith, E. and Lyon, D. (2013). Comparison of Survey Findings from Canada and the USA on Surveillance and Privacy from 2006 and 2012. *Surveillance & Society, 11.*

Takano, Y., Ohta, S., Takahashi, T., Ando, R., & Inoue, T. (2014, July). MindYourPrivacy: Design and implementation of a visualization system for third-party Web tracking. In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on* (pp. 48-56). IEEE.\

Tsai, J., P. Kelley, P. Drielsma, L. Cranor, J. Hong, and N. Sadeh. Who's Viewed You? The Impact of Feedback in a Mobile-location System. CHI 2009.

Turner, G., van Zoonen, L., & Harvey, J. (2014). Confusion, control and comfort: premediating identity management in film and television. *Information, Communication & Society, 17*(8), 986-1000.

Van Alsenoy, B. van, Kosta, E., & Dumortier, J. (2014). Privacy notices versus informational self-determination: Minding the gap. *International Review of Law, Computers & Technology*, *28*(2), 185-203.

Van Thiel, L. (2009). Evaluatie Elektronisch Patientendossier. TNS NIPO. http://www.hemochromatose.nl/documents/pdf-bestanden/epd-eindrapport-tns-nipo-npcf.pdf.

Van Zoonen, L. 1998, "Ethics of Making Private Lives Public." in *The Media in Question: Popular Cultures and Public Interests.* , eds. K. Brants, J. Hermes & L. van Zoonen, Sage, London.

Van Zoonen, L., & Turner, G. (2013, November). Taboos and desires of the UK public for identity management in the future: findings from two survey games. In *Proceedings of the 2013 ACM workshop on Digital identity management* (pp. 37-44). ACM.

Van Zoonen, L. e.a. (2014). What do users want from their future means of identity management? Final report. http://imprintsfutures.org/assets/images/pdfs/End%20report%20IMPRINTS.pdf

Vaniea, K., L. Bauer, L.F. Cranor, and M.K. Reiter. Out of sight, out of mind: Effects of displaying access-control information near the item it controls. In *Proceedings of the Tenth Annual Conference on Privacy, Security and Trust*, July 2012.

Young, A. L., & Quan-Haase, A. (2013) Privacy Protection Strategies on Facebook. *Information, Communication and Society* 16(4): 479–500, doi:10.1080/1369118X.2013.777757.

Zhang, R., Chen, J. Q., & Lee, C. J. (2013) Mobile Commerce and Consumer Privacy Concerns, *The Journal of Computer Information Systems* 53(4): 31–38.

Zukowski, T., & Brown, I. (2007) Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns, *South African Institute for Computer Scientists and Information Technologists*, 197–204.

## Bijlage 1. Aanpak

Deze onderzoeksrapportage is gebaseerd op drie onderdelen: een literatuurstudie, een secundaire analyse van survey-gegevens uit 2010, en expertgesprekken.

Te beginnen met de literatuurstudie, is er gezocht naar bestaand onderzoek over gevoelens van privacy en het koppelen van gegevens. Over dit laatste onderwerp bleek nog opvallend weinig wetenschappelijk onderzoek te zijn gedaan. Bij het doorzoeken van de bestaande literatuur was de werkwijze van breed, zoals algemene studies over privacy zorgen en gebruikers, naar meer specifiek, zoals informatie over contexten van privacy en e-overheden. Gevonden artikelen die relevant bleken te zijn voor de onderzoeksvraag van het Ministerie werden samengevat en geclusterd naar overkoepelende thema's. Hieruit werden ten slotte de belangrijkste uitkomsten gehaald, welke terug zijn te vinden in dit rapport.

De secundaire analyse van survey-gegevens betrof een analyse van de Eurobarometer survey-data, verzameld in 2010 in 27 EU landen. Deze speciale Eurobarometer bevatte, onder andere, vragen rondom het thema 'Databeveiliging en elektronische identiteit'. Zo werden de respondenten bijvoorbeeld gevraagd naar hun internetactiviteiten, hun mening over bepaalde typen informatie en naar welke gegevens zij als persoonlijk beschouwen. Daarnaast werden de attitudes van de respondenten verzameld met betrekking tot het verwerven, behandelen, bewaren en beschermen van persoonlijke gegevens door publieke en private organisaties. Uit de Eurobarometer zijn eerst de vragen die relevant waren voor de onderzoeksvraag van het Ministerie geselecteerd. Nadat primaire analyses voor deze variabelen waren uitgevoerd, werden twee variabelen nader onderzocht. De variabele 'vertrouwen in nationale publieke instanties' is nader geanalyseerd om te zien met welke andere variabelen dit samenhangt. Ook is het online privacygedrag van mensen verder onderzocht, om te zien of we aan de hand van andere variabelen zouden kunnen voorspellen in hoeverre mensen hun privacy beschermen op het internet. Een uitgebreide beschrijving van de manier waarop dit onderzocht is en andere informatie over de analyse van de Eurobarometergegevens is te vinden in Appendix II.

Het laatste gedeelte van het onderzoek bestond uit het houden van gesprekken met experts. De experts zijn geworven middels het professionele netwerk van de onderzoeker en tijdens een evenement over online identiteit[34], en zijn benaderd op basis van hun professionele expertise en ervaring met betrekking tot privacy gevoelige gegevens en zorgen hierom. Ze spraken niet namens hun organisatie. De experts waren divers in hun achtergrond; een expert was bijvoorbeeld werkzaam in de medische sector terwijl een andere expert in de financiële sector werkte. In de gesprekken werden de voorlopige uitkomsten en de ontwikkelde scenario's getoetst aan de ervaring en mening van de experts. Dit leidde zowel tot bevestiging van de bevindingen als tot interessante nieuwe inzichten. De onderstaande tabel laat een overzicht zien van de experts die wij geconsulteerd hebben.

[34] Evenement over Fast IDentity Online (FIDO), georganiseerd door het Platform Identity Management Nederland.

| Naam | Organisatie |
|---|---|
| **Henk van Cann** | 2Value |
| **Ruud Huijts** | Consultant |
| **Jaap Kuijpers** | Platform Identity Management Nederland |
| **Erik van der Laan** | Nationale Nederlanden |
| **Marc van Lieshout** | TNO |
| **Wouter Tesink** | VZVZ |
| **Maarten Wegdam** | InnoValor |
| **Marleen Stikker** | Centrum De Waag |
| **Robert Garskamp** | Platform E-ID |