Cookies en controle:
Privacy in een surveillancemaatschappij

Masterscriptie Nieuwe Media & Digitale Cultuur
Roos Vermeulen
Studentnummer: 3218031
Tutor: René Glas
Tweede lezer: Isabella van Elferen
Faculteit Geesteswetenschappen, Universiteit Utrecht
14 juni 2013

Samenvatting

Dit onderzoek gaat over controle over privacy, surveillance en internet cookies. De onderzoeksvraag hierbij is: *In hoeverre is controle over privacy mogelijk op internet als het gaat om de persoonlijke informatie die websites opslaan met behulp van cookies?* Deze vraag zal beantwoord worden door eerst een theoretisch kader over surveillance en privacy neer te zetten en vervolgens een kritische discoursanalyse van de casestudy, het Nederlandse cookiebeleid, te maken. Beargumenteerd wordt dat de huidige maatschappij een 'control society' (Deleuze, 1992) is waarin sprake is van een ongelijke machtsverdeling tussen bedrijven en consumenten door de manier waarop surveillance wordt uitgeoefend. Hoewel de maatschappij en het internet kenmerken vertonen van een transparant en gelijkwaardig systeem zoals het 'catopticon' (Ganascia, 2007) waarin gebruikers vrijwillig participeren aan 'self-surveillance' (Campbell en Carlson, 2002) kan een gebruiker nooit volledige controle over zijn informationele privacy hebben omdat de 'complete context' en 'perceived context' van een privacysituatie met betrekking tot cookies niet overlappen door informatieassymetrie. Pas als de internetgebruiker volledig op de hoogte is van de weg die zijn 'flow' (Nissenbaum, 2004) van (persoonlijke) informatie aflegt, kan hij controle hebben over privacy. Het Nederlandse cookiebeleid zet een stap in de goede richting door de internetgebruiker beter te informeren en mogelijkheden te bieden de controle over data in eigen hand te nemen.

Inhoudsopgave

Inleiding

> *Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations* (Solove, "Understanding Privacy", 2008, p. 1).

Zoals rechtsgeleerde Daniel Solove beschrijft, is privacy een moeilijk te definiëren concept. Vooral in de huidige maatschappij waarin het internet een groot goed is en informatie overal aanwezig is, vraagt men zich soms af of privacy wel te controleren valt en wat het nog inhoudt. Wat voor rol speelt privacy nog in onze huidige cultuur?

Volgens socioloog David Lyon leven we in een 'surveillance society' waarin iedereen constant in de gaten gehouden wordt door iedereen. Surveillance is hierin het observeren van individuen of groepen en het verzamelen, opslaan, overdragen, opvragen, vergelijken en verhandelen van persoonlijke gegevens (Lyon, 2008, p. 3). Naarmate de digitale technologie is ontwikkeld en het internet gegroeid, is surveillance van individuen toegenomen. Door de mogelijkheden die de technologie biedt, zoals onder andere het gebruiken van cookies om persoonsgegevens op te slaan, wordt het steeds makkelijker om deze gegevens te verkrijgen. Dit kan zowel voor- als nadelen hebben, bijvoorbeeld als een klant iets koopt bij *Amazon* en andere suggesties ziet die *Amazon* speciaal voor hem doet. Een voordeel kan zijn dat de suggesties aansluiten op zijn interesse, maar nadelig kan het zijn dat het moeilijk is om uit zijn eigen cirkel van interesses te komen: *"Once classified, it is difficult to break out of the box"* (Lyon, 2008, p. 1).

Van bijna alles wat je doet wordt informatie opgeslagen: een dagje in de stad wordt gefilmd door beveiligingscamera's, je pintransacties worden opgeslagen en je smartphone houdt bij op welke locatie je bent. Vooral op het internet valt de surveillance moeilijk te omzeilen. Je zoekresultaten op Google zijn gepersonaliseerd met behulp van de informatie die Google over jou heeft opgeslagen. Deze informatie komt uit je e-mails, wat voor filmpjes je kijkt op YouTube en wat voor advertenties je aanklikt. Websites plaatsen cookies op je computer om je surfgedrag te monitoren en een profiel over je op te bouwen, zo wordt gepersonaliseerde reclame voor je samengesteld. Als je erover nadenkt, krijg je het gevoel constant geobserveerd te worden. Alleen weet je vaak niet zeker wanneer het echt gebeurt. De vraag is in hoeverre dit de manier is waarop het internet werkt. Dus zoals bij *Amazon*; het gebruik van persoonlijke gegevens voor het maken van (persoonlijke) reclame. Of bijvoorbeeld op *Facebook*; men kan gratis gebruik maken van deze 'social networking site' door persoonlijke gegevens te delen. Is dit gewenst voor de internetgebruiker of moet hier meer kritisch naar gekeken worden en misschien zelfs verzet tegen geboden worden?

Toch doet de internetgebruiker hier vrijwillig aan mee; hij participeert door online content te leveren. Anonimiteit lijkt niet meer hoog in het vaandel te staan. Informatiewetenschappers Queiroz en De Queiroz stellen dat veel mensen hun eigen 'private life show' uitvoeren op het internet: *""The Private life show" is a phenomena which can be seen in the media and networking websites such as Facebook, MySpace and Orkut among others, a string of reality TV shows (e.g. Big Brother), and printed or electronic gossipy press"* (Queiroz en De Queiroz, 2010, p. 1). Het delen van persoonlijke informatie op internet is niet iets waar de internetgebruiker nog moeilijk over doet. Hij heeft juist behoefte om zichzelf te presenteren op internet.

Het onderwerp van dit onderzoek is controle over privacy. Het is moeilijk te bepalen wat dit precies is. Privacy heeft volgens verschillende wetenschappers (onder andere Solove, Rachels, Vedder, Waldo et al.) met controle over informatie te maken, controle in de zin van

de macht hebben over wat er met jouw informatie gebeurt. Privacy heeft in de huidige maatschappij veel te maken met informatie en de opslag hiervan, in deze vorm wordt privacy onder andere aangeduid als 'information privacy' (Bélanger en Crossler, 2011) en 'data privacy' (Queiroz en De Queiroz, 2010). Ik zal privacy in dit onderzoek zien als 'information privacy', oftewel informationele privacy. Dit zal ik doen omdat de invloed die cookies op privacy hebben, in eerste instantie gaat over informationele privacy. Het gebruik van persoonsgegevens kan deze privacy aantasten.

In dit onderzoek zal ik als rode draad het gebruik van cookies en de privacykwesties die hierbij komen kijken, aanhouden. Websites plaatsen deze cookies, bestandjes die zich installeren op een computer en bepaalde gegevens opslaan als de eigenaar van de computer websites bezoekt. Er bestaan verschillende soorten cookies. Ten eerste de first-party cookies; dit zijn cookies die door de bezochte website worden geplaatst voor eigen doeleinden. Dit kan bijvoorbeeld het onthouden van inloggegevens zijn. Daarnaast bestaan er third-party cookies; dit zijn cookies die door een website worden geplaatst en niet voor eigen doeleinden zijn. Vaak volgen deze cookies de gebruiker over meerdere webpagina's en wordt de persoonlijke informatie die verkregen wordt, gebruikt om een profiel van de gebruiker op te bouwen. Dit profiel kan onder andere ingezet worden om op de gebruiker persoonlijk gerichte reclame te maken. Naast cookies met verschillende doeleinden die door verschillende partijen geplaatst worden, bestaan er ook verschillende werkingen van cookies. Een cookie kan een http-cookie zijn of een flashcookie. Http-cookies hebben een vervaldatum en zijn makkelijker te verwijderen dan flashcookies, deze zijn hardnekkig, kunnen meer informatie bevatten en hebben geen vervaldatum (Pierson en Heyman, 2011, p. 35).

De reden dat cookies een belangrijke plaats innemen in het huidige privacydebat, is dat de juiste balans tussen het gebruik van het internet en beschermen van privacy nog niet is gevonden. Consumenten kunnen als het ware 'betalen' met persoonlijke informatie in ruil voor gratis internetdiensten (Pierson en Heyman, 2011, p. 32). Bedrijven gebruiken de informatie die cookies verzamelen om persoonlijke advertenties te plaatsen, door de advertentie aan te passen aan de interesses van de consument is er meer kans dat de consument op de advertentie klikt. Dit is een belangrijke manier van inkomstenvergaring op het internet, maar om meerdere redenen valt deze manier te bekritiseren. Ten eerste zijn veel mensen niet op de hoogte van de gevolgen voor hun privacy door de plaatsing van cookies op hun computer en is over het algemeen veel onduidelijkheid over waar en hoe lang de informatie wordt opgeslagen en waarvoor het precies gebruikt wordt (Christiansen, 2011, p. 510-511). Ten tweede is het lastig om zowel de rechten van de internetgebruiker als van de bedrijven te beschermen en vooral om een wetgeving te maken die hieraan bijdraagt (Solove, 2008).

De cookiewetgeving in Nederland zal ik als casestudy gebruiken voor dit onderzoek. In Nederland geldt sinds vijf juni 2012 een cookiewetgeving waarin is bepaald dat websites toestemming moeten vragen aan gebruikers voor het plaatsen van cookies. De meeste websites vragen deze toestemming door middel van pop-ups. Tegen deze wetgeving is veel verzet ontstaan, doordat het gebruiksgemak van het internet verminderde. Er bleek veel onwetendheid te zijn over de gevolgen die het accepteren van cookies voor je privacy kunnen hebben. Daarnaast bleek dat privacy al snel niet meer als probleem wordt gezien als het internet minder toegankelijk is (*Volkskrant,* 14-15 februari 2013).

