# PRIVACY ZAT

Informationele privacy herzien
met de kritische blik van Foucault

Iris van der Spoel

# PRIVACY ZAT

Informationele privacy herzien
met de kritische blik van Foucault

Iris van der Spoel
0328898

Master Nieuwe Media en Digitale Cultuur
Universiteit Utrecht
Thesis
Begeleider: M.T. Schäfer
15 augustus 2012

Omslagontwerp: Niki Padidar

*“Mark Zuckerberg won’t stop until he owns a photo of everybody’s anus.*
*That’s what this is all leading to. That’s the masterplan.”*

Charlie Brooker op Twitter
9 april 2012

# Inhoudsopgave

# Dank

Het produceren van deze masterscriptie heeft zat tijd gekost. Daarom houd ik het hier kort.
Mijn dank gaat uit naar iedereen die mij heeft gesteund en geholpen tijdens het schrijven van deze scriptie; inhoudelijk, geestelijk, thuis, op het werk, of in de kroeg mij afleidend van de studie waar ik eigenlijk mee bezig had moeten zijn. In het bijzonder wil ik de volgende mensen bedanken: mijn stagebegeleider Joost Raessens die me heeft geholpen aan een door mij zeer gewilde stage bij de VPRO, waarop een geweldig leuke baan volgde die uiteindelijk ook voor alle vertraging in het schrijven van mijn scriptie heeft gezorgd. Het was het waard. Mijn scriptiebegeleider Mirko Tobias Schäfer die in de afgelopen twee jaar iedere keer als ik weer zijn werkkamer binnenstapte met de mededeling dat ik mijn scriptie nu écht af ging maken, mij telkens met hetzelfde enthousiasme ontving en hielp mijn ideeën op de rails te krijgen. Totdat het er wonder boven wonder ook daadwerkelijk van kwam.
In het bijzonder gaat mijn dank uit naar mijn ouders, die mij in de mogelijkheid stelden om al die jaren te kunnen studeren, zelfs als ik dat effectief gezien niet deed. Ik dank jullie hartelijk.

Rotterdam,
15 augustus 2012

# Inleiding

In februari 2010 onderwierpen twee redacteuren van NRC Next zich aan een experiment: een week zonder Google leven. Dit deden zij als reactie op een interview met mediatheoreticus Geert Lovink in dezelfde krant, waarin werd verwezen naar zijn kritiek op Google's zogenoemde "data-obesitas": het verzamelen van gebruikersgegevens om daaraan geld te verdienen door ze door te verkopen aan adverteerders (Teffer 2010). In zijn essay 'The society of the query and the Googlization of our lives' uit 2008 wijst Lovink op Google's zucht naar informatie, waarbij het bedrijf niet gestoord door enige idealistische drijfveer om bijvoorbeeld met het Google Books-project ons cultureel erfgoed digitaal beschikbaar te maken, slechts bezig zou zijn met het genereren van zoveel mogelijk advertentieinkomsten door middel van die informatie. In het interview in NRC Next en in het essay van Lovink wordt Google neergezet als een datamoloch die met al onze persoonlijke gegevens opgeslagen op hun servers en gedreven door een zucht naar advertentiegelden een potentiële bedreiging voor onze privacy zou vormen. En dit was slechts een van de gevaren waaraan Google met haar ondoorzichtige bedrijfsstrategieën ons zou onderwerpen, aldus Lovink.

De jongens van NRC Next wilde wel eens zien of we überhaupt nog zonder die diensten van Google konden leven. Hadden we ons niet massaal vrijwillig afhankelijk gemaakt van het bedrijf? Ze hielden het geen week vol. Als fervente gebruikers van Google Calendar, Gmail en YouTube stuitten ze continue op beperkingen in hun dagelijkse routine. Wat bij mij de vraag deed rijzen: moeten we ons niet afvragen of we die gegevens dan niet uit handen wíllen geven in ruil voor die

nuttige, gratis diensten waar we zo graag gebruik van maken? Immers bestaan ze bij de gratie van de gegevens die wij erin stoppen.

Vanuit deze gedachte schreef ik een artikel waarin ik stelde dat de diensten zoals Gmail, Google Maps, de browser Chrome en de zoekmachine juist zo goed functioneren vanwege de door ons 'achtergelaten' gegevens tijdens het gebruik ervan. Die worden gelijktijdig gebruikt om de diensten te optimaliseren en eraan te verdienen. Juist omdat Google ons niet goed informeert vanwege bijvoorbeeld lange, complexe teksten in gebruikersovereenkomsten, zijn ze groot geworden, zo schreef ik. Want wie zou de vraag of zijn gegevens doorverkocht mogen worden aan adverteerders van nature willen beantwoorden met 'ja'? In onze onwetendheid maakten we dankbaar gebruik van de functionaliteit waarvan we steeds meer afhankelijk leken te worden, zo bewezen de redacteuren van NRC Next. Dat maakte Google machtig, onderkende ook ik in het stuk. Maar zo'n groot en vooraanstaand bedrijf kon mijns inziens geen eindeloze macht hebben. Immers als ze de fout in zouden gaan, zou het ze de kop kosten. We waren uiteindelijk allemaal vrij om dan over te stappen naar andere aanbieders van zoekmachines, e-mailaccounts en digitale kaarten. Mijn conclusie luidde dat we, voordat we over een schending van onze privacy begonnen, eerst maar eens goed moesten nadenken over wat we onder privégegevens verstaan; zijn we immers niet bereid ze af te staan als we daarmee mogen toetreden tot het 'Google-universum'? En hoe privé zijn die gegevens dan?

Het artikel werd als opiniestuk gepubliceerd in NRC Next op 9 maart 2010. Veelgehoorde kritiek was dat ik over het hoofd had gezien dat er een gebrek aan bewustzijn was onder veel

gebruikers over de hoeveelheid en gevoeligheid van de informatie die ze afstonden: namen van contactpersonen en hun e-mailadressen, persoonlijke en zakelijke correspondentie en welke websites ze hebben bezocht om maar een paar voorbeelden te noemen. En dat gaven we allemaal in handen van één bedrijf. Dat gaf Google macht, en hoewel ik dat niet ontkende, moest ik wel degelijk vraagtekens zetten bij onze afhankelijkheid van het bedrijf. Als gebruikers bevonden we ons in een bijzonder kwetsbare positie. Met Google als eigenaar van onze e-mails, video's op YouTube en foto's op Picasa, gaven we de controle over onze data uit handen. Wat als Google de kraan zou dichtdraaien? In theorie waren we vrij om Google's diensten wel of niet te gebruiken. In de praktijk werden de door ons ingevoerde gegevens al op tientallen servers opgeslagen en doorverkocht, was het volstrekt onoverzichtelijk wat de gevolgen waren van zo'n bron aan informatie in handen van één bedrijf en waren we voor tientallen dagelijkse gebruiken afhankelijk van een commerciële partij. Alle kritiek kon in een paar woorden worden samengevat: naïef en slecht geïnformeerd.

Nu twee jaar later kan ik niet anders dan het eens zijn met veel van de commentaren die op het artikel verschenen. Mijn doel was om de *googlization* positief te benaderen door te wijzen op de voordelen van kosteloze, gebruiksvriendelijke diensten die ons steeds beter konden bedienen doordat ze ons leerden 'kennen' uit de door ons ingevoerde informatie. Maar mijn argument dat we daarvoor maar bereid moesten zijn onze privégegevens in te ruilen, kwam voort uit een bijna dogmatische manier van anti-conservatief denken die ik aan mezelf had opgelegd. Ik wilde per se niet in de behoudende hoek gaan zitten waarvan ik vreesde dat men van daaruit zou redeneren op basis van angst voor nieuwe media, iets

waartegen Lisa Gitelman me had gewaarschuwd in de introductie van *Always Already New* (2006) die ik tijdens mijn studie onder ogen had gekregen. Ik formuleerde een standpunt waarmee ik Google zou omarmen vanuit het idee dat er naast de twee journalisten van de krant nog miljoenen anderen internetters niet meer zonder Google zouden kunnen leven.

Nu zou ik niet meer willen beweren dat een eenentwintigste eeuws productenpakket zoals dat van Google alleen kan gedijen als wij bereid zijn onze persoonlijke informatie ervoor op te geven. Maar dat neemt niet de vraag weg wat we nu precies verstaan onder die privégegevens. En daarmee, wat de betekenis is van privacy in een informatiemaatschappij.

**Een hele korte geschiedenis van het begrip privacy**

Wat men precies verstaat onder privacy is door de jaren heen veranderd. Het privédomein stond eerst nog voor de huishoudelijke sfeer die strikt gescheiden werd gezien van de openbare sfeer van het politieke handelen. Het huiselijke, wat werd gelieerd aan de verantwoordelijkheid van de vrouw en de noodzakelijke voortplanting werd inferieur geacht aan de publieke zaak omdat die daarvoor geen enkele relevantie had. Later ontstond de opvatting van privacy, waarbij het private ook buiten het huishoudelijke een plaats krijgt. Als mijlpaal voor het ontstaan van ons huidige privacybegrip wordt vaak een essay van de Amerikaanse rechters Warren en Brandeis uit 1890 aangehaald waarin het recht om met rust gelaten te worden voor het eerst wordt omschreven als een wettelijk recht op privacy. Hierbij wordt informatie over een individu geacht beschermd te worden, zelfs als die informatie voortkomt uit iets wat zich publiekelijk afspeelt. De betekenis van privacy hangt hier sterk samen met het idee van

persoonlijke vrijheid. Het Westerse eenentwintigste eeuwse privacybegrip wordt volgens verschillende bronnen nog steeds bepaald door dit streven naar persoonlijke vrijheid. Maar tegelijkertijd wordt duidelijk dat er niet één geschiedenis van privacy is: de idee van privacy kan betrekking hebben op het zich kunnen terugtrekken in een bepaalde ruimte, op zelfbeschikkingsrecht over het lichaam of op informatie. En daarbuiten maakt het idee van privacy niet overal ter wereld dezelfde ontwikkeling door (Roessler 2006, Solove 2008).

De vragen die Geert Lovink, de redacteuren van NRC Next en ik in mijn artikel stellen hebben betrekking op het debat over wat Roessler informationele privacy noemt: het recht om als individu met rust gelaten te worden en de controle te hebben over welke persoonlijke gegevens wanneer en bij wie terecht komen (704-5). Het debat wordt gekenmerkt door een focus op de bedreigingen en gevaren voor die informationele privacy, onder andere als gevolg van toegenomen opslag- en distributiemogelijkheden van gegevens, een gebrek aan (wetgeving ter) bescherming van gegevens, te weinig transparantie over deze twee zaken en over verlies van controle over informatie (Boyd 2010, Solove 2004, De Vries 2009, Kirkpatrick 2010).

Zoals gezegd wijst Roessler op de verschillende betekenissen van privacy in samenhang met de historische context waarin er over het begrip wordt nagedacht. Maar ook op een minder algemeen niveau lijkt ‘context’ het sleutelwoord als het op informational privacy aankomt. Danah Boyd zegt in haar artikel ‘Why Privacy is Not Dead’ (2010) dat privacy niet alleen te maken heeft met de controle over de toegang tot gegevens maar vooral om het begrijpen van de sociale context waarin er met die gegevens omgesprongen wordt. Mancini et al. (2009)

deden vanuit diezelfde gedachte onderzoek naar informationele privacy bij het gebruik van online mobiele apparaten: op welke plaats bevinden mensen zich in de fysieke ruimte als ze statusupdates plaatsen op Facebook, met wie waren ze en wat was de reden dat ze een update plaatsten? Helen Nissenbaum komt in Privacy in Context (2010) zelfs tot de conclusie dat gevoeligheid voor nuances in actoren en normen in een situatie *"...means resisting, once and for all, the idea of public information..."* (216). Met andere woorden, informatie is niet in zichzelf publiek of privé maar krijgt die lading puur op basis van de context waarin hij wordt verspreid.

**Opbouw**

Het opiniestuk in NRC Next vormt de aanleiding voor deze masterthesis. Die korte vermeende bespiegeling over privacyschending door Google vormde de aanzet voor de grotere vraag wat informationele privacy online nou eigenlijk betekent.
In deze scriptie pak ik de vraag op die aan het einde van mijn artikel blijft liggen en zal ik onderzoeken wat informationele privacy betekent in een maatschappij met een sterk ontwikkelde online infrastructuur.