Het debat over cookies weerspiegelt het grotere debat rondom privacy op internet over de verwachtingen van de gebruiker van een gratis en toegankelijk internet en de behoefte van de gebruiker om informatie te delen op internet en te participeren aan de internetcultuur (Queiroz en De Queiroz, 2010). De vraag die Daniel Solove in zijn werk stelt, geeft de basis van dit onderzoek mooi weer: "*How can the free flow of information make us more free yet less free as well?*" (Solove, 2007, p. 17). In dit onderzoek zal ik de huidige

maatschappij typeren als het gaat om de mate van surveillance en de waarde en betekenis van privacy in deze maatschappij. Ook zal ik naar de geschiedenis van de 'surveillance society' kijken en op welke manier deze zich heeft ontwikkeld in de huidige cultuur. Het gebruik van cookies om persoonlijke informatie op te slaan, staat in dit onderzoek centraal en de betekenis van surveillance en privacy in de huidige cultuur zal dan ook worden toegespitst op het gebruik van cookies. De hoofdvraag die ik hierbij zal aanhouden is: *In hoeverre is controle over privacy mogelijk op internet als het gaat om de persoonlijke informatie die websites opslaan met behulp van cookies?*

De methoden die ik in mijn onderzoek zal gebruiken, zijn een kwalitatieve literatuurstudie en een kritische discoursanalyse van een casestudy. De werkwijze bij kwalitatief onderzoek wordt door socioloog Hennie Boeije beschreven als: "*literature including theory is used mainly to understand what is going on in the field and to discover theoretical perspectives, including proper concepts to look at the social phenomenon of interest"* (Boeije, 2010, p. 5). Vanuit de literatuur wil ik dus naar het fenomeen privacy kijken en specifiek de controle over privacy. In de literatuurstudie zal ik bronnen vanuit de media- en informatiewetenschap, maar ook enkele vanuit de rechtsgeleerdheid, analyseren. Om mijn hoofdvraag te beantwoorden moet ik onderzoek doen op het gebied van surveillance, privacy en cookies. Ten eerste zal ik een analyse uitvoeren van primaire bronnen over surveillance van Foucault en Deleuze en vervolgens hun theorieën bekijken vanuit de huidige cultuur met behulp van secundaire bronnen van onder andere Lyon, Elmer, Ganascia, Campbell en Carlson over de werking van surveillance in de huidige maatschappij. Deze bronnen zullen mij inzicht geven in de toepassing van de theorieën op de huidige cultuur en hierdoor zal ik de huidige rol van surveillance in de maatschappij kunnen identificeren. Daarna zal ik privacy en specifiek informationele privacy plaatsen binnen de omschreven surveillance society door (informationele) privacy te bekijken vanuit de context. Hierbij zal ik een tekstanalyse maken van primaire bronnen van Nissenbaum, Pierson en Heyman, en Solove over de context van privacy en het onderscheid tussen publiek en privé. Als secundaire bronnen zal ik onderzoeken gebruiken van onder andere Dawes, Barth et al. en Bélanger en Crossler. Deze bronnen zullen mij inzicht geven over informationele privacy en hoe dit in een maatschappij van surveillance past.

Ten slotte zal ik het Nederlandse cookiebeleid bestuderen met behulp van een discoursanalyse. Dit houdt in dat ik het discours rondom het Nederlandse cookiebeleid zal onderzoeken, hierbijzal ik krantenartikelen, kamerbrieven en andere bronnen analyseren om de receptie en uitvoering van het beleid kritisch te bekijken en hier vervolgens de theorie uit het theoretisch kader aan te verbinden. Discoursanalyse wordt door methodoloog Harry van den Berg gedefinieerd als "*onderzoek naar de manier waarop meningen en werkelijkheden discursief – dat wil zeggen in taal – geconstrueerd worden"* (Van den Berg, 2004, "KWALON 26"*,* p. 30). Het gaat uit van het constructivisme, oftewel dat de werkelijkheid maakbaar is en dat sociale werkelijkheden worden geconstrueerd door taal (Van den Berg, 2004, "KWALON 26"*,* p. 34). Een taaluiting wordt hierin als een aparte werkelijkheid gezien en niet alleen als representatie van een werkelijkheid. Ik zal de uitleg van 'critical discourse analysis' van taalkundige James Paul Gee aanhouden. Hij legt uit dat het doel van 'critical discourse analysis' is "*to intervene in, social or political issues, problems, and controversies in the world"* (Gee, 2010, p. 9). Er wordt dus niet alleen naar de taaluiting gekeken, maar ook naar de context van de taaluiting. Ik zal hiernaast de uitleg van Van den Berg over het in praktijk brengen van discoursanalyse aanhouden. Hij schrijft dat 'sociale categorisering' een belangrijke rol speelt in de discoursanalyse, dit houdt in dat in de analyse gekeken wordt hoe mensen hun sociale leefomgeving categoriseren (Van den Berg, 2004, "KWALON 27"*,* p. 27). Van den Berg legt uit dat het *"uitgangspunt is dat categorisering een kenmerk is van taalgedrag, dat – evenals andere vormen van sociaal gedrag –*

contextafhankelijk en dus variabel is" (2004, "KWALON 27", p. 28). In de casestudy zal de 'interdiscursiviteit' naar voren komen, oftewel hoe de teksten verschillende, soms tegenstrijdigige, vertogen bevatten (Van den Berg, 2004, "KWALON 27", p. 33).

In deze discoursanalyse zal ik als volgt te werk gaan: Ten eerste zal ik de ontwikkeling van de Nederlandse cookiewet analyseren aan de hand van discoursen van de Rijksoverheid, krantenartikelen en parlementaire brieven. Vervolgens zal ik het onderzoek van Kool et al. in opdracht van het TNO bestuderen om de situatie voor de invoering van de cookiewet te verduidelijken. Daarnaast zal ik de onduidelijkheden in de cookiewet toelichten door de analyse van documenten van de Nederlandse organisaties OPTA (Onafhankelijke Post- en Telecom Autoriteit) en Bits of Freedom, een organisatie die staat voor digitale burgerrechten. Ten slotte zal ik een terugkoppeling maken naar de hoofdvraag en de behandelde theorie uit de voorafgaande literatuurstudie.

Ik heb gekozen voor een casestudy naast de literatuurstudie omdat ik op deze manier de abstracte theorie aan de praktijk kan verbinden. De casestudy maakt de theorie tastbaarder en laat de mogelijkheden van toepassing op de praktijk zien. De keuze voor een kritische discoursanalyse heb ik gemaakt omdat ik naar de constructie van werkelijkheid om de fenomenen privacy en surveillance wil kijken en hoe de indeling in sociale categorieën door verschillende betrokken partijen verschilt. Dus bijvoorbeeld hoe het verplichten van een cookiewall voor sommigen meer onder de categorie privacy valt, maar voor anderen onder gebruiksgemak of marketing .

Dit onderzoek is relevant aangezien het actueel is. Het internet en de manier waarop surveillance hierop een rol speelt, blijft veranderen. Overheden zijn op zoek naar een manier om het cookiegebruik te reguleren en zo de privacy van internetgebruikers te beschermen. Het controleren van (informationele) privacy is een belangrijk onderwerp op het moment. Dit onderzoek sluit aan op de discussie hoe de burger zelf om moet gaan met surveillance en wat de verantwoordelijkheid van bedrijven is. Doordat het cookiebeleid in Nederland recentelijk aangepast is, vormt dit een goede case voor mijn onderzoek.

In het eerste hoofdstuk zal ik beargumenteren hoe de huidige maatschappij nog steeds als 'control society' (Deleuze, 1992) getypeerd kan worden. Hoewel veel internetgebruikers het internet zien als een 'catopticon' (Ganascia, 2007) waarin transparantie en gelijkheid zegevieren, is er nog steeds sprake van een ongelijke machtsverdeling. Een gedeelte van het hoofdstuk zal over de rol van de internetgebruiker gaan: Hoe de internetgebruiker als consument zelf participeert aan het 'participatory panopticon' (Campbell en Carlson, 2002) en zonder tegenstribbeling het protocol volgt (Galloway, 2004).

Vervolgens zal ik in het tweede hoofdstuk specifieker ingaan op de vraag wat privacy is en wat controle over privacy betekent in de huidige maatschappij. Ik zal privacy in dit onderzoek zien als informationele privacy in navolging van Bélanger en Crossler (2011). In dit hoofdstuk wordt gesteld dat een privacykwestie per situatie verschilt, dus dat er geen duidelijk onderscheid tussen publieke en privé-informatie kan zijn (Solove, 2007). Elke situatie kent een verschillende 'flow' van informatie met verschillende 'informational norms' (Nissenbaum, 2004). Of een internetgebruiker controle uit kan oefenen over zijn informationele privacy hangt af van de mate van overlapping tussen de 'complete context' en de 'perceived context' (Pierson en Heyman, 2011), oftewel in hoeverre de internetgebruiker op de hoogte is van de weg die zijn informatie aflegt.

Ten slotte zal ik, in het derde hoofdstuk, beargumenteren dat het Nederlandse cookiebeleid een stap in de goede richting heeft gezet wat betreft het beschermen van informationele privacy. Het heeft de Nederlandse burger handvatten aangereikt voor het controleren van zijn privacy. Toch hangt de werkelijke controle over privacy af van de

welwillendheid van de burger, zolang er sprake is van een informatieassymetrie tussen de burger en de bedrijven die cookies plaatsen, zal de burger weinig controle kunnen uitvoeren over zijn privacy.

Hoofdstuk 1: Van disciplinary society naar sousveillance society, waar zijn we nu?

De informaticus Roger A. Clarke schreef in 1988 als een van de eersten over surveillance mogelijk gemaakt door informatietechnologie. Hij noemt dit 'dataveillance' en definieert het als: "*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"* (Clarke, 1988, p. 499). Hij schrijft over surveillance met als doel het monitoren van criminele activiteiten, specifiek om verdachte personen en groepen in de gaten te houden. Clarke volgt hierin de definitie van surveillance uit 'The Oxford Dictionary': "*watch or guard kept over a person, etc., esp. over a suspected person, a prisoner, or the like; often spying, supervision; less commonly, supervision for the purpose of direction or control, superintendence"* (Clarke, 1988, p. 499).

Nu, 25 jaar later, is de informatie technologie verder ontwikkeld en de hoeveelheid surveillance toegenomen, onder andere door de mogelijkheden die nieuwe technologieën hebben gebracht. De socioloog David Lyon beweert dat surveillance behoort tot de manier waarop de wereld georganiseerd is in de éénentwintigste eeuw (Lyon, 2008, p. 1). Hij beargumenteert dat surveillance niet meer alleen om het monitoren van verdachte activiteiten gaat, maar steeds meer te maken heeft met het moderne verlangen naar efficiëntie, snelheid, controle en coördinatie (Lyon, 2008, p. 1).

In dit hoofdstuk zal naar de surveillance in de maatschappij gekeken worden en naar hoe het systeem van surveillance in de huidige cultuur werkt. Cookies vervullen een surveillerende rol aangezien ze het gedrag van internetgebruikers volgen. Om de controle over online privacy te bepalen, is het dus belangrijk om eerst naar surveillance te kijken. Dit hoofdstuk biedt een theoretisch kader van surveillance theorie, aan het eind van het hoofdstuk zal de plaats van surveillance in de huidige maatschappij duidelijk worden. Dit zal gebeuren door vanuit de geschiedenis van surveillance te kijken naar de huidige situatie en binnen de huidige situatie zowel de rol van de observeerders als de geobserveerden te beschrijven. Belangrijk bij het onderzoek naar surveillance zijn ook de machtsrelaties en de conditionerende effecten die zich in een systeem van surveillance bevinden en de invloed van de internetgebruiker, die binnen de huidige surveillance op het internet vaak als consument wordt beschreven.

Disciplinary en control societies

De manieren waarop controle en surveillance uitgeoefend worden in een maatschappij zijn veranderd door de eeuwen heen. Volgens de filosoof Michel Foucault bestonden er in de achttiende, negentiende en begin van de twintigste eeuw 'disciplinary societies'. Onder discipline verstond Foucault het volgende: "'*Discipline' may be identified neither with an institution nor with an apparatus; it is a type of power, a modality for its exercise, comprising a whole set of instruments, techniques, procedures, levels of application, targets; it is a 'physics' or an 'anatomy' of power, a technology"* (Foucault, 1977, p. 10). Discipline is dus een vorm van macht die op allerlei verschillende wijzen uitgevoerd kan worden en niet gebonden is aan een instituut. Foucault beschrijft de beweging van gesloten 'disciplinary societies' naar een meer open vorm van 'panopticism'. In een gesloten 'disciplinary society' wordt discipline uitgevoerd in afgesloten instituten zoals gevangenissen, ziekenhuizen en scholen. De verschillende omgevingen van discipline interfereren niet met elkaar. In een omgeving van 'panopticism' wordt een begin gemaakt aan een meer effectieve, overkoepelende vorm van dwang (Foucault, 1977, p. 7). Het panopticon is een ontwerp voor een gevangenis door Jeremy Bentham waarin de gevangene constant het gevoel heeft in de gaten gehouden te worden, maar dit niet zeker weet. De constructie van de gevangenis

maakt het mogelijk een constante surveillance uit te oefenen op de gevangenen zonder daar veel bewakers voor nodig te hebben:

> *At the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other, on the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy* (Foucault, 1977, p. 3).

Doordat de gevangene zich constant bekeken voelt, oefent de 'supervisor' altijd macht uit op de gevangene (Foucault, 1977, p. 3) en hoeft er nooit kracht gebruikt te worden om de gevangene onder controle te houden (Foucault, 1977, p. 4). Het vergaren van kennis is een belangrijk onderdeel van het panopticon: "*The Panopticon functions as a kind of laboratory of power. Thanks to its mechanisms of observation, it gains in efficiency and in the ability to penetrate into men's behaviour; knowledge follows the advances of power, discovering new objects of knowledge over all the surfaces on which power is exercised*" (Foucault, 1977, p. 5). Door te observeren vergaart de bewaker kennis over het gedrag van de gevangene. Deze kennis wilde de gevangene misschien niet delen, maar aangezien hij constant onder surveillance staat, heeft hij geen keus. Het panopticon beïnvloedt ook het gedrag van de gevangene, het werkt als het ware zelf-disciplinerend. De gevangene past zijn gedrag aan omdat hij denkt dat hij constant in de gaten gehouden wordt (Foucault, 1977, p. 3). De machtsrelatie tussen de gevangene en de bewaker wordt in stand gehouden in het panopticon, zelfs op de momenten dat de bewaker niet daadwerkelijk aan het bewaken is. De gevangenen behouden zelf de machtsrelatie door het gevoel van constante surveillance: "*The inmates should be caught up in a power situation of which they are themselves the bearers"* (Foucault, 1977, p. 3). Belangrijk voor het verdere onderzoek is dat het panopticon vaak als metafoor wordt gebruikt voor het beschrijven van een systeem van machtsrelaties. In de verdere toespitsing op de huidige cultuur zal het panopticon dus niet specifiek verwijzen naar een gevangenis.

De filosoof Gilles Deleuze schreef dat de 'control societies' de 'disciplinary societies' vervangen (Deleuze, 1992, p. 4). Hij beargumenteert dat in de 'disciplinary societies' de fabriek en industriële machines belangrijk waren. In de 'control societies' is de fabriek vervangen door de corporatie en zijn computers belangrijker geworden. Marketing is hierin de 'ziel' van de corporatie (Deleuze, 1992, p. 4-6). In de 'disciplinary societies' moest men steeds opnieuw beginnen in een nieuwe omgeving van discipline. In de 'control societies' begeeft men zich in een netwerk waarin controle en disciplinering plaatsvindt (Deleuze, 1992, p. 5-6). Foucault schreef ook dat de disciplinering steeds minder te vinden is in afgesloten instituten en steeds meer een gegeneraliseerd mechanisme wordt (Foucault, 1977, p. 10). In zijn argumentatie betrekt Deleuze een gedachte van Felix Guattari waarin een 'Big Brother' scenario in een 'control society' wordt beschreven:

> *Felix Guattari has imagined a city where one would be able to leave one's appartment, one's street, one's neighborhood, thanks to one's (dividual[1]) electronic*

[1] Alexander Galloway beschrijft 'dividual' als volgt: "*Deleuze's neologism comes from the word "individuate." Dividuation would thus be the opposite: the dissolving of individual identity into distributed networks of information"* (Galloway, 2004, p. 12).

> *card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position – licit or illicit – and effects a universal modulation* (Deleuze, 1992, p. 7).

In dit scenario wordt, net als in het panopticon van Foucault, de burger constant in de gaten gehouden. In de 'control societies' spelen gegevens en de opslag hiervan echter een grotere rol dan in het panopticon. In de 'disciplinary societies' wordt men geobserveerd in instituten en kunnen dit aparte omgevingen zijn. In 'control societies' wordt geobserveerd binnen een netwerk en is er minder sprake van afscheiding tussen verschillende omgevingen van surveillance.

Ondanks dat de huidige maatschappij nog kenmerken vertoont van de 'disciplinary societies', bijvoorbeeld door het disciplinerende regime in gevangenissen en afgesloten instituten, valt de huidige maatschappij te typeren als een 'control society'. Controle wordt uitgeoefend door onder andere de overheid en corporaties. Het internet biedt een platform voor het uitvoeren van deze controle. Belangrijk is dat er informatie verzameld wordt in de 'control society', in de huidige maatschappij gebeurt dit onder andere door het inzetten van cookies. Doordat er in de 'control society' minder op zichzelf staande instanties van surveillance bestaan, verspreid de verkregen informatie zich snel. Deleuze beschrijft marketing al als de ziel van de corporatie, dit geldt nog steeds. Deze ziel wordt in de huidige 'control society' als het ware gevoed met persoonlijke gegevens van internetgebruikers door middel van cookies. Hierdoor kunnen effectieve marketingstrategieën worden ingezet en kan gepersonaliseerde reclame worden gemaakt.

Het panopticon of het catopticon?

De huidige maatschappij is een omgeving waarin surveillance in hoge mate aanwezig is. Zowel het internet waarop gegevens van gebruikers worden verzameld als een stadscentrum waarin camera's alles registreren, bieden mogelijkheden voor het gebruik van het panopticon als metafoor. Vooral het gegeven dat men in de gaten wordt gehouden zonder dat men weet door wie en wanneer precies, komt overeen met de opzet van het panopticon. In dit gedeelte van het hoofdstuk zal ik ingaan op het panopticon (als metafoor) in de huidige cultuur van surveillance. Dit is van belang voor mijn onderzoek omdat de opzet van het panopticon doet denken aan de manier waarop bedrijven persoonlijke informatie opslaan met behulp van cookies. Vooral het gegeven dat de geobserveerde niet precies weet wanneer hij geobserveerd wordt.

Mediawetenschapper Greg Elmer beschrijft verschillende interpretaties van het panopticon in de huidige cultuur. Hiermee maakt hij een brug tussen de klassieke theorie van Foucault en Deleuze en de huidige maatschappij. Één interpretatie van het panopticon noemt hij 'inversed panopticism', hierin is sprake is van een synoptische relatie in het panopticon. In deze synoptische relatie gebeurt het omgekeerde als in het originele panopticon: Hierin observeren een paar mensen de massa, bij een synoptische relatie observeert de massa een paar mensen, zoals politici of popsterren (Elmer, 2003, p. 232). Elmer noemt dit 'spectatorship', dus de meeste mensen zijn toeschouwers, dit doet aan een fancultuur denken (2003, p. 232-233). Deze synoptische relatie is dus niet disciplinerend, omdat er niet het gevoel heerst dat men constant geobserveerd wordt, zoals in het originele panopticon.

Elmer omschrijft 'panoptic surveillance' hierna als: "*a multiplicity of processes that work to increasingly quantify and qualify not only the specific behaviours of consumers (or other sales, inventory or distribution data), but also the efficiency of the panoptic process itself"* (Elmer, 2003, p. 233). Elmer bekijkt het panopticon in de huidige cultuur dus vooral

binnen een context van consumentisme. In zijn interpretatie van het panopticon gaat het om zowel efficiëntie van het surveillance systeem als het disciplineren van consumentengedrag.

De benadering van Elmer lijkt op de control society van Deleuze, maar Elmer argumenteert nog een stap verder. Deleuze schrijft ook over marketing en het volgen van mensen door informatie op te slaan, maar Elmer vult dit aan met de invloed die dit heeft op het gedrag van consumenten. Deleuze kijkt dus meer vanuit de corporatie en Elmer vanuit de consument die verbonden is aan de corporatie. Dit is belangrijk voor het beantwoorden van de vraagstelling aangezien de cookies die de privacy mogelijk kunnen schaden onder andere persoonsgegevens opslaan met als uiteindelijk doel de consument te interesseren voor bepaalde diensten of producten door middel van gepersonaliseerde reclame.

Elmer beschrijft hoe, in wat hij het 'panoptic diagram' noemt, consumenten niet alleen worden gedisciplineerd maar ook beloond[2]. Hiermee doelt hij op de manier waarop gegevens worden gebruikt voor onder andere persoonlijke reclame en gepersonaliseerde zoekresultaten op internet. "*The panoptic diagram, in other words, only disciplines consumers if they actively seek out the unfamiliar, the different, the previously unseen, purchased, or browsed*" (Elmer, 2003, p. 245). Dus zolang de gebruiker binnen zijn eigen cirkel van interesses blijft, werkt het systeem mee met de gebruiker. Pas als de gebruiker zich buiten de gebaande paden wil begeven, ondervindt hij hinder van het 'panoptic diagram'. Dit heeft onder andere te maken met het gebruik van cookies door websites. Met behulp van (third-party) cookies wordt een profiel van de gebruiker opgesteld. Dit profiel bestaat onder andere uit de interesses van de gebruiker en hiermee kan gepersonaliseerde reclame worden gemaakt. Deze gepersonaliseerde reclame draagt bij aan de 'panoptic diagram' waarin de gebruiker binnen een bepaalde cirkel van interesses blijft. Aangezien de reclame telkens weer dezelfde interesses aanspreekt, komt de gebruiker minder snel in aanraking met onbekende terreinen.