In het eerste deel zet ik de verschillende posities uiteen die zich in het huidige debat omtrent online informationele privacy gevormd hebben. Omdat een goed begrip van de maatschappelijke context van belang is om invulling te kunnen geven aan de betekenis van privacy, zal ik eerst de belangrijkste kenmerken van die context benoemen. Ik typeer deze naar een term van Frans Vogelaar als een 'hybride ruimte'; de samenkomst van de fysieke wereld en daaroverheen gelegde communicatienetwerken (Vogelaar

2012). Of simpeler gezegd, de versmelting van de offline en de online ruimte. In deze context plaats ik het privacydebat, waarin de posities grofweg uiteenlopen van privacy als een nastrevenswaardig ideaal tot een idee wat per definitie zou moeten worden losgelaten. Dit laatste laat zich de post-privacy positie noemen. De standpunten tonen een klassiek onderscheid tussen een behoudende en een progressieve houding ten opzichte van een relatief nieuw fenomeen.

Vervolgens zal ik in het tweede deel op zoek gaan naar de ideeën waaraan deze posities ten grondslag liggen. Ik bespreek een in de literatuur veel gemaakte vergelijking van privacyschending met het panopticum en Michel Foucault's uitwerking daarvan in het panopticisme. Langs deze weg kom ik uiteindelijk bij een ander begrip uit de filosofie van Foucault, te weten biopolitiek.

Uiteindelijk zal ik in het derde deel afstappen van de uitkijktoren waarvandaan ik de verschillende theorieën heb bezien en zal ik zelf positie innemen in het online privacylandschap. Omdat ik zelf in mijn artikel uit 2010, zoals ik eerder al aangaf, een aan mezelf opgelegde progressieve positie innam, ben ik het in deze verhandeling aan mijzelf verplicht hier die progressieve houding serieus te heroverwegen in mijn analyse. Dit maal wordt er genoeg tegenwicht geboden door de meer behoudende opvatting van privacy als een nastrevenswaardig ideaal en 'kritische blik' van Foucault, om tot een mijns inziens weloverwogen opvatting van informationele privacy te komen.

# Privacydebat in de hybride ruimte

*In dit hoofdstuk worden de verschillende posities in het actuele debat omtrent informationele privacy uiteengezet. Eerst worden de relevante kenmerken van de maatschappelijke context waarin het debat plaatsvindt geschetst. Deze context laat zich sterk typeren door de idee van de hybride ruimte: de versmelting van de fysieke ruimte met netwerken van online communicatie. Het inzichtelijk maken van deze eigenschappen biedt handvatten om de lijnen waarlangs het actuele privacydebat zich ontwikkelt te begrijpen. Vervolgens bespreek ik dan ook de verschillende posities in het privacydebat.*

De meeste literatuur over de hybride ruimte in de betekenis van de samenkomst van de fysieke werkelijkheid en digitale communicatienetwerken is geschreven voor 2007. Hoewel het concept betrekking heeft op een rap veranderend medialandschap, blijken de toen omschreven basisprincipes zes jaar later nog steeds relevant. De toepassingen van communicatie- en informatietechnologie hebben zich echter verder ontwikkeld en hun sporen in de sociaal-culturele context nagelaten, wat betekent dat het concept wel dient te worden herzien en waar nodig naar aanvullende literatuur moet worden gezocht. Om een paar voorbeelden te noemen; Apple's revolutionaire iPhone kwam pas in 2007 op de markt en het alomtegenwoordige gebruik van sociale media zoals Facebook en Twitter is ook iets van na deze tijd. Ik wil toewerken naar een hedendaags begrip van het concept hybride ruimte, om het actuele privacydebat daarin te kunnen plaatsen en uiteindelijk de betekenis van informationele privacy daarin vorm te kunnen geven.

## Hybride ruimte

In 2006 verscheen een nummer van het tijdschrift voor kunst en architectuur *Open* met als thema 'Hybride ruimte'. Verschillende sociologen, mediawetenschappers en architecten geven hierin hun visie op hoe draadloze media de publieke ruimte mobiliseren en daarmee vormen zij een definitie van de hybride ruimte. Voor de constructie van de hybride ruimte zien zij een rol weggelegd voor kunst en architectuur, maar in de basis komt deze ruimte voort uit een versmelting van de fysieke werkelijkheid met netwerken van communicatie. Mediatheoreticus Erik Kluitenberg spreekt van een ruimte

> "waarin het publieke op een nieuwe wijze wordt geconfigureerd door een veelheid van media- en communicatienetwerken die zich met de sociale en politieke functies van die ruimte verweven tot een zogenaamde hybride ruimte. Over de traditionele ruimte zijn elektronische netwerken gelegd zoals die van mobiele telefoons en andere draadloze media. Deze stapeling vormt een zeer instabiel, ongelijkmatig en voortdurend veranderend systeem." (Kluitenberg 2006, 8)

De hybride ruimte ontstaat dus uit een combinatie van wat we traditioneel als de fysieke ruimte kennen en de (draadloze) media die daarin aanwezig zijn. Zoals Frans Vogelaar en Elizabeth Sikiardi in hetzelfde nummer schrijven, zijn deze ruimten

> "tegelijkertijd analoog en digitaal, virtueel en materiaal, lokaal en mondiaal, tastbaar en abstract (85)." Voorbeelden van waar die hybride ruimte zich manifesteert zijn "eilandjes van privé-ruimte", gecreëerd door bijvoorbeeld een mobiel

> telefoongesprek in de openbare ruimte en in “beveiligde omgevingen waar camera’s toezicht houden op open stedelijke gebieden (84).”

Mediawetenschapper Lev Manovich publiceerde in 2006 een artikel over *augmented space* in het tijdschrift *Visual Communication*. Hoewel hij een andere term gebruikt sluiten zijn observaties aan bij wat bovenstaande auteurs een paar jaar later over de hybride ruimte schrijven. Hij omschrijft *augmented space* als de fysieke ruimte bedekt met een laag dynamisch veranderende informatie. Technologie zorgt ervoor dat de informatie dynamisch aan de fysieke ruimte wordt toegevoegd: zoals via interfaces van mobiele telefoons en beeldschermen die CCTV-registraties of commerciële boodschappen vertonen. Ook wordt er informatie aan de ruimte onttrokken, bijvoorbeeld wanneer beveiligingscamera’s opnames maken. De *augmented space* is volgens Manovich dus bij uitstek een informatieruimte: *dataspace* (226). Ook hij legt hij de de nadruk op de rol van architectuur in de constructie van de hybride ruimte en de manifestatie ervan in kunst, waarmee Manovich aansluit bij Kluitenberg en bij Vogelaar en Sikiardi.

Maar waar Kluitenberg nog spreekt van een soort laag die over de traditionele ruimte heen is gelegd, gaat de versmelting naarmate de jaren vorderen en de technologie zich ontwikkelt steeds verder. De interfaces worden kleiner, individuele gebruikers krijgen ze in handen en volgens Manovich zal dat bijdragen aan de *augmentation* van de ruimte zelf (224-5). Daarmee wordt die ruimte dus daadwerkelijk hybride: de technologie wordt steeds minder zichtbaar. Kluitenberg wierp een paar jaar geleden al op dat de technologie daarmee ook uit het bewustzijn ging verdwijnen en een vanzelfsprekendheid

zou worden (13). De voorwaarde voor de *dataspace* is niet langer de met technologie aangevulde architectuur, maar een functionerende infrastructuur waarop individuele gebruikers kunnen intappen. Die maakt een daadwerkelijke versmelting van de offline en online wereld mogelijk. De sleutelbegrippen hierbij zijn mobiliteit en connectiviteit.

*Mobiliteit*

Wat de *augmented space* van Manovich als informatieruimte fundamenteel doet verschillen van de hybride ruimte, zijn volgens communicatiewetenschapper Adriana De Souza e Silva de fysieke en sociale verbanden die daarin vorm krijgen (De Souza e Silva 2006). De hybride ruimte bestaat volgens haar niet alleen uit technologie. De Souza e Silva gebruikt mobiele telefoons als voorbeeld. Hiermee kunnen we vanuit de ruimte waarin we ons bevinden contact maken met iemand in een andere ruimte. Zo kunnen we de verschillende ruimten in elkaar laten overvloeien. We gebruiken mobiele telefoons zo om een sociale laag aan de fysieke ruimte toe te voegen. En dat doen we niet meer alleen door te bellen. Waar Kluitenberg in 2006 nog schrijft dat e-mailen met mobiele telefoons “erg omslachtig” is, heeft de smartphone dat in 2012 makkelijk gemaakt. Om nog maar te zwijgen van het gemak waarmee we online sociale netwerksites en andere sociale toepassingen betrekken in de fysieke werkelijkheid.

*Connectiviteit*

Door ons vertrouwen op het functioneren van mobiele apparaten is de hybride ruimte afhankelijk geworden van een bepaalde mate van connectiviteit. Zowel De Souze e Silva als Kluitenberg wijzen hierop. Laatstgenoemde geeft nadrukkelijk het belang aan van juist de discontinuïteit van de connectiviteit, die de grenzen van de hybride ruimte bepaalt.

Adrian Mackenzie geeft een mooi voorbeeld van hoe deze discontinuïteit de hybride ruimte voelbaar maakt. In zijn bijdrage aan het boek *Mobile Technologies of the City* (2006) schrijft hij hoe hij er niet in slaagde met zijn laptop verbinding te maken met internet op Picadilly Circus, een plek die in Londen volgens Mackenzie juist bekend staat als Wi-Fi hotspot. Hier verwachtte hij dus zeker een internetverbinding tussen het netwerk en zijn computer tot stand te kunnen brengen. Wanneer dit niet lukt, voelt hij de grenzen van de hybride ruimte.
Hij kent een creërende rol toe aan Wi-Fi netwerken voor het stadslandschap. Die netwerken leggen een onzichtbare laag op de geografische kaart van de ruimte, waar mobiele apparaten zoals laptops en PDA's hun online functionaliteit vandaan halen. Mackenzie spreekt van een *landscape of data transmission* (141) of van *dataflows* (142). Op dezelfde manier zijn de mobiele telefoons uit het voorbeeld van De Souza e Silva voor hun functioneren afhankelijk van het telefoonnetwerk. De smartphone heeft e-mailen met de mobiele telefoon dan wel makkelijk gemaakt, maar is daarvoor afhankelijk van een functionerend WiFi-netwerk of 3G-verbinding. Als het netwerk niet functioneert worden de grenzen van de hybride ruimte voelbaar en Mackenzie's voorbeeld maakt duidelijk dat we als gebruikers zijn gaan vertrouwen op het functioneren van de ruimte als informatieruimte.

*Social space*

We kunnen dus zeggen dat de hybride ruimte als *dataspace* afhankelijk is van mobiliteit van apparaten en de mate van connectiviteit van het netwerk. Zoals gezegd zijn de basisprincipes van de auteurs in kwestie nog altijd van toepassing op de hybride ruimte in zijn huidige vorm. Maar nu

die *dataflows* zo'n vanzelfsprekendheid zijn geworden, is het van belang ze ook eens inhoudelijk te bekijken. Dan zien we snel dat er een belangrijke rol voor sociale media is weggelegd.

Sociale netwerksites hebben een sterke ontwikkeling doorgemaakt de afgelopen jaren. Facebook groeide van 7 miljoen gebruikers in 2006 tot 955 miljoen maandelijks actieve gebruikers in juni 2012 (Vogelstein 2007, Facebook 2012). Facebook is niet alleen een sociale netwerksite die mensen online met elkaar verbindt, maar zorgt er tevens voor dat sociale media in het DNA van het internet terecht zijn gekomen. Facebook's Like-knop is al sinds april 2010 een manier voor gebruikers om met hun netwerk te delen in wat voor content op externe websites ze geïnteresseerd zijn. Maar sinds 2012 kunnen we ook volgen wat iemand gelezen of bekeken heeft op een website die deze informatie via apps deelt op je Facebookprofiel. Als men Facebook koppelt aan muziekstreamingdienst Spotify kunnen Facebookcontacten onderling live zien waar ze naar luisteren en steeds vaker wordt het mogelijk om voor het gebruik van verschillende diensten in te loggen met gebruikersnaam en -wachtwoord van Facebook. Een speciaal account aanmaken bij een aanbieder, om bijvoorbeeld een spelletje op je telefoon te kunnen spelen, is dan niet langer nodig en hiermee kunnen je spelactiviteiten gelijk weer sociaal worden. De *dataspace* is voor een deel dus ook een *social space* geworden.