Cookies spelen hier dus een surveillerende rol en hoewel de surveillance door cookies vanuit veel verschillende punten gebeurt, is er toch een vergelijking te trekken met panoptische surveilance. De bedrijven die achter de cookies staan en dus uiteindelijk verantwoordelijk zijn voor de surveillance (de cookies zijn het technologische middel dat ze gebruiken) kunnen worden gezien als de centra in het panopticon (zoals Elmer 'panoptic surveillance' beschrijft) van waaruit de surveillance wordt uitgeoefend. Communicatiewetenschappers John Edward Campbell en Matt Carlson noemen dit 'corporate surveillance': "*It is the corporation that appears to dictate the conditions of the marketplace, and, correspondingly, constructs and maintains our participatory Panopticon*" (Campbell en Carlson, 2002, p. 603). Volgens Campbell en Carlson doet de internetgebruiker vrijwillig mee aan 'self-surveillance' en wordt hij zo een 'economic subject' (p. 588). Bij 'self-surveillance' deelt de gebruiker persoonlijke gegevens op het internet die zo bij corporaties terecht komen en gebruikt worden voor economische doeleinden. Als we niet vrijwillig meedoen aan de 'gaze' van marketeers, worden we buitengesloten van de voordelen die de corporaties geven (Campbell en Carlson, 2002, p. 592). Dus als een gebruiker geen cookies accepteert, kan hij niet profiteren van gepersonaliseerde reclames en dergelijken. Dit komt dus op hetzelfde neer als het 'panoptic diagram' van Elmer dat alleen een disciplinerende werking heeft als de consument ander gedrag vertoont dan verwacht.

[2] Elmer noemt dit 'diagram' in navolging van Deleuze die hiermee uitleg geeft van een model voor "*the process of encoding, distributing, and deploying information flows from decentralized apparatuses* (Elmer, 2003, p. 242). Het 'diagram' is dus een soort model van informatie 'flows' in een gedecentraliseerd netwerk.

Informaticus Steve Mann, mediawetenschapper Jason Nolan en socioloog Barry Wellman behandelen ook het panopticon in de huidige maatschappij, ze hebben het over 'neo-panopticons': "*In post-Industrial societies, new communication techniques are exploited by neo- panopticons"* (Mann et al., 2003, p. 335). In deze 'neo-panopticons' is de technologie tussen de observant en geobserveerden gekomen. In eerste instantie zijn de 'subjects of observation' bij surveillance 'subjects of the camera' en in tweede instantie "*subjects are under the potential control of people in positions of authority who are organizational monitors of their behavior"* (Mann et al., 2003, p. 335). De disciplinering wordt dus ten eerste bewerkstelligd door de technologie en daarna pas door de mensen die deze technologie controleren ("*people in positions of authority"*). Mann et al. stellen over de geobserveerden: "*the knowledge that they may be under surveillance may be sufficient to induce obedience to authority"* (Mann et al., 2003, p. 335). Dus net als bij het panopticon van Foucault, kan het neo-panopticon zelf-disciplinerend werken. Later in dit hoofdstuk volgt uitleg over de 'sousveillance' die onder andere Mann et al. beschrijven. Hierin reageert de geobserveerde op de surveillance door als het ware terug te surveilleren.

In een neo-panopticon hebben de mensen achter de camera's meer macht dan de geobserveerden: "*There is a digital divide in the unequal access to these technologies* [bovengenoemde camerasurveillance] *by the general public*" (Mann et al., 2003, p. 335). De technologie vormt het instrument voor het uitoefenen van macht en de mensen achter de camera's zijn beter in staat dit instrument te gebruiken. Dus hoewel er niet één centraal punt van observatie meer is, zoals in het oorspronkelijke panopticon, maar een gedecentraliseerde observatie, zorgen de meerdere observatiepunten in de vorm van camera's en cookies op een computer nog steeds voor een oneerlijke machtsverdeling. Dit aangezien de technologie altijd wordt beheerd door mensen en niet ieder mens dezelfde toegang heeft tot deze technologie en tot de informatie die geregistreerd wordt.

Filosoof en informaticus Jean-Gabriel Ganascia beschrijft dat 'access' een belangrijk punt is in het debat over surveillance en het panopticon: "*The information technologies now make it possible to live in a glass-house, where everything is transparent to everybody. However, for social and psychological reasons, this total transparency is not always desirable. One of the most acute ethical issues today concerns the norms on which an ethical justification of opacity can be based"* (Ganascia, 2007, p. 502). Hij benadrukt dus dat mensen in de huidige maatschappij zichzelf niet meer afschermen, waardoor anderen (waaronder bedrijven) makkelijk toegang vinden tot iemands gegevens. Ganascia schrijft dat de moeilijkheden met de 'opacity' van de maatschappij te maken hebben met het 'catopticon' waarin we op dit moment leven. De huidige maatschappij omschrijft Ganascia als 'modern technological societies' waarin iedereen opnames kan maken van anderen en deze informatie vrijuit kan verspreiden (p. 497). Het 'catopticon' is geïnspireerd door het panopticon maar bevat de belangrijkste waarden van deze 'modern technological societies: *"total transparency of society; fundamental equality, which gives everybody the ability to watch – and consequently to control – everybody else; total communication, which enables everyone to exchange with everyone else"* (Ganascia, 2007, p. 497). Deze waarden zijn tegenovergesteld aan de waarden van het originele panopticon: totale transparantie van de cellen, fundamentele ongelijkheid en isolatie van de gevangenen (Ganascia, 2007, p. 496). Dit 'catopticon' beschrijft Ganascia als het algemene systeem in de huidige maatschappij. Hiernaast kunnen echter nog wel verschillende panopticons bestaan, als een vorm van discipline bestaat in een afgesloten instituut als een gevangenis. Het 'catopticon' bestaat in een cultuur waarin anonimiteit eerder gevreesd wordt dan gezocht en waarin het belangrijker is om als individu aandacht te generen dan om je privacy te bewaken (Ganascia, 2007, p. 492).

Om het panopticon als metafoor voor de huidige informatiemaatschappij te gebruiken, moet het dus op een aantal punten aangepast worden. Er moet ten eerste rekening worden gehouden met de huidige cultuur waarin de waarden van privacy zijn veranderd en anonimiteit niet per se meer gewenst is (Ganascia, 2007). Ten tweede is er de tussenkomst van techniek tussen de observant en de geobserveerden (Mann et al., 2003). Deze techniek zorgt ervoor dat gegevens makkelijk kunnen worden opgeslagen en verspreid kunnen worden. Ten slotte bestaat er geen centraal punt van observatie meer in de huidige cultuur en op het internet (Mann et al., 2003). Belangrijk is de notie van het 'participatory panopticon' waarin de geobserveerde vrijwillig aan 'self-surveillance' doet (Campbell en Carlson, 2002). De geobserveerde heeft hierin, ten onrechte, het gevoel in het Catopticon (Ganascia, 2007) te verkeren waarin geen sprake is van machsrelaties. Het internet lijkt open en toegankelijk voor iedereen, maar ik als internetgebruiker kan geen cookies plaatsen bij een bedrijf, om dit bedrijf te monitoren.

Surveillance of sousveillance?

Bovengenoemde theorieën gaan over de macht die de observeerders uitoefenen over de geobserveerden. Verschillende wetenschappers, zoals Lyon, Ganascia en Mann et al., hebben echter gesteld dat de geobserveerden ook terug kunnen observeren in de huidige maatschappij. Zo kunnen zij verzet bieden tegen de macht van de observeerders.

Volgens Mann et al. kan men verzet bieden tegen de macht van organisaties als het op surveillance aankomt: "*One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in authority. We call this inverse panopticon "sousveillance" from the French words for "sous" (below) and "veiller" to watch*" (Mann et al., 2003, p. 332). Dus als individuen de surveillerende partijen gaan observeren, is sprake van 'sousveillance' of 'reflectionism' (Mann et al., 332). Hierdoor wordt volgens Mann et al. de surveillance geneutraliseerd en de gelijkheid tussen beide partijen vergroot (Mann et al., 2003, p. 333). 'Sousveillance' heeft veel gelijkenissen met 'inversed panopticism' dat Elmer als voorbeeld van moderne interpretatie van het panopticon geeft. Beiden gaan over het 'terugkijken' van de geobserveerden, waardoor de surveillance wordt omgekeerd. Alleen gaat 'inversed panopticism' meer over 'spectatorship' waarin de massa, als in een soort fancultuur, een paar mensen in de gaten houdt. Hierbij gaat het niet over het opheffen of veranderen van machtsrelaties en bij 'sousveillance' wel. De theorie van 'sousveillance' is meer van nut voor dit onderzoek dan 'inversed panopticism', aangezien het controleren van privacy wel te maken heeft met machtsrelaties.

'Sousveillance' wordt mogelijk gemaakt door 'wearable computing devices' waarmee individuen data kunnen verzamelen over de 'watchers' door ze bijvoorbeeld te filmen of te fotograferen. Daarnaast schrijven Mann et al., over de 'gaze', oftewel de blik, waarmee men constant in de gaten wordt gehouden (Mann et al., 2003, p. 336). Foucault schrijft ook over de 'gaze' die bij hem uitgevoerd wordt door onder andere bewakers en militaire leiders (Foucault, 1977, p. 1). Door 'sousveillance' kan men de 'gaze' omkeren en een spiegel voorhouden aan de maatschappij met als doel het bereiken van een eerlijkere machtsverdeling en sociaal engagement (Mann et al., 2003, p. 336-347).

Ganascia gebruikt de uitleg van 'sousveillance' van Mann et al. om de overgang van 'surveillance societies' naar de 'sousveillance society' toe te lichten: "*Local surveillance societies, which dominated the 19th and the 20th centuries, have now been replaced by a generalized sousveillance society which reaches incredible proportions, since it not only covers a region, a country or a continent, even the whole world, but also the world of*

'inforgs'[3]*"* (Ganascia, 2007, p. 496). Hoewel Ganascia in dit citaat argumenteert dat de 'surveillance societies' zijn vervangen door een 'sousveillance society', stelt hij dat surveillance en 'sousveillance' naast elkaar bestaan. De huidige maatschappij kan dus als een 'sousveillance society' worden bestempeld, maar surveillance bestaat hierin nog wel. Volgens Ganascia vormen ze nu een soort evenwicht waarin macht eerlijker verdeeld is dan in de eerdere 'surveillance societies' (Ganascia, 2007, p. 491).

Ganascia beschrijft de 'surveillance societies' op dezelfde manier als Foucault de 'disciplinary societies' beschrijft: gecentraliseerd en geïnstitutionaliseerd. De 'sousveillance society' doet meer denken aan de 'control societies' van Deleuze, waarin de computer en toenemende informatietechnologieën een belangrijke rol spelen en de macht gedecentraliseerd is. 'Control societies' hebben echter geen functie als 'bevrijding' van de 'disciplinary societies', en bieden geen verzet tegen de machtsrelaties in een maatschappij waarin surveillance een belangrijke rol speelt. Dus hoewel er overeenkomsten te vinden zijn tussen de 'sousveillance society' en de 'control societies' is er ook één belangrijk verschil: De surveillance in 'control societies' gaat maar één kant op, bedrijven observeren de consument oftewel internetgebruiker. Bij de 'sousveillance society' gaat het juist om het bereiken van een eerlijkere machtsverdeling.