**Het debat in context**

Al met al is een informatieruimte met een sterke sociale component bij uitstek een ruimte waarin informatie aan gebruikers wordt gestuurd maar waar evengoed data aan worden onttrokken. Volgens Manovich maakt dit de hybride

informatieruimte ook een ‘gemonitorde ruimte‘ (223). En dat wekt argwaan. Ook Helen Nissenbaum wijst daarop in *Privacy in Context* (2010), maar ook noemt zij na *monitoring* en *tracking* het opslaan, analyseren en distribueren van data.

> “Information can be compressed, sorted, manipulated, dicovered, and interpreted as never before, and thus can be more easily transformed into useful knowledge.” (Nissenbaum 37).

Bedrijven kunnen die kennis over gebruikers uit verschillende databanken combineren en verkopen aan bijvoorbeeld marketeers (45). Maar doordat de informatie op het web is gedemocratiseerd en daarmee voor meer partijen toegankelijk, en we in veel gevallen niet weten wie die partijen zijn, kan onze informatie in handen komen van partijen waar we het liever niet zouden zien. En dat wakkert het informationele privacydebat aan.

De kern van Nissenbaum’s argument over de waarde van informationele privacy wordt gevormd door dit verschil in betekenis van informatie in verschillende contexten. Ze noemt bekende voorbeelden Google Street View foto’s die duidelijk maken dat informatie in de ene context geen inbreuk op de privacy hoeft te veroorzaken en dat wel kan in de andere context. Zoals de foto op Street View van zonnende studentes op de campus van Stanford University en een plaatje van een man die een stripclub verlaat in New York. Het spreekt voor zich dat de zonnende studentes wisten dat omstanders hen in hun bikini konden zien, het is duidelijk dat ze zich in de openbare ruimte bevinden. Er werd echter verbolgen gereageerd toen deze beelden als foto’s op internet gepubliceerd werden: het bereik van de informatie werd veel

groter, het beeld kon meermaals worden opgeroepen, opgeslagen en verder verspreid. En hoewel Google's ultieme excuus voor Street View is dat alleen publieke plaatsen worden gefotografeerd en gepubliceerd, lijken doodnormale zaken een "morele transformatie" te ondergaan zodra ze tot digitale informatie verworden, aldus Nissenbaum (52, 57). In de de rest van dit hoofdstuk neem ik haar beschouwing van het privacydebat als leidraad voor mijn eigen analyse van de verschillende posities in het privacydebat.

## Het actueel debat rond informationele privacy

Nissenbaum plaatst de volgens haar belangrijkste bestaande opvattingen over informationele privacy in een schema. De verschillende theorieën zoeken de waarde van privacy allemaal in een andere hoek en Nissenbaum brengt verschillende dimensies te berde waarbinnen de volgens haar van belang zijnde theorieën ondergebracht kunnen worden (67).

De drie *dimensions of difference* die zij onderscheidt zijn:

- normatieve vs. descriptieve concepties van privacy
- definities die geformuleerd worden in termen van toegang tot en controle over gegevens
- benaderingen die in privacy een probaat middel zien om andere morele, politieke of maatschappelijke waarden te promoten vs. benaderingen die privacy waarderen om de privéruimte pur sang.

Nissenbaum is er duidelijk over dat deze benaderingen naast elkaar bestaan. Maar zoals ze zelf al toegeeft, is het door haar gegeven overzicht van de theorie niet volledig (74). Bij het doen van literatuuronderzoek heb ik gemerkt dat er theoretici,

kunstenaarsinitiatieven en praktijkvoorbeelden zijn die de waarde van privacy zoeken in andere dimensies die niet door Nissenbaum onderscheiden worden. Hoewel ik niet wil beweren dat mijn onderzoek wel een volledige analyse biedt, is het zinvol in dit hoofdstuk haar analyse aan te vullen door nieuwe posities onder te brengen bij bovenstaande dimensies en daarnaast ook de eigenschappen van deze dimensies aan te vullen op de plaatsen waar ze mijns inziens tekort schieten. Zo zet ik tegenover de tweede dimensie ook defenties die uitgaan van volledige openheid aan data en voeg ik de categorie technologisch determinisme vs. constructivisme toe. Hiermee creëer ik ook een plaats voor de progressieve post-privacy beweging, wiens positie mij zoals eerder aangegeven in het bijzonder interesseert. Daarnaast licht ik Nissenbaum's dimensies en mijn aanvullingen inhoudelijk toe. Op deze manier breng ik het debat omtrent *informational privacy* in kaart.

**Normatieve concepties van privacy**

Allereerst onderscheidt Nissenbaum de normatieve van de descriptieve manieren om rekenschap te geven van privacy. Een normatieve benadering houdt bij Nissenbaum in dat men privacy ziet als iets wat per definitie nastrevenswaardig is; een recht waar iedereen aanspraak op kan maken op morele gronden. Een descriptieve benadering van privacy noemt zij ook wel een neutrale zienswijze, waarbij privacy niet per se als iets goeds of slechts wordt gezien. Een descriptieve benadering spreekt bijvoorbeeld over een afname van privacy, waar men in een normatieve benadering spreekt van een schending van de privacy. Het voordeel van een neutrale conceptie van privacy is dat het de ruimte laat om na te denken over gradaties van privacy, waar in het ene geval meer privacy gewenst is dan in het andere (67-9, 72). In het debat

blijken vanuit de verschillende posities eigenlijk altijd normatieve kwaliteiten aan privacy te worden toegeschreven, wat vrij logisch is als men positie neemt in een discussie. Descriptieve posities zullen dan ook niet benaderd worden in onderstaande analyse. Wel is er ruimte voor een normatieve betekenis waarbij privacy niet als iets goeds wordt gezien, maar als iets wat verwerpelijk is. Dit biedt een aanvulling op Nissenbaum's uiteenzetting. Ik begin hier echter met normatieve posities die privacy nastrevenswaardig achten.

*Normatieve betekenis: nastrevenswaardig*

De meeste theoretici focussen op de normatieve significantie van het begrip en vragen zich alleen af of een neutrale conceptie nodig is (69). Nissenbaum concludeert in dezelfde lijn dat een evaluatie van de sociaal-technologische systemen die het privacyvraagstuk doen aanwakkeren al om een normatieve benadering vraagt; immers vragen we ons af hoe die systemen ertoe leiden dat we het gevoel hebben aangetast te zijn in onze privacy, waarmee men dus uitgaat van privacy als iets wat nastrevenswaardig is. Ook zijzelf schrijft afwisselend over een moreel gelegitimeerde claim op privacy en een recht op privacy (74). Niet als een recht op controle over of toegang tot informatie, maar als een moreel recht op een passende stroom van informatie:

> "... a right to privacy is neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information. (...) Privacy may still be posited as an important human right or value worth protecting through law and other means, but what this amounts to is a right to contextual integrity and what *this* amounts to varies from context to context." (127, nadruk in origineel)

Door privacy als een moreel recht te omschrijven, valt haar benadering ook onder de normatieve visies.

Ook uit de door mij bestudeerde literatuur blijkt dat de meeste posities in het debat gebaseerd zijn op een gevoelde bedreiging voor de informationele privacy en derhalve privacy als normatief classificeren. Evgeny Morozov bijvoorbeeld wijst in *The Net Delusion* (2011) op een te positieve voorstelling van zaken in de Westerse politiek en media van de voordelen van het internet en een gebrek aan de bescherming van gegevens. Een groot deel van zijn boek verhandelt over de volgens hem utopische idee dat activisten via het internet democratie zouden kunnen bevorderen in autoritaire regimes. Cyber-utopisten zouden teveel focussen op wat er naar Westerse begrippen aan goeds gedaan kan worden middels het internet, zoals het ontwikkelen van diensten als Twitter waarmee dissidenten kunnen oproepen tot demonstraties die uiteindelijk democratisering moeten bevorderen. De cyber-utopisten vergeten volgens Morozov de mogelijke negatieve gevolgen: door zich op internet te begeven laten activisten sporen van gegevens na die het voor overheden makkelijker maken ze op te sporen. Een gevaar voor hun privacy, vindt Morozov (26).
Aan zijn zijde staat Rebecca MacKinnon, die onder andere wijst op de gevaren van Facebook's *real name policy* (de voorwaarde dat je je account koppelt aan je echte naam) in combinatie met het zonder aankondiging wijzigen van het privacybeleid. Politieke activisten die Facebook inzetten om tot protest op te roepen kunnen van de een op de andere dag opeens een groot probleem hebben, aldus MacKinnon (2012).
Dezelfde redeneringen klinken in *The Net Delusion* door. Morozov koppelt autoritaire regimes direct aan "*Orwell-style*"-controle, die volgens hem wordt uitgevoerd door propaganda, surveillance en censuur. En juist vrijheid van informatie en het

“gedecentraliseerde karakter van het internet” maakt deze drie dingen mogelijk (82). Hiermee maakt hij van privacy iets wat beschermd moet worden en hij zou daartoe de vrije stroom van informatie aan banden willen leggen.
Morozov’s positie is in het debat van belang omdat hij één van de uiterste spectra van het debat representeert. Morozov pleit voor volledige controle over gegevens van internetgebruikers en acht privacy waardevol.

*Normatieve betekenis: verwerpelijk*
Wat we bij Nissenbaum niet zien is dat een normatieve benadering van privacy ook kan betekenen dat men privacy ziet als het tegenovergestelde van een nastrevenswaardige zaak die zelfs uitgeroeid zou moeten worden. Zij ziet in privacy uitsluitend iets goeds, maar neemt dan ook niet de post-privacy positie mee in haar analyse. Deze positie wordt weliswaar geformuleerd vanuit de vraag hoe sociaal-technologische systemen onze informationele privacy bedreigen, maar gaat die vermeende bedreiging voorbij en propageert juist het vrijgeven van zoveel mogelijk data. De Duister Christian Heller is een van de voorvechters van het opgeven van privésfeer en ziet vele voordelen in wat hij noemt de *Verdatung* van onze wereld.[1]

> “Die Welt der Daten gibt uns zudem neue Techniken des Selbst an die Hand: neue Gedächtnisse, neue Selbstbilder, neue Arten zu denken. Die Verdatung und Datenbewahrung unserer persönlichen Welt öffnet sie dem Zugang einer Zukunft, deren Möglichkeiten wir noch gar nicht vorausahnen können. Diese neuen Techniken des Selbst stellen sich oft quer oder ganz gegen das Konzept der «Privatsphäre»...Was

1 Met *Verdatung* wordt de opslag en verwerking van persoonsgegevens bedoeld.

> uns die Entfesselung der Daten an Sichtweisen, Werkzeuge und Möglichkeiten öffnet, das verdient Anerkennung. Diese Entfesselung liegt begründet in der Freiheit von Daten: ihrer ungehinderten Verfügbarkeit, dem ungehinderten Experimentieren mit ihnen." (*Post-Privacy* 2011, 72)[2]

De post-privacy positie wordt dus gekenmerkt door een focus op de kansen en oplossingen die ontstaan als we moeten inleveren aan privésfeer. Zo kan het combineren van data uit een elektronisch patiëntendossier waar ieders medische gegevens verplicht in opgenomen worden leiden tot nieuwe inzichten over ziektebeelden die betrouwbaarder zijn dan wanneer het om statistisch onderzoek uit een veel kleinere focusgroep gaat (55). Ook Jeff Jarvis' relaas *Public Parts* (2011), waarin hij zegt graag een stukje privacy in te willen leveren voor bijvoorbeeld meer veiligheid, past in de nieuwe traditie van post-privacy voorvechters. Journalist en blogger Jarvis staat bekend om hoe hij met zijn prostaatkanker in de openbaarheid trad en vrijuit blogde over de behandeling hiervan om bewustwording rond de ziekte te creëren. Cyber-utopisten, zou Evgeny Morozov deze heren noemen. Wat niet ongepast zou zijn daar Heller in het post-privacytijdperk niet uitkijkt naar maar ook niet bang is voor dystopische taferelen zoals gepresenteerd in George Orwell's roman *1984* (Heller

[2] Heller zet zijn theorie in het bijzonder af tegen het recht op 'informationele zelfbeschikking', wat in Duitsland in 1983 grondwettelijk werd vastgelegd in het zogenaamde *Volkszählungsurteil* werd besloten en wat gepaard gaat met wettelijke regelingen omtrent bescherming van persoonsgegevens (*Datenschutz*). Het is relevant deze begrippen nader toe te lichten en ik zal hierop terugkomen in de subparagraaf 'Toegang en controle vs. Open Data'.

161).[3] En dit terwijl Morozov de *dataspace* al wel vergelijkt met dit schrikbeeld (Morozov 75-9, 82-4). Als we terug gaan naar het indelen van deze positie bij de normatieve of descriptieve dimensies, dan is dit duidelijk geen neutrale visie maar een normatieve benadering. Echter zien zij privacy niet als moreel recht, maar eerder als plicht het op te geven. In de volgende paragrafen zet ik deze positie in meer detail uiteen aan de hand van de theorieën van Heller, Jarvis en ook Facebook's oprichter Mark Zuckerberg.

### Technologisch determinisme vs. technologisch constructivisme

Hoewel het privacydebat zich dus kenmerkt door een gebrek aan neutrale benaderingen van privacy, worden de technologische systemen die ten grondslag liggen aan het debat soms in meer en soms in mindere mate neutraal gepercipieerd. In dat laatste geval worden ze ofwel geacht een drijvende kracht te zijn achter het vormgeven van sociale processen (technologisch determinisme) ofwel uitsluitend vorm krijgen dankzij de maatschappelijke context waarin ze zijn ingebed (technologisch constructivisme). Net als bij de indeling tussen normatieve en descriptieve posities wordt al snel duidelijk dat een puur deterministische positie niet te vinden valt. Marianne van den Boomen (2003) zegt over

---

[3] George Orwell schreef in 1948 en publiceerde in 1949 de roman *1984*. Het boek is te lezen als een protest tegen totalitaire regimes. In deze dystopische samenleving mag men alleen lezen wat de partij voorschrijft, wordt enige vorm van verzet onmiddellijk de kop ingedrukt en worden oude waarheden vervangen door nieuwe die voor het functioneren van de staat beter uitkomen. Burgers worden gecontroleerd en onder de duim gehouden door surveillance. De uitspraak 'Big Brother is watching you' komt uit dit boek en verwijst naar de almachtige leider van de staat die burgers tot in hun woonkamers aan toe in de gaten houdt. Het schrikbeeld beeld wat geschetst wordt in de roman wordt in het privacydebat regelmatig aangehaald als verantwoording voor het beschermen van gegevens van burgers voor de overheid (*1984*, 2008).

technologisch determinisme dan ook dat het in onversneden vorm eigenlijk niet voorkomt, omdat je dan niets anders kan doen dan toezien hoe de technologie 'haar gang gaat' zonder daarover een positie in te nemen. Wel kunnen veel constructivistische posities volgens haar enkele technologisch-deterministische trekjes hebben, zoals we in onderstaande analyse ook zullen zien. De reden dat ik in mijn poging om het debat in kaart te brengen toch deze dimensie heb aangehouden, is dat de constructivistische elementen in de posities interessant zijn om benoemen.

Nissenbaum maakt zoals eerder gezegd duidelijk dat zij de technologische systemen absoluut ziet in de maatschappelijke context door te spreken van *socio-technical devices*, die hun betekenis krijgen door hun maatschappelijke inbedding. Zij meent technologieën zoals RFID chips die weerstand oproepen in de naam van privacy te moeten bezien als socio-technologisch:

> "(...) they afffect us not purely by dint of physical or material properties but by properties they acquire as systems and devices embedded in larger material and social networks and webs of meaning" (6).

Morozov pleit ervoor het internet te duiden vanuit de invloed die het geopolitieke klimaat in de huidige historische context op het medium heeft. Hij is er duidelijk in dat we de idee van technologisch determinisme, door hem in *The Net Delusion* gedefinieerd als "het geloof dat bepaalde technologieën onvermijdelijk bepaalde sociale, culturele en politieke effecten zullen veroorzaken" (289), moeten weerstaan. Technologisch determinisme leidt de aandacht af van de verantwoordelijkheid die de mens heeft in de interactie met technologie. Morozov is

van mening dat de mens een van de zwakke schakels is met de technologie. Om dit inzichtelijk te maken stap ik even af van de literatuur van Morozov om een voorbeeld te bespreken uit de *Thema*-uitzending 'Wat nou privacy?' van de VPRO (2010). Hierin zien we een man die uitlegt hoe hij te werk ging in het vakgebied van *pretexting*: het onder valse voorwendselen lospeuteren van gevoelige informatie over mensen bij instanties als de belastingdienst, het UWV en de politie. Zo zien en horen we hoe hij telefonisch salaris-, bank- en verzekeringsgegevens van de interviewer weet te ontfutselen bij onder andere diens werkgever en bank door zich achtereenvolgens voor te doen als medewerker van ING, als de interviewer zelf of zelfs zonder zich als wie dan ook te identificeren. De rekeningnummers die hij bij de bank opvraagt, kan hij later weer gebruiken om zich als de interviewer in kwestie te 'identificeren' om openstaande nota's op te vragen.
Dit voorbeeld geeft de rol van de mens in relatie tot techniek aan. Zelfs wanneer databanken zwaar beveiligd zijn en het onmogelijk zou worden om bijvoorbeeld telefoongesprekken af te luisteren, kan je er altijd nog zelf een voeren met een goedgelovige telefoniste.

Morozov plaatst zichzelf duidelijk tegenover de internet-centristen, die een sterk technologisch-deterministische filosofie aanhangen, en zegt dat de technische mogelijkheden van een medium ook direct betrekking zouden moeten hebben op wat er op dat moment in de maatschappij met die mogelijkheden gedaan wordt en kan worden. Journalist en auteursrechtenactivist Cory Doctorow (2011) noemt in zijn kritiek op *The Net Delusion* dat Morozov continu op de gevaren voor privacy wijst en maar weinig met heldere antwoorden of oplossingen voor het vraagstuk komt. Hierdoor

lijkt het alsnog alsof de techniek onvermijdelijk (negatieve) gevolgen produceert. Hoewel hij zichzelf cyber-realist noemt, is zijn toon er eerder een van cyber-negativisme. Vanuit zijn ervaring als activist meent Doctorow dat de privacy beter gewaarborgd is dan Morozov doet overkomen dankzij "programma's gericht op het terugbrengen van risico's als gevolg van het gebruik van internet" door activisten. We kunnen Morozov geen determinist noemen, maar wel een constructivist met een zeer negatief beeld van wat de internet-gebruikende activist kan doen om zijn gegevens te beschermen.

Een voorbeeld van zo'n dataprotectieprogramma wat Doctorow aanhaalt is *The Onion Router* project (TOR). Via de TOR software kan een internetgebruiker anoniem surfen: hij stuurt zijn gegevens dan gecodeerd over het net door gebruik te maken van verschillende servers. Zo valt de identiteit van de TOR gebruiker niet te herleiden. Dergelijke *zero-knowledge networking systems* zorgen ervoor dat de techniek in dienst blijft staan van de mens en dat gebruikers geen last ondervinden van ongewenste bijeffecten van het gebruik ervan.

Christian Heller is als voorvechter van de post-privacy positie duidelijk meer geïnteresseerd in de effecten die communicatie- en informatietechnologie 'toch wel' produceert. Heller opent zijn boek met de vraag:

> "Warum bin ich mir so sicher, dass das Ende der Privatsphäre gekommen ist?...Schuld ist das Internet...Sein Speicher ist unendlich groß, entsprechend auch sein Hunger nach Erfahrung, Input, Daten. Tabus wie Datenschutz oder Staatsgeheimnisse kennt seine Neugier nicht." (2011, 8)

Met deze woordkeus personificeert hij het internet bijna, zeker als hij vervolgens zegt dat je op internet begeven ook betekent dat je een communicatieproces met het net aangaat waarbij je iets vraagt en op antwoord moet wachten (9). Uiteindelijk wordt uit de rest van zijn betoog toch duidelijk dat de technologie door de mens voor verschillende doeleinden kan worden ingezet, al naar gelang wat we ermee willen. Hij heeft dus wel degelijk oog voor de techniek in relatie tot de sociale context, zoals we in de volgende subparagraaf zullen zien.

**Beperking van toegang en vorm van controle vs. open data**

In de dimensie die Nissenbaum gebruikt om haar analyse van het debat te maken zet ze het beperken van de toegang tot gegevens tegenover het bewaren van de controle over gegevens. Hiermee duidt Nissenbaum één enkele dimensie aan. Hoewel de ene theoreticus meer uitgaat van een pro-actief controle uitoefenen terwijl de ander focust op het beperken van de toegang die anderen hebben tot informatie die toch al *'out there'* is, sluiten de twee posities elkaar niet uit. De post-privacy positie valt buiten deze indeling omdat zij voor het zoveel mogelijk open stellen van persoonsgegevens is, zoals we in Heller's theorie zien.

Zoals eerder gezegd valt onder *Verdatung* te verstaan de opslag en verwerking van persoonsgegevens door de staat, iets waar *Datenschutz* de burger tegen in bescherming moet nemen en zo de privésfeer en het recht op informationele zelfbeschikking moet beschermen. Dit recht werd in Duitsland als grondrecht erkend in het *Volkszählungsurteil* in 1983. Het doel van *Datenschutz* is de burger zelf de controle te geven over diens eigen gegevensstroom (Heller, 74-94).

Heller koppelt een vrije datastroom aan voordelen die door Datenschutz alleen maar belemmerd zouden worden. Met een databank van medische gegevens kunnen we statistiek toepassen op daadwerkelijke gegevens in plaats van met minder nauwkeurige steekproeven te werken (64). Hij geeft voorbeelden van bedrijven die met behulp van onze tweets, e-mails, foto's en andere egodocumenten ons na overlijden weer tot leven zouden kunnen wekken, omdat ze op basis van die gegevens kunnen voorspellen wat we bij leven zouden hebben gedaan (69, 71). Het is lastig Heller hier serieus te nemen, zeker als we de bedrijfsfilosofie van een van die bedrijven, CyBeRev, er op na slaan:

> "AI's in the future will be able to recreate people from the information left behind about them if suitable backups of their brain were not made (in which case it would be straightforward). Neural nanobots would obtain all the available information about them from other people's brains. The AI would also consider all of the person's writings, pictures, movies, etc. also their genetic code. And it could then create a person who would pass a Turing test for that person with their best friends as the judges...The recreated person by the AI is probably at least as close as we are to ourselves after some time passage." (Cyberev.org, 2012)

Het lijkt of Heller een beetje is doorgeslagen in zijn 'open data'-filosofie, dat hij dit soort initiatieven ter verantwoording van de post-privacy positie gebruikt. Heel serieus lijkt hij het niet te nemen, maar met deze voorbeelden wil hij wel zeggen dat dergelijke utopische gedachten vaker invloed op de cultuur hebben gehad en daarom een vrijplaats verdienen. Het vrijelijk experimenteren met gegevens moet dit mogelijk maken (72). Voor hem betekent informationele zelfbeschikking niet het recht om zelf te bepalen waar jouw persoonlijke gegevens

naartoe stromen, maar dat iedereen uit elkaars datastroom zou mogen voor zijn eigen gewin zou mogen pakken wat hij wil (73). Informatie wordt bij Heller een gemeengoed en zijn positie wordt er bijna een van dataverheerlijking.

Sociale netwerksite Facebook is een bekend voorbeeld van voorstanders van open data en is gebaseerd op het werken met echte identiteiten. Een bepaalde vorm van privacy was in de begindagen van het netwerk ingebouwd omdat de service in het begin alleen beschikbaar was voor studenten van Harvard (Kirkpatrick 2010, 100). Maar Facebook houdt vast aan de *real name policy.* Mark Zuckerberg baseert zich op radicale transparantie. Hij is van mening dat de tijden voorbij zijn waarin je verschillende identiteiten presenteerde afhankelijk van of je bijvoorbeeld op het werk was of onder vrienden. In onze transparante samenleving is het onmogelijk om verschillende gedaantes te hebben. Bovendien, zegt Zuckerberg, wijst het maar op een gebrek aan integriteit (199). Er gaat bijna geen aanpassing in Facebook's privacybeleid voorbij, of er is ophef over. Toen in 2006 News Feed werd geïntroduceerd, een functionaliteit die het mogelijk maakt de Facebookactiviteiten van al je contacten onder elkaar opgesomd te zien, was een veelgehoorde kritiek dat dit wel erg "stalker-esque" aandeed (190). Daarvoor moest je nog alle individuele gebruikersprofielen bezoeken om te zien wat iemand had gepost. Zuckerberg kan zijn filosofie van radicale transparantie echter baseren op het siteverkeer wat ontstond na de introductie van 'News Feed': bezoekers spendeerden meer tijd op de site en bezochten meer pagina's dan ooit tevoren (192). Anno 2012 is er zelfs een functionaliteit toegevoegd die de activiteiten van contacten zelf *real-time* in beeld brengt: de ticker.