Om de situatie van surveillance in de huidige maatschappij echt accuraat te duiden, moet ook naar het gedrag van de internetgebruiker zelf worden gekeken. De internetgebruiker ondergaat de surveillance, maar is er volgens Campbell en Carlson grotendeels zelf verantwoordelijk voor dat hij geobserveerd wordt. Ze noemen dit 'self-surveillance' (2002, p. 588). De internetgebruiker werkt dus mee aan zijn eigen surveillance. Net zoals bij het gebruik van cookies; de internetgebruiker staat toe dat websites cookies plaatsen op zijn computer die surveillance uitoefenen. Hoewel de consumenten waar Campbell en Carlson over schrijven vrijwillig participeren aan de surveillance die door corporaties wordt uitgevoerd, stellen ze dat de consumenten niet op de hoogte zijn van waaraan ze precies participeren, er is geen sprake van 'informed consent' (Campbell en Carlson, 2002, p. 593). Volgens Campbell en Carlson is er ook geen evenwicht in de machtsverdeling, de corporaties beheren het 'participatory Panopticon' onder het mom van vrijwillige participatie door consumenten. Ook mediawetenschapper Richard Rogers schrijft dat "*according to surveillance theory after Foucault, consumers are enticed into participating in being watched in exchange for product, as Mark Poster and Greg Elmer write. Participatory surveillance describes how the consumer must leave traces and thereby becomes subject to dataveillance, as Roger Clarke has termed it*" (Rogers, 2008, p. 2; Clarke, 1988). Voor de consument bestaat de 'sousveillance society' dus nog niet, hij wordt gelokt om te participeren aan de 'surveillance society'. Rogers verwijst naar Elmer als hij uitlegt dat het uitzetten van cookies ook geen oplossing is om los te komen van deze manier van consumentisme aangezien het internet dan veel minder toegankelijk wordt. Elk cookie apart accepteren werpt ook veel blokkades op, dus "*eventually one yields back to the default setting* [van de browser]*, and carries on with "whatever""* (Rogers, 2008, p. 2).

Protocol

Mediawetenschapper Alexander Galloway kijkt met zijn theorie over protocol nog op een andere manier naar hoe internetgebruikers handelen. Een protocol legt hij uit als "*any type of correct or proper behavior within a specific system of conventions*" (Galloway, 2004, p. 7) en *"a technique for achieving voluntary regulation within a contingent environment"*

[3] 'Inforgs', oftewel 'informational organisms', zijn virtuele tussenpersonen zoals avatars (Ganascia, 2007, p. 495-496).

(Galloway, 2004, p. 7). Protocol werkt dus disciplinerend terwijl de internetgebruiker het gevoel heeft vrijwillig te handelen. Galloway schrijft specifiek over het protocol met betrekking tot technologie, dit protocol bevindt zich in een gedistribueerd netwerk:

> *I argue […] that protocol is how technological control exists after decentralization. The "after" in my title refers to both the historical moment after decentralization has come into existence, but also—and more important—the historical phase after decentralization, that is, after it is dead and gone, replaced as the supreme social management style by the diagram of distribution* (Galloway, 2004, p. 8).

Protocol omschrijft hij dus als een 'management style' van technologische controle. Hij noemt dit een 'computer protocol' waarmee hij aanduidt hoe *"specific technologies are agreed to, adopted, implemented, and ultimately used by people around the world. What was once a question of consideration and sense is now a question of logic and physics"* (Galloway, 2004, p. 7). Een voorbeeld is het gebruik van Google als zoekmachine. Als een internetgebruiker iets wilt vinden op het internet zal hij dit 'googlen'. Dit is de meest gebruikelijke manier geworden om snel informatie te vinden. Hij volgt dus het protocol dat is ontstaan en accepteert daarbij dat Google bijvoorbeeld zijn zoekinformatie opslaat. Ondanks dat het in eerste instantie geen gecontroleerde omgeving lijkt, reguleert Google toch op een bepaalde manier de weg die afgelegd wordt.

Galloway beargumenteert dat protocol bij Deleuze's 'control societies' past als het panopticon bij zijn 'disciplinary societies' (Galloway, 2004, p. 13). Protocol beïnvloedt ook het gedrag van mensen, net zoals het panopticon, maar doet dit op een meer democratische wijze. Het gaat uit van bepaalde conventies en verwachtingen waaraan men voldoet op het internet. Protocol bestaat uit ongeschreven regels die mensen volgen omdat het de makkelijkste weg is. De sociale uitleg van protocol lijkt op de 'panoptic surveillance' van Elmer, waarover hij stelt dat de efficiëntie van het systeem onderdeel is van de werking ervan (Elmer, 2003, p. 233). Protocol gaat ook over de meest efficiënte weg in een technologische omgeving. Galloway benadrukt dat protocol niet omzeild moet worden, maar dat "*it is through protocol that one must guide one's efforts"* (Galloway, 2004, p. 17).

Er kan gesteld worden dat de manier waarop cookies worden ingezet op het internet onderdeel is van het protocol, het systeem van het internet zoals het nu werkt kan niet los gezien worden van het gebruik van cookies. De internetgebruiker volgt welwillend het pad dat voor hem uitgestippeld is door de cookies te accepteren en geen verzet te bieden tegen het opslaan van persoonlijke informatie waardoor hij moeiteloos gebruik kan maken van het internet. Als de internetgebruiker dus niet kritisch nadenkt over dit pad en over de gevolgen van deze vrijwillige disciplinering, kan hij ook geen controle hebben over het gebruik van zijn persoonlijke gegevens.

De maatschappij waarin we nu leven wordt dus getypeerd door een decentrale surveillance waarin het individu weliswaar 'terug kan kijken' ('sousveillance'), maar toch een consument blijft waarover 'dataveillance' (Clarke, 1988) wordt uitgeoefend. Daarnaast is er sprake van één vorm van een 'surveillance society' en niet van meerdere 'societies', zoals Foucault en Deleuze deze beschreven. Dit komt doordat we leven in een maatschappij die bestaat uit een gedistribueerd netwerk en niet uit verschillende losstaande instituten van controle. De technologie en vooral het internet hebben hierin een belangrijke rol gespeeld. Macht lijkt eerlijker verdeeld door gedecentraliseerde macht van bedrijven, maar de huidige 'control society' (Deleuze, 1992) is alsnog meer een 'surveillance society' dan een 'sousveillance society' (Mann et al., 2003; Ganascia, 2007), er is geen evenwicht. Doordat de internetgebruiker niet volledig op de hoogte is van de informatie die over hem verzameld wordt en ook niet dezelfde toegang heeft tot dergelijke informatie, leven we nog steeds in

een maatschappij waarin surveillance 'sousveillance' overheerst. Dus hoewel de maatschappij kenmerken vertoont van de boven omschreven 'sousveillance', het 'catopticon' (Ganascia, 2007) en 'inversed panopticism' (Elmer, 2003), blijft het een 'control society' (Deleuze, 1992) waarin bedrijven macht uitvoeren over consumenten. Deze consumenten, oftewel internetgebruikers, werken hier zelf aan mee door middel van 'self-surveillance' (Campbell en Carlson, 2002). Door onwetendheid participeren ze zonder tegenstribbeling aan hun eigen verlies van controle over privacy door het protocol (Galloway, 2004) te volgen.

Hoofdstuk 2: De context van privacy

In het vorige hoofdstuk kwam naar voren dat surveillance in de huidige maatschappij nog zeer aanwezig is als het gaat om het verzamelen van gegevens over internetgebruikers, in dit hoofdstuk zal de volgende stap genomen worden. Namelijk de invloed op de privacy door surveillance en de controle die over de privacy genomen kan worden. Om uit te leggen in hoeverre privacy gecontroleerd kan worden, moet eerst duidelijkheid worden gegeven over wat privacy betekent en inhoudt. Het begrip privacy is moeilijk te definiëren, zoals in de inleiding al is geschreven. In dit onderzoek beschouw ik de privacy die te maken heeft met het gebruik van cookies als informationele privacy, dus in hoeverre een individu controle kan hebben over zijn gegevens (Bélanger en Crossler, 2011). Door privacy vanuit de context van een situatie te bekijken (Nissenbaum, 2004) zal ik een zwart-wit onderscheid tussen publiek en privé verwerpen (Solove, 2007) en het verschil tussen 'perceived context' en 'complete context' in acht nemen (Pierson en Heyman, 2011).

Privacy?

Onder andere de filosoof James Rachels schrijft over privacy als een gevoel en hoe de inbreuk op privacy een gevoelsmatige kwestie is (Rachels, 1975, p. 325). Anderen, zoals rechtsgeleerde Daniel Solove, schrijven over privacy als een recht (Solove, "Understanding Privacy", 2008, p. 3). Vaak wordt een onderscheid gemaakt tussen privacy in het algemeen of fysieke privacy en informationele privacy, waarbij informationele privacy gaat over privacy met betrekking tot de data die over iemand bekend zijn. In dit onderzoek zal ik privacy benaderen als informationele privacy. Communicatiewetenschapper France Bélanger en informatiewetenschapper Robert E. Crossler beschrijven 'information privacy' als "*the desire of individuals to control or have some influence over data about themselves*" (Bélanger en Crossler, 2011, p. 1017). De privacybescherming van persoonlijke gegevens wordt steeds belangrijker, aangezien de participatie in de huidige maatschappij niet meer los te zien valt van het delen van persoonlijke gegevens. Daarnaast worden de opslagmogelijkheden van die gegevens steeds geavanceerder. Dit schrijft informaticus James Waldo naar aanleiding van de snelle technologische veranderingen die hij ziet in de maatschappij. "*The hardware underlying information technology has become vastly more powerful; advances in processor speed, memory sizes, disk storage capacity, and networking bandwidth allow data to be collected, stored, and analyzed in ways that were barely imaginable a decade ago*" (Waldo et al., 2010, p. 6). Ook filosoof Anton Vedder heeft geschreven over de huidige verwachtingen en betekenis van privacy. Hij beargumenteert dat privacy in de huidige cultuur gaat over de bescherming van gegevens, maar dat veel mensen echter onwetend zijn als het gaat om het verzamelen, opslaan en bewerken van hun persoonlijke gegevens (Vedder, 2009, p. 8-9). Hij schrijft dat de technologieën voor het opslaan van gegevens steeds geavanceerder worden. Het gevolg hiervan is dat de 'informatiehuishouding' van een individu te complex wordt om door hemzelf gecontroleerd te worden (Vedder, 2009, p. 15). Solove legt uit dat verschillende auteurs door deze toenemende technologieën het einde van privacy hebben aangekondigd. "Generation Google" zou het tevens niet meer uitmaken dat hun persoonlijke gegevens op straat liggen en privacy zou niet meer bij de internetcultuur passen (Solove, "End of Privacy, 2008, p. 102-103). Solove is echter van mening dat privacy nog wel een belangrijke rol speelt in de maatschappij. Om controle te kunnen houden over privacy en de privacy ook wetmatig te kunnen beschermen, is het nodig om het onderscheid tussen privé en publiek te verduidelijken (Solove, "End of Privacy", 2008, p. 106).

Publiek en privé

Als rechtsgeleerde bekijkt Solove privacy vanuit de wetgeving in de Verenigde Staten*: "According to the prevailing view of the law, if you're in public, you're exposing what you're doing to others, and it can't be private. If you really want privacy, you must take refuge in your home"* (Solove, 2007, p. 163). Privacy wordt in de wet dus uitgelegd op een binaire manier, iets is ofwel publiek ofwel privé. Solove pleit voor een benadering van privacy waarin privé en publiek niet recht tegenover elkaar staan maar ook in elkaar kunnen overlopen, Solove noemt dit de "*twilight between public and private*" (Solove, 2007, p. 166). Hij beargumenteert dat veel van het dagelijks leven zich in dit 'twilight' afspeelt. De publieke privacy van mensen moet dus ook beschermd worden, dit heeft volgens Solove veel te maken met de toegankelijkheid van informatie. Als voorbeeld geeft Solove de klachten die werden geuit naar aanleiding van de 'News Feed' van Facebook. Op deze 'News Feed' werd persoonlijke informatie van Facebookleden zichtbaar. Deze informatie hadden de leden van te voren al staan op hun profiel, maar doordat de toegankelijkheid ('accessibility') van de informatie vergrootte, voelden ze zich toch aangetast in hun privacy (Solove, "End of Privacy", 2008, p. 104).

Het verschil tussen privé-informatie en publieke informatie wordt door Solove als volgt uitgelegd:

> *Information should be considered private if it remains within a confined group—even if that group is rather large. Once it has traversed too many social circles, then it is no longer private. But if the information is confined in a particular social circle, and a person takes it beyond these boundaries, that's when the law should assign liability—to the person who crossed the boundary* (Solove, 2007, p. 179).

Dit verschil tussen privé-informatie en publieke informatie heeft te maken met vertrouwelijkheid ('confidentiality') en geheimhouding ('secrecy'). Solove benadrukt dat er een belangrijk verschil bestaat tussen deze twee termen. Geheimhouding gaat over het verbergen van informatie, vertrouwelijkheid over het delen van informatie met een beperkt aantal mensen. Door deze informatie te delen, wordt men kwetsbaar (Solove, 2007, p. 173). Solove stelt dat de grens tussen wat publieke informatie is en wat vertrouwelijke privé-informatie is, vaak onduidelijk is. Van belang is dat privé-informatie, wanneer het met een groep mensen gedeeld wordt, nog steeds privé kan zijn. Dit is anders dan het in de Amerikaanse wet staat; hierin wordt informatie die op één of andere manier publiek wordt, niet meer als privé gezien (Solove, 2007, p. 163). Solove is dus van mening dat privacykwesties niet zo zwart-wit zijn als de wet voorschrijft. De context van de kwestie moet, volgens hem, bepalender worden om de privacy hierin te bepalen.

Dit soms lastig te maken onderscheid tussen publiek en privé vormt de basis van de moeilijkheden omtrent het gebruik van cookies. Voor de internetgebruiker is het al moeilijk om dit onderscheid te maken op een site als *Facebook*, maar helemaal als cookies zonder dat hij het weet informatie over hem opslaan. De manier waarop de Amerikaanse wet privacy omschrijft, lijkt de internetgebruiker weinig kans te geven om controle uit te voeren over wat er met zijn persoonlijke gegevens gebeurt. Zoals Solove stelt, wordt privé-informatie publiek zodra het wordt gedeeld met anderen, volgens de Amerikaanse wet ("End of Privacy", 2008, p. 104).

Contextual integrity

Om, in navolging van Solove, de grens tussen privé- en publieke informatie minder zwart-wit te maken, moet er naar de context van privacykwesties gekeken worden. Filosofe Helen

Nissenbaum beschrijft de manier waarop de context van privacy de privacykwestie beïnvloedt als 'contextual integrity'.

> *A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which "anything goes." Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation* (Nissenbaum, 2004, p. 119).

De context van een situatie bepaalt of het delen van persoonlijke informatie gepast is en op wat voor manier. Nissenbaum argumenteert dat op elke plaats sprake is van 'informational norms' waaraan men verwacht wordt zich te houden (Nissenbaum, 2004, p. 121). De informatie die iemand deelt met een goede vriend verschilt bijvoorbeeld van de informatie die gedeeld wordt met een vage kennis.

Wetmatig wordt er een onderscheid gemaakt tussen publieke ruimte en privé ruimte, dit is volgens Nissenbaum echter niet voldoende om als algemene regel in acht te worden genomen. De schending van privacy moet volgens haar per situatie beoordeeld worden aan de hand van 'appropriateness', oftewel wat gepast is in een bepaalde situatie (Nissenbaum, 2004, p. 122). *"What matters is not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or flow, respects contextual norms of information flow"* (Nissenbaum, 2004, p. 123). Dit laatste punt is belangrijk aangezien de 'flow' van informatie moeilijk te controleren valt, vooral op internet. Dit is ook het probleem bij het controleren van persoonlijke data. De 'flow' van informatie is vaak onduidelijk voor de internetgebruiker bij het gebruik van cookies. Tracking cookies blijven de informatie die de internetgebruiker achterlaat op internet opslaan voor langere tijd. Daarnaast kunnen bedrijven de informatie doorspelen aan derden, het is dus lastig voor de internetgebruiker om zicht te houden op de 'flow' van informatie en controle over het opgeslagen dataverkeer te kunnen houden. Zo kunnen de 'informational norms' (Nissenbaum, 2004) van een internetgebruiker makkelijk overschreden worden.

Als uitgegaan wordt van het belang van context voor privacyzaken, betekent het dat elke zaak anders is en er dus geen vaste regels kunnen bestaan voor het handhaven van privacy. Dit is de kritiek die mediawetenschapper Simon Dawes onder andere geeft op de 'contextual integrity' theorie van Nissenbaum (die gevolgd wordt door Solove). Doordat Nissenbaum de dichotomie tussen publiek en privé verwerpt, is het lastig om wetten te maken over wat onder privacyschending valt en wat niet. Hierdoor dreigt het gevaar dat privacy juist niet beschermd wordt, volgens Dawes (2011, p. 118). Hoewel Solove erkent dat de context bij privacy belangrijk is, waarschuwt ook hij voor een focus die teveel op de context ligt want die zou onvoldoende mogelijkheden bieden voor het maken van een beleid en nemen van juridische beslissingen ("Understanding Privacy", 2008, p. 48).

Dawes beargumenteert dat Nissenbaum het recht op privacy verkeerd interpreteert: "*The right to privacy is reinterpreted as the right to have our expectations about the flow of personal information met, not the right to exercise control or restrict access"* (Dawes, 2011, p. 117). Dus de focus op de 'flow' van informatie van Nissenbaum beperkt juist de controle over deze informatie. Doordat de 'flow' elke keer anders is, is het onmogelijk om hier een vaste wetgeving voor te maken. Dawes is het wel eens met Nissenbaum dat deze 'flow' belangrijk is voor privacykwesties en dat bij deze kwesties niet alleen naar de privé-informatie moet worden gekeken maar ook naar de manier waarop deze informatie de privacy kan schaden: "*because it is not the nature of the information itself (whether highly personal or not) that is necessarily the issue, but the potential to increase the importance of information (or for data to become knowledge)"* (Dawes, 2011, p. 118).

Hoewel Dawes een goed punt lijkt te maken, heeft hij over het hoofd gezien dat er in 2006 onderzoek is gedaan naar de toepasbaarheid van de 'contextual integrity' theorie van Nissenbaum en hierbij een model om de theorie te gebruiken is gemaakt. Nissenbaum heeft zelf aan dit onderzoek door Adam Barth et al. meegewerkt. Mediawetenschappers Jo Pierson en Rob Heyman verwijzen naar dit onderzoek en beschrijven het model als volgt:

> *A logical system to assess privacy situations in a more abstract way (Barth et al., 2006)* [de abstracte benadering van privacy bij 'contextual integrity' wordt door Barth et al. in een logisch model verwerkt]. *In this logical system agents were able to distinct contexts and roles, but they were also able to see to what contexts the information flowed. This means that the agents in the system are fully aware of their context and therefore capable of controlling their flow of information, which results in full control over their privacy* (Pierson en Heyman, 2011, p. 33).

In dit model is sprake van drie 'agents': "*the one from whom the information flows, the one to whom the information flows, and the one – the information subject – about whom the information is''* (Barth et al. 2006 in Pierson en Heyman, 2011, p. 33). Deze 'agents' gaan alledrie uit van twee soorten normen van waaruit ze de context van de situatie kunnen identificeren: de 'norms of appropriateness' en de 'norms of distribution'. De eerste gaat over wat voor de 'agent' zelf gepast is om aan informatie te delen, de tweede over de verspreiding van de informatie. In het model van Barth et al. zijn de 'agents' dus volledig op de hoogte van de context, hierdoor kunnen ze de 'flow' van informatie controleren. Pierson en Heyman beargumenteren vervolgens dat dit niet het geval is bij online privacy, hier is sprake van een 'complete context' en een 'perceived context'. De 'complete context' is de echte context van een privacykwestie en de 'perceived context' de context die de persoon over wiens privacy het gaat, ervaart (Pierson en Heyman, 2011, p. 33). Hoe meer deze twee contexten overlappen, hoe meer 'empowerment' deze persoon ondervindt. 'Empowerment' leggen Pierson en Heyman uit als het controleren of beheersen van het eigen leven. In relatie met het internet gaat 'empowerment' over de mate waarin de gebruiker zicht heeft op en controle over het sociale landschap waarin hij zich bevindt (Pierson en Heyman, 2011, p. 30-31). Als er meer openheid over de 'complete context' is, heeft de gebruiker dus meer controle over wat er met zijn communicatie-uitingen gebeurt en zo ook over zijn privacy.
Ik zal deze theorie van Pierson en Heyman aanhouden in de rest van het onderzoek aangezien het een fundamenteel probleem bij het gebruik van cookies behandelt: Het verschil in zicht op de context van de 'flow' van informatie door de internetgebruiker en het bedrijf dat een cookie plaatst.

Cookies en privacy

Pierson en Heyman schrijven over de cookies die door social media gebruikt worden: "*the social layer upon web sites relies on cookie technology although this is a much older innovation than social media*" (Pierson en Heyman, 2011, p. 35). Ze argumenteren dat 'personal identifiable information' (PII) het betaalmiddel is om social media te gebruiken, PII definiëren ze als: "*information, which makes it possible to either directly or indirectly identify a person or what kind of data belong to that person*" (Pierson en Heyman, 2011, p. 32). Op deze manier kunnen mensen 'gratis' gebruik maken van onder andere social networking sites. De informatie die ze delen met het idee dat ze relaties onderhouden met hun vrienden wordt door cookies opgeslagen en door adverteerders gebruikt (Pierson en Heyman, 2011, p. 32), de leden van een social networking site worden dus als consumenten behandeld die hun privacy opofferen voor het gratis gebruik van het netwerk. Dit laatste is de mening van rechtsgeleerde Ian D. Mitchell, hij schrijft: "*in order to use the internet for any purpose,*

individuals must sacrifice their right to data privacy in some measure" (Mitchell, 2012, p. 9).