Radicale openheid wordt op meer online plekken uitgebuit, bijvoorbeeld in de traditie van open source software. Zoals het kunstenaarscollectief *Free Art and Technology Lab (F.A.T.)* doet met onderzoek en ontwikkeling van technologie en media. Ze doen dit in het openbaar door alle ontwikkelde software beschikbaar te stellen voor iedereen. Zo willen zij het publieke domein verrijken, innovatie bevorderen en zich uitspreken tegen het traditionele auteursrecht (F.A.T. 2012). De 'open data'-filosofie lijkt dus niet op zichzelf te staan of zich uitsluitend te koppelen aan het privacybegrip, maar kan als een onderdeel van een grotere paradigmawisseling gezien worden waarbij transparantie het sleutelwoord is. Het meer behoudende kamp bestempelt deze visie vaak als naïef. Niet voor niets wordt Mark Zuckerberg's idee van radicale transparantie en het onderhouden van slechts één identiteit bestempeld als een klassieke *"classical college student view"* (Kirkpatrick 202).

Privacy kan volgens Jeff Jarvis ook als ruilmiddel functioneren voor andere waarden, zoals veiligheid. Hijzelf is op het vliegveld meer dan bereid zijn bagage te laten doorzoeken als hij daarmee weet dat dit ook bij de rest van de passagiers gebeurt en zo terroristen kunnen worden onderschept. En het is fijn dat gemeentes via Google Earth een blik in achtertuinen kunnen werpen om illegaal aangelegde zwembaden op te sporen, vindt Jarvis (61-2). Daarnaast ziet hij informatie ook als een valuta waarmee we relevantie kunnen 'kopen', op Facebook bijvoorbeeld. Als je er data instopt krijg je er interactie voor terug. Op dezelfde manier kan het delen van medische gegevens ingezet worden om bijvoorbeeld betere ziektebeelden te schetsen. Hier noemt hij hoe het aantal zoekopdrachten op Google naar woorden als 'loopneus' en 'verkouden' al van tevoren een griepepidemie kunnen

aankondigen. Ook Christian Heller ziet, zoals eerder vermeld, een voordeel in deze *trade-offs* en wijst op de mogelijkheid om met dit 'positieve dataverkeer' bijvoorbeeld statistieken uit patiëntgegevens te halen. Hoe opener de databank en hoe minder restricties op het doel waarvoor gegevens gebruikt mogen worden, hoe meer potentiële betekenis de gegevens hebben: *"Daten von jedem, Daten für jeden* (54-7)." Dat we bang zijn dat er op die databanken in te breken valt, onze medische gegevens op straat komen te liggen en we zo een sociaal stigma kunnen krijgen noemt Jarvis een probleem van de maatschappij. Een oplossing biedt hij niet, maar wel lijkt het erop dat hij en Heller de *scope of transmission*, zoals Nissenbaum dat zou noemen (204), uit het oog verliezen. Op het moment dat we informatie beschikbaar stellen weten we niet wie het waarvoor ooit zal gebruiken. Dit verschilt fundamenteel van Nissenbaum's opvatting over de behoefte aan een gepaste stroom van informatie.

Helen Nissenbaum past meer in de traditie van *Datenschutz.* Haar theorie in *Privacy in context* komt tot uitdrukking in het zogenaamde *framework of contextual integrity*. Hiermee geeft zij ruimte aan verschillende invullingen van privacy in verschillende sociale contexten waarin steeds andere normen gelden voor wat wel en niet tot privé-informatie behoort (148). Daarom is volgens haar een gepaste stroom van informatie belangrijk, zodat iedereen weet welke informatie in welke context voor wie beschikbaar is.

De manier waarop Google met gebruikersgegevens omgaat kan dit illustreren. Google biedt naast een zoekmachine ook andere diensten aan zoals een videocommunity (YouTube) en een e-mail service (Gmail) die de database alleen maar rijker maakt. Sinds maart 2012 is het privacybeleid gewijzigd en

geeft Google aan gebruikersinformatie (accountinformatie) uit de verschillende platformen te combineren om zo naar eigen zeggen een “simpelere, meer intuïtieve Google ervaring’ te kunnen bieden (Google 2012). In de praktijk houdt dit in dat Google gebruikersprofielen kan samenstellen die voor adverteerders zeer interessant zijn. Echter, als gebruiker van Google diensten weet je niet wat die informatie over jou precies inhoudt, naar welke bedrijven die informatie stroomt en of die verzamelde gegevens bij Google wel goed beveiligd worden.

Vanuit deze gedachte vroeg de Duitse politicus Malte Spitz bij zijn telecomprovider T-Mobile zijn telefoniegegevens op over de periode augustus 2009 tot februari 2010. Hij kreeg ze niet zomaar mee, maar moest het bedrijf eerst voor het gerecht slepen om dat wat hij als zijn persoonlijke gegevens zag in handen te kunnen krijgen. Hij wilde weten welke informatie van hem het bedrijf had opgeslagen en of dat gedaan was volgens de wettelijke richtlijnen. Hij verzamelde in totaal 35.000 gegevens, waarbij de telefoonnummers die hem hadden gebeld of ge-sms’t en die hij had gekozen niet eens vermeld waren, ook al worden die wel opgeslagen. Om aan te geven wat deze data over iemand kunnen prijsgeven als ze gecombineerd worden met andere openbare gegevens bood hij zijn gegevens aan het Duitse weekblad *Die Zeit* aan (Spitz 2011). *Die Zeit* publiceerde de gegevens in combinatie met zijn eigen tweets, website of de website van zijn politieke partij en journalistieke media (Die Zeit 2011). De telefoongegevens maakte zijn GPS locatie inzichtelijk zolang hij in Duitsland was. Zo kunnen we op een interactieve kaart zien wanneer hij de trein of het vliegtuig pakte, wanneer hij werkte en wanneer hij sliep en in welke *Biergarten* hij zijn vrije tijd het liefst

doorbracht. *“All in all, it reveals an entire life,”* schreef *Die Zeit* (Biermann 2011).

Dit is waarom Helen Nissenbaum pleit voor de gepaste stroom van informatie, waarbij zowel het beperken van de toegang tot bestaande gegevens als het controleren van de toegang ertoe een rol speelt. Het kan zijn dat een gebruiker het niet erg vindt om gepersonaliseerde advertenties te ontvangen op basis van verzamelde zoek- en browsergeschiedenis, maar hij kan wel bang zijn voor een inbraak op de server van Google waarbij zijn informatie toegankelijk wordt voor partijen waarvoor die informatie nooit bedoeld is geweest. Ook hebben we volgens haar te vrezen van de samenstelling van uitgebreide gebruikersprofielen als gevolg van het combineren van gegevens van verschillende platformen (Nissenbaum 42-4), zoals ook het geval van Malte Spitze illustreert.

Verschillende initiatieven van webbouwers en privacyactivisten wijzen op de onvoorziene manieren waarop beschermd geachte persoonlijke informatie via sociale netwerksites beschikbaar is. Youropenbook.org, later openbook.org, was een zoekmachine waarmee men willekeurige zoekopdrachten kon uitvoeren in statusupdates in Facebook die onder het predicaat ‘openbaar’ geplaatst waren. Het enige wat de website hiervoor nodig had was de openbare API software van Facebook, waarmee deze informatie uit de website gefilterd kon worden en op een ander platform beschikbaar gemaakt werd. Hiermee wilden de makers aantonen dat we vaak denken te weten aan wie we onze informatie blootstellen, maar dat het niet altijd zo werkt als gevolg van ondoorzichtig privacybeleid op sociale netwerksites (Youropenbook.org 2012).

Ook Evgeny Morozov wijst op het gevaar van gebrekkig privacybeleid van sociale mediabedrijven zoals Facebook (82, 143-178). Op het eerste gezicht heeft zulk beleid voor gebruikers in democratieën niet zo veel effect, maar dezelfde technologie kan voor gebruikers in een totalitaire staat verstrekkende gevolgen hebben, omdat autoriteiten ook op sociale netwerksites kunnen surveilleren, censureren en propaganda maken:

> "A laissez-faire regulatory approach that glosses over high-profile mistakes in the name of innovation may eventually give us a shiny portable guide to the best frappuccinos in the neighborhood, but it may also inadvertently compromise the security of Iranian bloggers, who won't be treated to many frappuccinos in Theran's Evin Prison." (224)

De Nederlandse burgerrechtenbeweging Bits of Freedom (BoF) zoekt een middenweg tussen openheid en afscherming in het voordeel van de burger ten opzichte van de staat. Zij pleiten voor een open internet waar iedereen gebruik van kan maken en informatie kan delen zoals de gebruiker dat wil en "waar privécommunicatie privé blijft" (Bits of Freedom 2012). In 2012 behaalden zij een succes met de kwestie van netneutraliteit, waarbij zij lobbyden voor een wetsvoorstel wat de netneutraliteit middels wetgeving zou bewaken. Internet service providers mogen dataverkeer niet afknijpen bij het gebruik van diensten die veel bandbreedte gebruiken, zoals het downloaden van films maar ook het gebruik van telefoondiensten zoals Skype. Dit is gegrond in BoF's standpunt dat data vrij moeten stromen ten behoeve van de gebruiker, maar ook dat diens privacy bewaakt moet worden. Immers, als internet service providers specifiek dataverkeer van hun gebruikers afknijpen betekent dat dat ze niet alleen het dataverkeer maar ook de inhoud daarvan in de gaten

houden (Deep Packet Inspection). En dat ziet BoF als een schending van privacy (Bits of Freedom 2010).

**Privéruimte pur sang vs. door privacy vertegenwoordigde waarden**

In de vorige subparagrafen is gebleken dat alle hier besproken posities in het informationele privacydebat normatief van karakter zijn en de informatie- en communicatietechnologieën die hierin een rol spelen in meer of mindere mate als een product zien van de sociaal-maatschappelijke context. In deze laatste subparagraaf van dit hoofdstuk zal ik achterhalen op welke grond de verschillende posities waarde aan privacy toekennen. Nissenbaum onderscheid daarin benaderingen waarin het belang van privacy wordt gezocht in de waarde van de privésfeer zelf ("*a private zone for humans*") van posities die het recht op privacy in zekere morele en politieke waarden zoeken en waar tevens met het beschermen van privacy deze andere waarden verdedigd moeten worden (73).

Kluitenberg schreef in *Open*'s themanummer over hybride ruimte nog over het belang van 'selectieve disconnectiviteit'. Vanuit een idealistische gedachte dat we moeten "voorkomen dat de bedwelming door de techniek omslaat in een vergiftiging" meent Kluitenberg dat we de mogelijkheid moeten hebben om soms toe te geven aan de behoefte om even niet *connected* te zijn. Als we dit niet doen, vraagt hij zich af of de connectiviteit in de hybride ruimte onze autonomie dan vergroot of juist verkleint. We verwachten wel overal aangesloten te kunnen zijn, maar of we dat echt willen is nog maar de vraag (29-31). Als we bijvoorbeeld op vakantie zijn, lezen we liever geen e-mails van het werk. Maar verwacht onze baas niet dat we dat toch even doen?

Ook veel privacybewakers houden autonomie hoog in het vaandel. Helen Nissenbaum kent aan privacy de rol toe om onze autonomie te bewaken. In een privéruimte, afgesloten van de openbaarheid, kunnen we doen, zeggen en denken wat we willen zonder dat wie dan ook daarvan notie zal nemen. Hierdoor kunnen we ons vrijelijk ontplooien in zowel ons gedrag als in onze denkwijzen. Waar Nissenbaum voor vreest bij een inbreuk op privacy is dan ook dat als we bekeken worden, en hierbij maakt zij de vergelijking met een situatie zoals in een panopticum, we vaker sociaal wenselijk gedrag zouden vertonen om stigma's te voorkomen. Deze vergelijking komen we vaker tegen in het debat. Jeremy Bentham ontwierp het panopticum als een gevangenis, waarin de gedetineerden zich in een constructie bevonden waarin ze continu gezien konden worden door een bewaker in één enkele bewakingstoren. Hoewel zij vanuit de toren te allen tijde zichtbaar waren, konden de gevangenen niet de bewaker in de toren zien, waardoor ze nooit wisten of ze nu wel of niet bewaakt werden. Hierdoor zouden de gevangenen, al dan niet in het oog gehouden door een bewaker, zich altijd gedragen alsof ze onder surveillance stonden (Schirato et al. 2012, 87-8).

Nissenbaum vreest dat deze situatie als deze wordt doorgetrokken in instituties in de huidige maatschappij, zoals Michel Foucault aanduidt, ervoor zorgt dat ook als we ons alleen al bekeken voelen we ons behouden zullen gedragen.[4] Dit leidt er uiteindelijk toe dat onze persoonlijkheid niet volledig tot wasdom zal komen en we zouden schikken met een "*middle-of-the-road conventionality*" (76). Jeffrey Reiman, een Amerikaanse professor in filosofie gespecialiseerd in strafrecht, koppelt ditzelfde mechanisme aan een bedreiging

[4] In het volgende hoofdstuk wordt dieper ingegaan op de filosofie van Foucault en het panopticisme.

voor onze vrijheid, in plaats van aan autonomie. We zullen impopulaire meningen voor ons houden en ons presenteren als afgevlakte persoonlijkheden, maar dat uiteindelijk wellicht als het effect van zelfcensuur ook daadwerkelijk worden (75).

Dit is in feite ook waar Evgeny Morozov in *The Net Delusion* op wijst als hij zegt hoe de staat activisten angst inboezemt door ze te vertellen dat hun online activiteiten zwaar onder toezicht staan en dreigen met zware straffen op dissidentie. Morozov vreest dat de activist zichzelf aan censuur zal onderwerpen of zijn online activiteiten in het geheel zal staken (145).

Jeff Jarvis schrijft in de traditie van de post-privacy voorvechters juist aan het wegvallen van een privésfeer een bepaalde waarde toe. Dat wat hij de 'mythe van perfectie' noemt kan zo bestreden worden. Dit houdt in dat als we allemaal open zouden zijn over die dingen die we nu uit schaamte angstvallig geheim houden, bijvoorbeeld een van de maatschappelijke norm afwijkende seksuele geaardheid, we iedereen de ruimte bieden zichzelf te zijn in plaats van dat we allemaal zouden willen voldoen aan een geaccepteerde norm (53-56). Dat is een mooie gedachte achter het idee om autonomie te bewaken, maar in de praktijk volstrekt onwerkbaar als je het Helen Nissenbaum vraagt. Als we privacy als een dekmantel voor morele timiditeit zien, dan denken we dus de maatschappij te kunnen opleiden door alles in het openbaar te doen. We moeten maatschappelijke gebruiken niet aanpassen op een soort ideaal volk, maar op hoe de mensen in die maatschappij daadwerkelijk zijn, zegt Nissenbaum (77). Daarom pleit zij juist voor een privéruimte om zichzelf aan het publiek onttrekken en te ontplooien. Jarvis ondermijnt onbedoeld zijn eigen argument wanneer hij over de

*ethics of publicness* schrijft (110-2). Een van de regels zou zijn dat we altijd de context moeten aangeven wanneer we informatie van iemand anders delen. Zelf heeft hij naar eigen zeggen altijd openlijk geblogd over zijn ziekte, prostaatkanker. Een van de details die hierbij de revue passeerde was het feit dat hij tijdens de behandeling luiers droeg vanwege incontinentie. Hij gaat ervan uit dat iemand die verantwoord omspringt met die publieke informatie nooit uit de context zal halen dat hij die luier moest dragen omdat hij aan prostaatkanker leed en dat diegene niet de indruk zal wekken dat Jarvis *"odd urges"* zou hebben. Hier zegt hij dus zelf dat hij het eigenlijk maar vreemd vindt als iemand een luier zou willen dragen zonder dat het ergens voor nodig zou zijn. Dit geeft eens en te meer aan, dat we allemaal oordelen. Ook al zouden we niemand stoppen om te doen waar hij zin in heeft, vormen we wel een mening van iemand en om die reden stelt Nissenbaum de mogelijkheid op prijs om bepaalde zaken voor onszelf te houden ten behoeve van onze autonomie.

Bit of Freedom bewijst dat privacy van de internetgebruiker naast vrijheid en autonomie ook andere waarden kan bevorderen. De organisatie wijst op het belang van keuzevrijheid en innovatie in het licht van netneutraliteit. Wanneer providers snuffelen in het dataverkeer van hun gebruikers kunnen zij besluiten de bandbreedte naar bepaalde diensten af te knijpen wat de ontwikkeling van die diensten belemmerd. BoF vraagt zich af wat er was gebeurt als de datastroom naar diensten als Skype was beperkt en of deze services zich dan ook ontwikkeld hadden tot wat ze vandaag de dag zijn. Hetzelfde geldt voor keuzevrijheid: als een provider het dataverkeer naar een concurrerende dienst afknijpt, dan beperkt dat de keuzevrijheid van de consument in diens internetgebruik (Bits of Freedom, 2012).

**Het debat in kaart**

Alle posities worden gedefinieerd vanuit de gedachte dat onze privacy bedreigd wordt. De meeste zijn geënt op het beschermen van privacy vanwege de waarden die in de privéruimte tot ontplooiing kunnen komen. De post-privacy positie signaleert ook de bedreiging van privacy, echter om privacy vervolgens helemaal de rug toe te keren.

Christian Heller zegt over die gevoelde bedreiging dat mensen er wel over klagen, maar in praktijk zich er toch weinig van aan lijken te trekken. Het privacybeleid van Facebook en Google wordt alom bekritiseerd, maar niemand lijkt erdoor te stoppen met het gebruik van de diensten (15). Nissenbaum's *framework of contextual integrity* verklaart waarom er geen paradox bestaat tussen aan de ene kant zorgen over privacy en aan de andere kant het vrijelijk delen van bijvoorbeeld persoonlijke foto's op een sociale netwerksite: zo lang er een gepaste stroom is van die persoonlijke informatie voelen we dat niet als een schending van onze privacy (2010, 187).

Maar zolang de informatiestroom niet gepast is en privacybeleid van mediabedrijven niet transparant, blijft men alert op een mogelijke schending van de informationele privacy. Als we kort door de bocht gaan zouden we kunnen denken dat dit mechanisme is te herleiden op angst voor het nieuwe medium internet. Mediahistorica Lisa Gitelman, die ik in de inleiding al even heel kort aanhaalde, zegt daarover dat media hun autoriteit pas verkrijgen als ze sociaal gedefinieerd zijn en geaccepteerd. Nieuwe media ondergaan een inburgeringsproces en pas als dit voltooid is worden ze voor vol aangezien. Het succes van media hangt daarmee af van een zekere "blindheid" voor de achterliggende technologie (2006). In mijn artikel in NRC Next in 2010 greep ik dit

mechanisme aan om het privacydebat op dat moment te verklaren: alsof we Google zouden beschuldigen van het aantasten van onze privacy terwijl we eigenlijk gewoon nog niet gewend waren aan het medium en bang waren voor de nog onduidelijke gevolgen voor de toekomst.

Na de analyse van het informationele privacydebat in het vorige hoofdstuk kunnen we stellen dat het privacydebat wel degelijk is gebaseerd op een zekere angst, namelijk die om aangetast te worden in onze privacy. Hierbij wordt meermaals het schrikbeeld voorgehouden van Orwelliaanse praktijken, de staat als een soort panoptische voyeur en zelfs het dytopisch beeld van een 'Orwelliaans panopticum'. Allen verwijzen naar ofwel George Orwell's roman *1984* ofwel het panopticum zoals uitgelegd in de filosofie van Michel Foucault (en soms zelfs naar allebei tegelijk). Dat hieraan ook een zekere theoretisch ongegronde maar gezonde argwaan kleeft jegens de media en hoe deze functioneren zoals de mens gewoon is, is niet ondenkbaar. Maar privacy is een goed wat verder reikt dan het medium waarmee we te maken krijgen: privacy is én representeert waarden in de hedendaagse maatschappij en dat die worden bedreigd is wat het privacydebat drijft. Daarom is het van belang in het volgende hoofdstuk deze vergelijking nader te onderzoeken.

## De staat van privacy in relatie tot biopolitiek

*De bescherming van informationele privacy gebaseerd op de vrees voor een soort panoptische maatschappij, voor zover we daarvan zouden kunnen spreken, blijkt een klassieke koppeling in het debat. Daarom zet ik hier eerst kort uiteen wat Foucault, naar wiens uitleg van het panopticum wordt verwezen, bedoelde met het panopticisme om zo de vergelijking te verklaren. Ik plaats deze vervolgens in de context van zijn filosofie over governmentality en de biopolitiek.*

De Franse filosoof Michel Foucault gebruikte het principe van het panopticum, wat van oorsprong betrekking had op de architectuur van een penitentiaire inrichting, om de werking van machtsstructuren in de samenleving uit te leggen. In het vorige hoofdstuk werd de werking van het panopticum als gevangenis, zoals ontworpen door Jeremy Bentham in de achttiende eeuw, al uitgelegd. In deze inrichting worden alle gedetineerden bewaakt vanuit één wachttoren waaruit alle gevangenen kunnen worden gezien. Zelf weten ze niet wanneer ze bekeken worden, maar zullen zich wel altijd gedragen alsof ze onder toezicht staan omdat de sancties op ongewenst gedrag te groot zijn om te riskeren daarop betrapt te worden.
Foucault gebruikt het panopticum als een metafoor voor machtsstructuren in andere gelederen van de samenleving. Hierbij verwijst hij naar wat in het Engels vertaald wordt als het *carceral continuum*, waarmee hij wil aanduiden dat de werking van deze gevangenisconstructie zich uitstrekt over meerdere entiteiten in de samenleving. Deze machtsstructuur heeft dus niet alleen betrekking op gevangenissen, maar strekt zich uit over allerlei instituties zoals scholen, werkplaatsen, maar ook

bijvoorbeeld het gezin. De bewaker, die dus ook in de vorm van leraar, gezinshoofd of manager kan optreden, bezit niet letterlijk de macht, want Foucault ziet macht altijd als iets wat relationeel is: overdraagbaar en afhankelijk van factoren in de samenleving (Schirato et.al., 8, 50). Uiteindelijk gaat het Foucault niet om de al dan niet aanwezige blik van de bewaker op het subject maar om hoe dit subject de macht internaliseert. Hij transponeert de werking van het panopticum naar machtsstructuren in de samenleving

> "as a procedure...to supervise the conduct of individuals while increasing the profitability and productivity of their activity" (Foucault 2008, 67)

die uiteindelijk vorm krijgen in de mate waarin het subject de kritische blik in zich opneemt, en zal gaan handelen, en uiteindelijk zelfs denken, alsof hij altijd onder toezicht staat. Dergelijke machtsmechanismen schaart Foucault, zodra ze niet meer alleen van buitenaf druk op ons uitoefenen, onder *technologies of the self* (Schirato et.al., 164).

De vergelijking van het leven in een hybride informatieruimte met de situatie zoals in een panopticum wordt vaak gemaakt, maar is niet altijd even helder. Ook wordt soms verwezen naar het panopticisme als machtsmechanisme zoals gebezigd door Foucault terwijl men alleen doelt op de architectuur van Bentham (Caluya 2010). Evgeny Morozov en Helen Nissenbaum gebruiken de vergelijking duidelijk wanneer zij respectievelijk zeggen dat surveillancepraktijken in autoritaire regimes "veel gemeen hebben met het ontwerp van de perfecte gevangenis" zoals omschreven door Bentham (145-6) en de "fundamentele notie van het panopticum" gebruiken om het principe van de kritische blik uit te leggen (82). Lev

Manovich' uitleg is minder helder wanneer hij het panopticisme van Foucault ongeldig acht in een samenleving waar communicatietechnologieën niet langer de *"straight lines of human sight"* nodig hebben om te kunnen functioneren (224). Doelt hij erop dat er via dergelijke communicatiemiddelen nog intensiever gesurveilleerd kan worden omdat fysieke aanwezigheid nooit meer nodig is? Maar hoe zit dat dan met de verinnerlijking van de kritische blik?