Bij het delen van persoonlijke informatie op internet heerst, naast onwetendheid, de gedachte dat het niet uitmaakt als anderen veel van je weten als je niks te verbergen hebt (Solove, 2011). Solove beargumenteert dat dit op zichzelf al een foute aanname is aangezien privacy niet gaat over "*hiding bad things"* (Solove, 2011, p. 4):

> *The deeper problem with the nothing-to-hide argument is that it myopically views privacy as a form of secrecy. In contrast, understanding privacy as a plurality of related issues demonstrates that the disclosure of bad things is just one among many difficulties caused by government security measures. (…) The harms are bureaucratic ones - indifference, error, abuse, frustration, and lack of transparency and accountability* (Solove, 2011, p. 4).

Hij stelt dat men de keuze moet kunnen maken over wat te delen op internet. Iemand kan deze keuze pas echt bewust maken als de 'perceived context' en de 'complete context' (Pierson en Heyman) volledig overlappen. Zolang de internetgebruiker of de social media gebruiker nog niet helemaal op de hoogte is van de informatie die opgeslagen wordt en mogelijk zelfs doorgespeeld aan derden, kunnen deze contexten niet volledig overlappen en kan de gebruiker dus nooit volledige controle hebben over wat en met wie hij informatie deelt op internet en dus over privacy. Maar hoe meer de contexten overlappen, hoe meer 'empowerment' de internetgebruiker ervaart (Pierson en Heyman, 2011, p. 30-31).

In dit hoofdstuk heb ik privacy voornamelijk als informationele privacy beschreven, omdat dit onderzoek over cookies de beïnvloeding van privacy op dataniveau behandelt. In de rest van het onderzoek zal het ook over informationele privacy gaan als het over privacy gaat. Er is verder gebleken dat er geen vaste scheidingslijn tussen publieke en privé-informatie moet en kan zijn aangezien de 'informational norms' per situatie kunnen verschillen (Nissenbaum, 2004). Het is dus belangrijk om de context van de situatie te bestuderen zodat de 'flow' van informatie goed in beeld gebracht kan worden en de 'norms of appropriateness' en 'norms of distribution' voor beide partijen duidelijk kunnen zijn (Pierson en Heyman, 2011).

Hoofdstuk 3: De Nederlandse cookiewet

In dit hoofdstuk zal het Nederlandse cookiebeleid worden gebruikt als voorbeeld van vooruitgang als het gaat om controle over persoonsgegevens. Met behulp van onder andere het TNO-rapport van Linda Kool et al., informatie over cookies van OPTA (Onafhankelijke Post en Telecom Autoriteit) en krantenartikelen zullen de stappen voorafgaand aan de invoering van het beleid en na de invoering beschreven worden. Deze zullen duidelijk maken dat, hoewel de Nederlandse cookiewetgeving verre van perfect is, het een goed begin maakt aan het reguleren van het cookiegebruik. Doordat in dit hoofdstuk zowel bronnen van voor de implementatie van de cookiewet als erna zijn geanalyseerd, biedt het een duidelijk inzicht in wat de veranderingen op beleidsniveau kunnen betekenen voor de controle over privacy van burgers.

De kritische discoursanalyse die uitgevoerd wordt in dit hoofdstuk schept een beeld van de invloed van de cookiewet op verschillende partijen. Duidelijk wordt dat vanuit de politiek geworsteld wordt met de bescherming van de privacy tegenover de economische groei en innovatiemogelijkheden op het internet. De internetgebruiker is bezorgd over zijn privacy, maar nog meer over het gebruiksgemak van het internet. De terugkoppeling naar het voorafgaande theoretisch kader verheldert deze sociale categoriseringen vanuit de theorie. De werkelijkheid die de internetgebruiker construeert als het gaat om cookies, verandert vaak van de werkelijkheid die bedrijven construeren. Hiermee duid ik op het eerder behandelde verschil tussen 'perceived context' en 'complete context' (Pierson en Heyman, 2011). Ook wordt er opnieuw ingegaan op de theorie over disciplinering en controle uit het eerste hoofdstuk. Het wordt duidelijk dat er in de 'control society' (Deleuze, 1992) sprake is van verschillende categoriseringen van de fenomenen privacy en surveillance door verschillende groepen mensen. Door dit uit te leggen, kan een betere benadering van de controle die over privacy mogelijk is, gemaakt worden.

De Nederlandse cookiewet

Sinds vijf juni 2012 is er een cookiebepaling opgenomen in de Nederlandse Telecommunicatiewet. Artikel 11.7a van deze wet schrijft voor dat een websitebezoeker altijd geïnformeerd moet worden over en toestemming moet geven voor de cookies die een website gebruikt, dit wordt ook wel een opt-in regeling genoemd (*Rijksoverheid,* "Rijksoverheid Cookie Opt-in"). Deze wet sluit aan op de e-Privacyrichtlijn die gehanteerd wordt in Europa. Op dit moment maken Nederlandse websites gebruik van pop-up vensters om deze toestemming te vragen. In deze pop-up vensters staat meestal een link naar een uitgebreide uitleg van het cookiegebruik door de betreffende website. Sommige websites zijn pas toegankelijk na het accepteren van de cookies.

Vanaf 1 januari 2013 is het amendement van Van Bemmel toegevoegd aan artikel 11.7a van de Telecommunicatiewet waarin is bepaald dat tracking cookies persoonsgegevens opslaan. Hierbij wordt zelfs een IP adres als persoonsgegeven gezien (Doodewaerd en Bulkema, 2012, p. 7). Omdat dit soort cookies met privacy te maken hebben, moet de plaatser van de tracking cookies zich houden aan de Wet bescherming persoonsgegevens. Volgens deze wet mogen "*persoonsgegevens slechts worden verwerkt indien de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend.*"[4] Dit is de belangrijkste reden voor de huidige pop-up vensters waarin toestemming wordt gevraagd voor het gebruik van cookies.

Deze regeling krijgt echter veel kritiek te verduren, geleverd door zowel internetgebruikers als bedrijven. De pop-ups worden als een belemmering gezien voor het

[4] Wet bescherming persoonsgegevens, artikel 8a.

gebruiksgemak van het internet. Websitebezoekers klagen over de hinder die ze ondervinden door de vensters en websitebeheerders over de onduidelijkheid rondom de cookiewetgeving (*Volkskrant,* 14 februari 2013). Zelfs CDA kamerlid Mona Keijzer zegt op 15 februari 2013 in de Volkskrant dat het constante aanklikken van pop-ups 'idioterie' is en dat de pop-ups volgens haar nooit werkelijk gelezen worden. Als de interviewer vervolgens vraagt of ze privacy dan niet belangrijk vindt, antwoordt ze: "*Ja, zeker belangrijk, maar dat vind ik bij dit soort onderwerpen niet zo interessant"* (*Volkskrant,* 15 februari 2013). Dit toont onwetendheid aan betreffende het gebruik van cookies. Deze onwetendheid kan onder andere worden veroorzaakt door het positieve beeld dat veel websites van cookies schetsen. Facebook heeft bijvoorbeeld bij zijn uitleg over cookies staan: "*Cookies en andere, vergelijkbare technologieën dragen bij aan een betere, snellere en veiligere ervaring"* (*Facebook,* "Cookies, pixels en vergelijkbare technologieën"). Maar maken cookies het internet echt veiliger? Staat het belang van de internetgebruiker voorop of die van bedrijven?

De Persgroep was één van de partijen die actie ondernam tegen het beleid. Op alle sites van de Persgroep (van de Volkskrant, de Trouw, het AD en het Parool) werd op vijftien februari 2013 de cookiemuur, waar explicite toestemming werd gevraagd aan de gebruiker, vervangen door een informatiestrook (*Volkskrant,* 15 februari 2013). Hiermee speelde de Persgroep in op de uitspraak van minister Kamp van Economische Zaken van dertien februari 2013 over het versoepelen van het cookiebeleid (*NRC,* 13 februari 2013). De pop-up vensters zijn inmiddels alweer gedeeltelijk verdwenen van Nederlandse websites en op de site van de Rijksoverheid staat dat er momenteel wordt nagedacht over een versoepeling van de cookiewet waarbij geen toestemming hoeft te worden gevraagd voor het plaatsen van cookies die de privacy niet schaden, zoals analytische cookies (*Rijksoverheid,* "Internetbezoek volgen met cookies"). In een brief van minister Kamp aan de Tweede Kamer wordt bekend gemaakt dat 20 mei 2013 begonnen zal worden met de openbare consultatie van het vernieuwde wetsvoorstel. In dit voorgestelde wetsvoorstel staat dat analytische cookies, functionele cookies en andere cookies die "*geen of slechts geringe gevolgen hebben voor de privacy van de internetgebruiker*" gedoogd moeten worden (Brief 'Consultatie cookiebepaling', 20 mei 2013, p. 1). Over dit soort cookies hoeft de internetter niet geïnformeerd te worden en hij hoeft er geen toestemming voor te geven. Wat minister Kamp verstaat onder 'geringe gevolgen voor de privacy' wordt niet uitgelegd.

Op 24 mei 2013 verzond minister Kamp opnieuw een brief naar de tweede kamer over de kabinetsvisie op e-privacy en de stappen die ondernomen moeten worden voor een beter internationaal beleid hiervoor: *"Het kabinet gaat een gerechtvaardig digitaal vertrouwen bevorderen en daarmee een impuls geven aan economische groei"* (Brief "Kabinetsvisie op e-privacy", 24 mei 2013, p. 16). De balans tussen het beschermen van persoonsgegevens en het behouden van ruimte voor innovatie en economische ontwikkeling vormt het kernpunt van de brief. Om deze balans goed te houden is meer 'digitaal vertrouwen' nodig bij de burger. Dit vertrouwen kan vergaard worden door de zogenaamde informatieassymetrie weg te werken (p. 2). Dit komt neer op hetzelfde als de privacy context theorie van Pierson en Heyman. Hoe meer de 'perceived context' (wat de gebruiker ziet als de context van de situatie) overlapt met de 'complete context' (de echte, volledige context), hoe meer vertrouwen de burger kan hebben in digitale diensten. Uit het 'Eurobarometer onderzoek' uit 2011, een onderzoek van de Europese Commissie onder eindgebruikers in de EU-lidstaten, blijkt dat er bij internetgebruikers veel twijfel speelt als het gaat om de bescherming van persoonsgegevens en de persoonlijke levenssfeer (Brief 'Kabinetsvisie op e-privacy, 24 mei 2013, p. 2). Hoewel bedrijven wettelijk verplicht zijn de internetgebruiker te informeren over het gebruik van persoonsgegevens, is de informatie die wordt gegeven veelal ingewikkeld en onbegrijpelijk voor de gemiddelde gebruiker (p. 2).