Het plaatsen van informationele privacy in het licht van het panopticisme is over het algemeen evident: de idee van het panopticum hangt samen met een machtsrelatie, surveillance en controle. Het panopticisme van Foucault laat zien dat deze machtsstructuren aanwezig zijn in allerlei instituten in de maatschappij en dat grijpt Nissenbaum aan om te wijzen op de internalisering van de macht als een bedreiging voor de autonomie, die met de bescherming van onze gegevens kan worden afgewend. In de filosofie van Foucault is de vorming van machtsstructuren afhankelijk van een visie op de mens als hulpbron, als een middel om te regeren aan de hand van de biologische kenmerken van de populatie. Het is derhalve interessant om Foucault's notie van biopolitiek nader te onderzoeken. Tevens zal het worden toegepast op een hedendaags instituut waarin de relatie tussen machthebber en populatie zichtbaar wordt.

## Biopolitiek

Foucault beschrijft een politieke strategie die zich vanaf de achttiende eeuw baseert op het fenomeen biomacht: basale biologische kenmerken van de mens zoals gezondheid, hygiëne, levensverwachtingen en ras, als onderwerp van regeringspraktijken, waarmee de mens als 'soort' wordt gezien. Deze strategie heet biopolitiek. (Schirato et al.. 2012: 90, Foucault 2007: 16, Foucault 2008: 317).

Biopolitiek is gebaseerd op de gedachte dat de staat om te regeren en de eigen ontwikkeling te kunnen faciliteren moet weten waaruit ze is opgebouwd: wat zijn haar middelen? De populatie, de mens dus, wordt als middel gezien, wat het managen van de populatie tot de basistaak van de staat maakt. Hiertoe moet de populatie ook wetenschappelijk geanalyseerd worden: statistieken over de populatie worden gebruikt om beleid te creëren waarmee het gedrag van de populatie gereguleerd moet worden (Schirato et al. 71-3). Deze vorm van macht bestempeld Foucault als *modern governmentality* en daaronder verstaat hij:

> "... the ensemble formed by institutions, procedures, analyses and reflections, calculations, and tactics that allow the exercise of this very specific, albeit very complex, power that has the population as its target, political economy as its major form of knowledge, and apparatuses of security as its essential technical instrument." (Foucault 2007, 144)

Foucault kent vooral aan disciplinerende *apparatuses* de rol toe om de populatie op effectieve wijze in de hand te houden.[5] Deze disciplinerende praktijken spelen zich niet alleen af in penitentiaire inrichtingen, zoals de gevangenis gemodelleerd naar een panopticum, maar verspreiden zich over andere maatschappelijke instituties, waarmee ook deze vorm van macht zich verspreid. De sancties die staan op overtredingen

---

[5] Foucault duidt een *dispositif*, in het Engels vertaald als *apparatus*, aan als zijnde: *"...the interrelation of forces, discourses, institutions, fields, technologies, actions and contents that work to produce and naturalise things-as-sense -the state, the world as historically explicable narrative- via the notion of the apparatus, or dispositif"* (Schirato et.al.,7). Het valt uit te leggen als een set begrippen, werkingen, acties, eigenschappen die samenhangen met betrekking tot een verschijnsel. Het *apparatus*, hoewel het zelf ook discoursen omvat, kan discoursen en daarmee ook gedragingen en meningen beïnvloeden.

bepalen wat gewenst gedrag is en daarmee als normaal gezien wordt, maar creëert ook een abnormale categorie (Foucault 2007, 84-5). Hier spreekt Foucault over de *microphysics of power:* een individueel subject wordt gevormd door een regime van surveillance en training en heeft de potentie daardoor een handelbare, volgzame burger te worden (80). In tegenstelling tot een *macrophysics of power*, waar de macht van een soevereine entiteit met vooral het inboezemen van angst door onder andere het vertonen van lijfstraffen kenbaar wordt gemaakt, komt de macht in het geval van biopolitiek tot stand in de hoofden van de subjecten. Foucault noemt zulke maatschappijen *"control societies"*, naar een term van Deleuze en deze functioneren langs lijnen van toezicht en directe communicatie. Foucault meent dat deze vorm van *modern governmentality*, die zich in het liberalisme begint te vormen tussen de zestiende en achttiende eeuw, in Westerse maatschappijen heden ten dage nog steeds gepraktiseerd wordt (Schirato et al. 72-3).

In biopolitiek speelt ook het concept van rassenverschillen een rol in het categoriseren van het normale en het abnormale. Zo ziet Foucault het nazisme  als een vorm van "veralgemeende biomacht" (Schirato et al. 95-6). Het is volgens Christian Heller daarom, dat het idee van de *Verdatung* in tegenstelling tot de informationele zelfbeschikking van de mens, zeker in Duitsland, sterk gekoppeld wordt aan het idee van menselijke waardigheid. Vanuit de gedachte dat het Derde Rijk zich ook liet gelden als een gegevensstaat boezemen machtsstructuren die functioneren op basis van statistieken, en de mens reduceren tot hulpbron, terecht angst in (Heller 76-8, 99-102). Heller, die zich in *Post-Privacy* fel kant tegen het beschermen van een privésfeer, komt op basis hiervan zelfs tot de verrassende conclusie: *"Datenschutzer haben recht"* (102).

Verzamelde statistieken werden in Nazi-Duitsland als verantwoording gebruikt om de ene bevolkingsgroep superieur te achten ten opzichte van de andere. Dat dit mechanisme wordt aangehaald om te pleiten voor het beschermen van persoonsgegevens zal niet snel verbazen. Maar Heller doet deze redenering gauw af met de opmerking dat de macht in het Derde Rijk in veel meer besloten lag dan alleen in de statistiek. Wat had er van geworden zonder geweren, fabrieken, en: "...de bereidheid en gehoorzaamheid van mensen" (104)?
Hoewel Heller eerder in zijn boek de werking van het panopticisme nauwkeurig omschrijft, mist hij in bovenstaande beredenering de filosofie van Foucault. Volgens de notie van *governmentality* zou die bereidheid en gehoorzaamheid van mensen juist voortkomen uit de disciplinerende machtsstructuur die door de kenmerken van de mensheid als population functioneert.

## Carceral continuum in dataspace: Facebook

*Apparatuses* van macht en disciplinering hebben het discours omtrent privacy beïnvloed, getuige de vele vergelijkingen met het panopticum die we in het debat tegenkomen. En de hybride ruimte als *dataspace* faciliteert de constante surveillance en controle van burgers via informatie die bedrijven over hen verzamelen, zij zelf achterlaten op het web en die de staat over hen bezit.

Zo bezien kunnen we de bedrijven die onze gegevens beheren -Google, Facebook, de telecomproviders uit het voorbeeld van Malte Spitz en alle andere instanties waarvan we ons niet eens bewust zijn- ook aanmerken als disciplinaire instituties. We kunnen Facebook als voorbeeld nemen van een instituut waarin deze machtsrelaties vorm krijgen.

Facebook met haar eigen beleid, gekleurd door de ‘radicale transparantie’-filosofie van haar oprichter, onderwerpt haar gebruikers aan een set instructies, regels en mogelijkheden waarbinnen de gebruiker zich kan bewegen. Zo kun je op Facebook nooit aangeven in een relatie te zijn met meer dan één persoon: polyamorie bestaat hier niet. Alle contacten moet je op Facebook ‘vrienden’ noemen en wanneer je bepaalde vrienden als familie wilt aanmerken is het niet mogelijk iemand als stiefvader of -moeder te aan te merken. Hier is het *apparatus* van Facebook aan het werk. Dat leidt er bijvoorbeeld ook toe dat men dingen alleen ‘leuk’ kan vinden en nooit ‘niet leuk’.
Op basis van de *real name policy* is een gebruiker verplicht zijn of haar echte naam op te geven, voor zover als Facebook dat in eerste instantie kan controleren. Dat levert problemen op wanneer je een naam hebt die lijkt op een zelfverzonnen bijnaam zoals Elmo, iets met ‘*gay*’ of ‘*beer*’. Als je dit als naam invoert bij het aanmaken van een profiel word je door Facebook automatisch geweerd en kun je soms pas na het opsturen van een kopie van een identiteitsbewijs een profiel aanmaken (Moses 2008). Het bedrijf bepaalt wat ‘normale’ namen zijn en wat abnormale.

Waar de *real name policy* begon als aan gebruikers opgelegd bedrijfsbeleid, kunnen we ons afvragen of gebruikers nog wel onder een pseudoniem zouden willen opereren op Facebook. De sociale netwerksite speelt een steeds groter wordende rol in de levens van veel gebruikers, omdat het in steeds meer hoeken van het internet opduikt en in een hybride ruimte als vanzelfsprekend ook in andere facetten van het leven. Door koppelingen met verschillende online diensten houdt Facebook bij welke muziek, films en boeken we leuk vinden, welke artikelen we lezen op de website van *the Guardian* en

welke liedjes we op welk moment luisteren op *Spotify*. Via een Facebookaccount kun je zonder een nieuw profiel aan te maken je bij verschillende online diensten aanmelden. En als je dan op Facebook niet onder je echte naam staat ingeschreven, kun je je ook voor die andere dienst niet meer onder je eigen naam aanmelden.
Als we mee willen doen moeten we toegeven aan de regels van Facebook. We internaliseren de regels, instellingen en wensen van Facebook en gebruiken onze echte namen, laten vrienden foto's van ons taggen en plaatsen geen inhoud die het bedrijf ongepast acht: plaatjes van blote borsten, maar ook foto's van zoenende mannen worden verboden (waar een afbeelding van een heteroseksueel koppel wel is toegestaan) (Nelson 2012). Foucault zou zeggen dat we onszelf onderwerpen aan de machtsstructuur om mee te kunnen draaien in het systeem. Zoals fabrieksarbeiders moesten leren met machines te werken onder erbarmelijke omstandigheden om verder te komen op de maatschappelijke ladder, zo moeten wij, om in de *social dataspace* van onze maatschappij mee te draaien, meedoen op Facebook (Schirato et al. 83).

Het moet gezegd worden dat Facebook wel luistert naar haar gebruikers wanneer zij een privacyprobleem constateren. Tegenwoordig is het op Facebook mogelijk vrienden in lijsten in te delen, waarvan je de privacyinstellingen per lijst kunt wijzigen en dus bijvoorbeeld voor collega's niet dezelfde inhoud openbaar maakt als voor familie. Maar ook dit in acht nemen van de publieke opinie is volgens Foucault onderdeel van de machtsrelatie. De publieke opinie wordt gezien als een eigenschap van de populatie. De steun van in dit geval de gebruikers kan niet voor lief genomen worden en derhalve wordt hun opinie meegenomen in het handhaven van het beleid. Het is onderdeel van een politieke strategie op basis

van een kosten-batenanalyse van aan de ene kant het onderdrukken van verzet en aan de andere kant het subject net genoeg speelruimte geven naar gelang diens behoefte (Schirato et al. 93, Foucault 407-22).

Wie over privacy spreekt met betrekking tot Facebook heeft het over persoonlijke gegevens zoals namen, e-mailadressen, foto's en voorkeuren maar ook nagelaten sporen van aanwezigheid in de fysieke ruimte (bezochte evenementen, woonplaatsen en adressen van scholen en bedrijven). Het zijn gegevens die we in principe zelf ter beschikking stellen vanaf het moment dat we toetreden tot het Facebookuniversum. De aanwezigheid van Facebook heeft van privacy iets controversieels gemaakt, door de manier waarop het bedrijf omspringt met haar beleid, het raamwerk waarbinnen zij gebruikers laat functioneren en de combinatie met onze behoefte onszelf uit te drukken in onze omgeving.

Zo bezien is het discours van privacy in relatie tot Facebook slechts één van de elementen die het vormt tot disciplinerend *apparatus*. Wat we doen als we onszelf *verdaten* op Facebook is niets anders dan onszelf onderwerpen aan de machtsstructuur die is doorgesijpeld in dit instituut. Dat we onszelf hieraan onderwerpen om 'mee te doen' in de maatschappij is niet meer dan een natuurlijk gevolg van het feit dat we mens zijn. Als we Facebook zien als een op zichzelf staande entiteit, een soort mini-staat, lijkt het logisch dat we onszelf als onderdeel van de Facebookpopulatie overgeven aan hun *governmentality*. Volgens Foucault is biopolitiek een politieke strategie waarlangs Westerse staten al sinds de achttiende eeuw functioneren. Echter is Facebook slechts een instituut in een grotere samenleving en moeten we ons als gebruikers afvragen of wij ons willen onderwerpen aan deze

machtsstructuur, die in de maatschappij gesitueerd is in relatie tot andere instituties zoals werkgevers, medische instanties, verzekeraars en niet in de laatste plaats de staat.

## Tot besluit

In het informationele privacydebat zijn twee tegengestelde posities te ontwaren. Aan de ene kant van het spectrum vinden we een beweging die privacy ziet als iets wat coûte que coûte bewaard moet blijven om onze vrijheid en autonomie te bewaren -middels een *framework of contextual integrity* en de gepaste stroom van informatie volgens Helen Nissenbaum, door zich anoniem op internet te kunnen begeven zoals Evgeny Morozov zegt en het TOR-project realiseert en door privacyinstellingen van sociale netwerksites standaard op 'privé' aan te bieden, waar youropenbook.org aandacht voor vroeg.

Aan de andere kant vinden we een positie die privacy ziet als iets wat we zouden moeten opgeven, juist om onze vrijheid te bewaren -vanuit het idee dat 'open data', *real name policies* en radicale transparantie, naar ideeën van Jeff Jarvis en Mark Zuckerberg, ons los zullen maken van de mythe van perfectie en, volgens Jarvis en Christian Heller, ons waardevolle data zullen leveren waarmee we bijvoorbeeld medische vooruitgang kunnen boeken.

Deze laatste positie zich laat omschrijven als de post-privacy traditie en wil de voordelen van de zogenaamde *Verdatung* van de samenleving en van de burger daarin benadrukken. Zo zouden we ons niet moeten laten beperken door mogelijk impopulaire acties, door Jarvis de mythe van perfectie genoemd en tot uitdrukking komend in radicale transparantie van Zuckerberg. Het opgeven van privacy betekent het einde van de schone schijn waarin we onszelf soms anders moeten voordoen dan we werkelijk zijn, vinden zij. Als iedereen open zou zijn over zijn of haar seksuele geaardheid wordt

homoseksualiteit vast als een stuk normaler beschouwd en gaan afwijkende gedragingen er gewoon ‘bij’ horen, zouden post-privacy aanhangers zeggen. Buiten deze traditie kunnen we deze mythe ontkrachten als we de maatschappij en daarin het privacydiscours zien als een biopolitieke staat, zoals omschreven door Foucault. Hierin worden via zogenaamde disciplineringsmechanismen normale en abnormale categorieën onderscheiden. In zo’n samenlevingsvorm, waarop Westerse staten zich als sinds de achttiende eeuw baseren, is het derhalve onmogelijk om het beoordelen van mensen op afwijkend gedrag uit te roeien. Sociale uitsluitingsmechanismen zijn, of we het nu leuk vinden of niet, onderdeel van de samenleving.
Daaraan verwant zullen de *Datenschutzer,* over wie Heller schreef, de link tussen de *Verdatung* van mensen en de geïnternaliseerde blik die de machtsrelatie constitueert relateren aan het Derde Rijk en deze vergelijking lijkt mij dan ook evident.

De tegengestelde positie, gevormd door privacybewakers, ziet om deze reden in de privésfeer juist een toevluchtsoord en een ontplooiingsmechanisme om autonomie te bewaren. Alleen in een veilige ruimte waarin we ons aan het oog van de maatschappij kunnen onttrekken, zullen we tot ontwikkeling kunnen komen.

Menselijke eigenschappen zoals het zich willen ontplooien, maar ook het willen delen van persoonlijke verhalen en het zich willen uitdrukken in meningen en voorkeuren ten opzichte van de sociale omgeving zijn een natuurlijk onderdeel van de samenleving en een instituut als Facebook leent zich hiervoor uitstekend als katalysator. Facebook, met haar eigen *apparatus* aan regels, technologieën en discours functioneert

als een machtsstructuur zoals we die in het panopticum zien. Het bedrijf maakt gebruik van de menselijke eigenschappen van haar populatie en verzamelt haar gegevens om in haar onderhoud te kunnen voorzien. Facebook staat niet los van de andere instituten in de maatschappij en daarom zijn die gegevens ook buiten het instituut Facebook gewild, bijvoorbeeld voor andere commerciële partijen of de sociale dienst. Dit komt slecht uit in een maatschappij die zich kenmerkt als een *dataspace* die zich zwak toont in de zin van technologische infrastructuur (gevoelig voor hackers), in de zin van menselijke infrastructuur (die ten grondslag ligt aan de technologische) en in de zin van onze eigen rol als subject wat zich wil onderwerpen aan de regels van de machthebber om mee te kunnen draaien in het Facebookuniversum. Aangezien de meeste gebruikers een gepaste stroom van informatie willen zien, en er een contrast is tussen wat we met een selecte groep andere Facebookgebruikers willen delen en met andere instituten zoals commerciële bedrijven, maar ook de staat, ontstaat er een privacyprobleem wat typisch is voor een hybride ruimte. In zekere zin is dit een zelfde probleem als waar gebruikers van Google in het voorbeeld uit de inleiding tegenaan lopen. Hoe reguleren we onze data in een maatschappij waarin ze gevoelig zijn, zonder dat we worden uitgesloten van deelname?

Hoe moeten we in een dergelijk machtsconstructie functioneren? Om te beginnen zouden we een balans moeten vinden tussen het internaliseren van de kritische blik van de machthebber in het instituut waartoe we behoren en het opzetten van een bril van een goed geïnformeerde entiteit die deze mechanismen overziet en inzet op een gepaste stroom van informatie. We moeten ons bewust worden van de zwakheden van het systeem; notie nemen van het feit dat

wanneer data er zijn, ze gebruikt kunnen worden en ons baserend op een staat die mede draait op statistische gegevens van hun burgers, dat ook zullen worden. Op die manier moeten we onze eigen censor worden. En ons tevens beseffen dat we, vrij naar Rebecca MacKinnon, een burger zijn in de hybride *dataspace* in plaats van een gebruiker.

Het was mijn missie om mijn opvatting uit 2010 over informationele privacy te herzien middels een analyse van de posities in en goed onderbouwde beschouwing van het debat. Mijn conclusie hierboven staat in schril contrast met de post-privacy positie. Wie meent dat hij niets te verbergen, en dus niets te vrezen, heeft en -naar een bekende uitspraak van Google-baas Eric Schmidt- zegt: *"if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place,"* heeft een idee wat alleen in de meest ideale, vreedzame, gelijke, onbedorven, vrije democratie kan functioneren. Een utopisch idee dus.

# Literatuur

Biermann, Kai. ‘Betrayed by your own data.’ *Die Zeit Online* 26 maart 2011. Web. 14 augustus 2011.

Bits of Freedom. *Position paper netwerkneutraliteit* 5 januari 2010. Web. 13 augustus 2012.
---. *Over Bits of Freedom* Web. 13 augustus 2012.

Boomen, Marianne van den. ‘Wie is er bang voor technologisch determinisme?’ *I & I: kwartaalreeks over informatie en informatiebeleid* Vol. 21, no. 2, 2003. 6-7.

Boyd, Danah. ‘Why Privacy is Not Dead.’ *Technology Review.* September-oktober 2010. Web. 1 augustus 2012.

Caluya, Gilbert. ‘The post-panoptic society? Reassessing Foucault in surveillance studies.’ *Social Identities* Vol 16, No 5, september 2010. 621-633.

Cyberev.org Web. 9 juni 2012.

De Souza e Silva, A. ‘From Cyber to Hybrid: Mobile Technologies as Interfaces of Hybrid Spaces.’ *Space and Culture.* Vol 9, no 3, augustus 2006. 261-278.

Doctorow, Cory. ‘We need a serious critique of net activism.’ *The Guardian.* 25 januari 2011. Web.

Facebook. *Facebook Newsroom.* Web. 1 augustus 2012.

F.A.T. Lab. *About.* Web. 13 augustus 2012.

Foucault, Michel. *Security, Territory, Population. Lectures at the Collège de France 1977-78* Palgrave Macmillan. 2007.
---. *The Birth of Biopolitics* Palgrave Macmillan. 2008.

Google. ‘Updating our Privacy Policies and Terms.’ *Google Blog* 2012. Web. Laatst bekeken: 14 april 2012.

Gitelman, Lisa. *Always Already New* Cambridge: MIT Press. 2006.

Kirkpatrick, David. *The Facebook Effect* Ebury Publishing. 2010.

Kluitenberg, Eric. ‘Netwerk van golven.’ In: ‘Hybride ruimte: Hoe draadloze media de publieke ruimte mobiliseren. *Open* Nr. 11 (2006) Print. 6-16.

Kluitenberg, Eric. en Howard Rheingold. ‘Welbewust afhaken’. In: ‘Hybride ruimte: Hoe draadloze media de publieke ruimte mobiliseren. *Open* Nr. 11 (2006) Print. 28-37.

Lovink, Geert. ‘The society of the query and the Googlization of our lives.’ *Eurozine.* 5 september 2008. Web.

Mackenzie, Adrian. ‘From Café to Parkbench: WIFI and Technological Overflows in the City.’ *Mobile Technologies and the City*. Ed. John Urry & Mimi Sheller. London, New York: Routledge, 2006. 137-151.

MacKinnon, Rebecca. ‘Webspecial: Rebecca MacKinnon.’ *VPRO* 25 mei 2012. Web. 1 juni 2012.

Mancini, C. et.al. ‘From Spaces to Places: Emerging Contexts in Mobile Privacy’. In: *Proceedings of the 11th International conference on Ubiquitous Computing.* 30 september - 3 oktober 2009, Orlando, Florida, USA. Print.

Manovich. Lev. ‘The Poetics of Augmented Space.‘ *Visual Communication* Vol 5, no 2, juni 2006. 219-240.

Moses, Asher. ‘Banned for keeps on Facebook for odd name.’ *SMC.com.au* 25 september 2008. Web. 14 augustus 2012.

Nelson, Sara C. ‘Facebook removes image of two men kissing.’ *Huffington Post UK* 23 maart 2012. Web. 15 augustus 2012.

Nissenbaum, Helen. *Privacy in Context* Stanford, California: Stanford U.P. 2010.

Orwell, George. *1984* Londen: The Penguin Group. 2008.

Roessler, Beate. ‘New Ways of Thinking About Privacy.’ *The Oxford Handbook of Political Theory.* Oxford U.P. 2006. 694-712.

Schirato, Tony, Geoff Danaher, en Jen Webb. *Understanding Foucault* Londen: SAGE Publications Ltd. 2012.

Solove, Daniel J. *Understanding Privacy* Cambridge: Harvard UP. 2008.
---. *The Digital Person* New York: New York U.P. 2004.

Spitz, Malte. ‘Six monts of my life in 35,000 records.’ *Malte-Spitz.de* 4 maart 2011. Web. 14 augutus 2012.

Spoel, Iris van der. ‘Googlen in ruil voor je gegevens is geen slechte deal.’ *NRC Next* 9 maart 2010.

Teffer, Peter. ‘Pas op voor mega-bedrijf Google, dat lijdt aan data-obesitas, zegt mediatheoreticus Lovink.’ *NRC Next* 1 maart 2010.

Vogelaar, Frans. ‘Hybrid Spaceman I - Frans Vogelaar’. *Blik* No. 5, maart 2012. 28-35.

Vogelaar, Frans, Elizabeth Sikiardi. ‘Soft Urbanism.’ ‘ In: ‘Hybride ruimte: Hoe draadloze media de publieke ruimte mobiliseren. *Open* Nr. 11 (2006) Print. 82-95.

Vogelstein, Fred. ‘How Mark Zuckerberg Turned Facebook into the Web’s Hottest Platform.’ *Wired.com* 9 juni 2007. Web. 1 augustus 2012.

‘Wat nou privacy?’ *VPRO Thema.* VPRO. Nederland 2. 27 oktober 2010. Televisie.

Vries, Imar de. ‘The vanishing points of mobile communication.’ *Digital Material.* Amsterdam: Amsterdam U.P. 2009. 81-93.

Youropenbook.org Web. 29 april 2012. <website niet langer beschikbaar>

Die Zeit. ‘Tell-all telephone.’ *Die Zeit Online* 2011. Web. 14 augustus 2011.