In de brief worden drie randvoorwaarden gepresenteerd waardoor de gebruiker meer controle kan krijgen over zijn gegevens: Het moet voor gebruikers mogelijk zijn om controle te hebben over hun persoonsgegevens, er moet transparantie zijn betreffende de verzameling en verwerking van gegevens en bedrijven moeten hun verantwoordelijkheid voor een correcte verwerking van persoonsgegevens dragen (Brief "Kabinetsvisie op e-privacy", 24 mei 2013, p. 3). Bij de randvoorwaarde over controle wordt specifiek genoemd dat de eindgebruiker het recht moet krijgen om vergeten te worden en het recht van dataportabiliteit (het verplaatsen en meenemen van data naar bijvoorbeeld een ander platform of andere aanbieder) (p. 3).

Bovenstaande kabinetsvisie lijkt zeer veel op de 'Consumer Privacy Bill of Rights' van de Verenigde Staten. Ian Mitchell noemt dit adviesdocument dat in februari 2012 door de regering van president Obama werd uitgebracht. De volledige naam ervan is: "*Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*" (Mitchell, 2012, p. 7). De titel van het document illustreert de tegenovergestelde belangen van de burger en de bedrijven. De benadering van het cookiebeleid vanuit het Nederlandse kabinet is ook gericht op economie en innovatie. Minister Kamp benadrukt dat met behulp van een digitaal vertrouwen de economische groei bevorderd kan worden. Het gebruik van cookies is dé manier waarop adverteerders veel inkomsten kunnen vergaren, er kan dus beweerd worden dat minister Kamp ervan uitgaat dat een groter digitaal vertrouwen internetgebruikers er niet van zal weerhouden om de cookies te accepteren. In de brief gaat het weinig over het wel of niet accepteren van cookies, maar meer over de informatievoorziening en de mogelijkheden na het accepteren van de cookies, zoals de dataportabiliteit. Aan de juistheid van het systeem van het verzamelen van persoonlijke informatie met behulp van cookies wordt niet getwijfeld. Voor de controle over privacy door een internetgebruiker biedt deze brief wel enigszins een vooruitgang. Als de internetgebruiker het recht om vergeten te worden en het recht op dataportabiliteit krijgt, worden hem wederom een paar handvatten aangereikt om controle te behouden over zijn informationele privacy. Ook lijkt het mij goed als bedrijven meer verantwoordelijkheid krijgen voor het correcte gebruik van cookies. Bedrijven zijn ten slotte de surveillerende partijen, oftewel de observeerders, in deze zaak.

Voorafgaand aan de cookiewet

Kool et al. hebben voorafgaande aan de verandering in de telecommunicatiewet betreffende de cookiewetgeving (5 juni 2012) een onderzoek verricht in opdracht van OPTA (Onafhankelijke Post en Telecom Autoriteit). Dit onderzoek belicht de toenmalige en nieuwe wetgeving omtrent cookies en de moeilijkheden die de wetgeving met zich meebrengt als het gaat om privacy, behavioural advertising en verschillende soorten cookies. Volgens de nieuwe wetgeving in Europa die ontstaan is door de aanscherping van de e-Privacyrichtlijn moet de internetgebruiker geïnformeerd worden over de cookies die een website gebruikt en deze accepteren (opt-in) voordat hij een website kan bezoeken. Voorheen was dit anders, de website moest wel informatie over de cookies bevatten, maar een opt-out procedure waarbij de gebruiker de keuze kon maken om geen cookies te accepteren, was voldoende (Kool et al., 2011, p. 2-4). Kool et al. stellen verschillende vragen bij deze opt-in procedure. Ze vragen zich af of een eenmalige toestemming van de gebruiker voldoende is, of dat dit periodiek moet gebeuren (p. 21). Daarnaast stippen ze aan dat vaak toestemming zal worden gevraagd voor het plaatsen van cookies terwijl het voor de gebruiker niet volledig duidelijk is welke gegevens worden gebruikt en waarvoor deze gebruikt worden. Ze suggereren hierom het gebruik van een 'tailor-made' benadering waarbij verschillende soorten cookies op verschillende manieren gehandhaafd worden (p. 62).

Bovenstaande argumenten zijn deels opgelost door de implementatie van de cookiewet in Nederland, aangezien elke website nu toestemming moet vragen voor het plaatsen van cookies, terwijl dit voorheen vaak via de browser werd geregeld die geen onderscheid maakte tussen verschillende sites of cookies. Toch is het voor de gebruiker ingewikkeld om op een unieke website, als om toestemming wordt gevraagd voor het gebruik van cookies, onderscheid te maken tussen de verschillende soorten en bijvoorbeeld alleen first-party cookies te accepteren (Kool et al., 2011, p. 46).

Onduidelijkheden in de cookiewet

In het document 'Veelgestelde vragen over de cookieregels' (februari 2013) beantwoordt de OPTA (Onafhankelijke Post en Telecom Autoriteit) verschillende vragen naar aanleiding van de cookiewet in Nederland. De volgende zin in het document is opvallend: "*De cookiebepaling beoogt de gebruiker een keuze te geven ten aanzien van zijn privacy. Als websites gebruikers alleen toegang geven indien alle cookies worden geaccepteerd, wordt de gebruiker juist beperkt in zijn keuze"* (p. 7). Een marktpartij mag een gebruiker de toegang ontzeggen als de cookies niet geaccepteerd worden. Het is voor websitebeheerders lastig en veel werk om een alternatieve site te maken voor gebruikers die geen cookies accepteren, dus vaak is het gevolg inderdaad dat de website niet goed werkt als de cookies niet geaccepteerd worden. Dit laat één van de belangrijke gebreken zien in het huidige cookiebeleid: Een gebruiker geeft al snel niet meer om zijn privacy als hierdoor websites niet meer goed werken. De keuze om geen cookies te accepteren, betekent de keuze voor niet geheel functionerende webpagina's.

Een ander opmerkelijk punt is dat de cookiewetgeving geldt voor alle websites, in alle talen en voor alle domeinen, volgens OPTA ("Veelgestelde vragen", p. 3). Dit maakt de situatie voor OPTA zo dat ze nooit volledige zicht kunnen hebben op de uitvoering van het cookiebeleid en dat het eigenlijk oncontroleerbaar is. De OPTA schrijft in het document ook dat zij voorstander zouden zijn van een "Do Not Track" systeem waarin de browser de mogelijkheid geeft aan de gebruiker om ervoor te kiezen niet gevolgd te worden. Dit systeem is op dit moment nog niet voldoende ontwikkeld om in werking te treden, maar de OPTA houdt de ontwikkelingen in de gaten (p. 9).

Ook de Nederlandse organisatie *Bits of Freedom*, die digitale burgerrechten verdedigt, levert kritiek op het cookiebeleid. Zij pleiten onder andere voor een betere definitie van het begrip 'persoonsgegevens'. Als niet duidelijk is wat hier onder valt, is het niet duidelijk welke cookies verkeerd omgaan met persoonsgegevens. *Bits of Freedom* vindt dat alle gegevens die online worden achtergelaten onder persoonsgegevens vallen (*Bits of Freedom,* "Privacy en persoonlijke data"). Het vernieuwde cookiebeleid van minister Kamp waarin bepaalde soorten cookies wel worden gedoogd en anderen niet kan dus, zoals Bits of Freedom het uitlegt, nooit volledig de persoonsgegevens van internetgebruikers beschermen. Een ander belangrijk punt dat *Bits of Freedom* maakt, is dat de informatie die verstrekt wordt aan internetgebruikers in duidelijke, begrijpelijke taal moet zijn. Alleen dan kan de toestemming die de internetter geeft echt zijn.

Deze kritiek op het Nederlandse beleid laat zien dat er nog veel onduidelijkheden zijn in het beleid. Vooral de rol van de gebruiker en de definitie van persoonsgegevens zijn niet duidelijk. Een tegenstelling binnen het beleid is dat een actieve instelling wordt verwacht van de internetgebruiker als het gaat om het controleren van zijn eigen dataverkeer, maar dat de gemiddelde internetgebruiker hier niet toe in staat is, volgens *Bits of Freedom.* De machtsrelaties in het systeem van surveillance op het internet worden dus wel erkend door de overheid, maar ze reiken de internetgebruiker nog niet genoeg handvatten aan om hun informationele privacy goed te controleren.

Controle over privacy en de Nederlandse cookiewet

De implementatie van de cookiewet in Nederland heeft veel losgemaakt bij zowel internetgebruikers als bedrijven, zoals te zien is in bovengenoemde media-uitingen. Dit heeft het debat rondom informationele privacy en het gebruik van persoonsgegevens nieuw leven ingeblazen. Dit is zeker een gunstige ontwikkeling als het gaat om de mate van bewustheid die gecreëerd wordt bij de gebruiker. Doordat het onderwerp leeft, worden meer mensen bereikt en groeit de interesse. Toch bleek dat internetgebruikers voornamelijk kritiek hadden op de pop-ups en zich meer zorgen maakten over het afnemende gebruiksgemak van het internet dan over hun privacy (*Volkskrant,* 6 februari 2013). Het is de vraag of veel mensen daadwerkelijk de informatie over cookies op sites gelezen hebben, of dat ze zo snel mogelijk de pop-up hebben weggeklikt. Toch geeft dit beleid de gebruiker de mogelijkheid om controle te hebben over wat er met zijn persoonlijke data gebeurt. Het biedt de kans om cookies te weigeren, vaak wel met als gevolg dat de website niet geheel toegankelijk is. Door de zogenaamde 'cookiewall' krijgt de gebruiker wel een beter overzicht van de context van zijn dataverkeer. De 'norms of distribution' (Pierson en Heyman, 2011) moeten nu duidelijk uitgelegd worden door een website. In navolging van Pierson en Heyman, is dus te zeggen dat de 'perceived context' en de 'complete context' meer overlappen waardoor de gebruiker meer 'empowerment' ondervindt (Pierson en Heyman, 2011, p. 33). Doordat de gebruiker beter op de hoogte is van de context, kan hij een meer bewuste keuze maken. Of hij dit ook daadwerkelijk doet, blijft de vraag.

Door de plaatsing van de cookiewall raakt de internetgebruiker in de war over het protocol (Galloway, 2004). Opeens verschijnt een tussenkomst van een pop-up of ten minste een informatiebalk over het gebruik van cookies, voordat de internetgebruiker een site kan openen. De acceptatie van cookies als onderdeel van het internet was onderdeel van het protocol, de internetgebruiker volgde dit gebaande pad. Maar nu de discussie over privacy oplaait en de overheid zich bemoeit met het gebruik van cookies, verandert het protocol. De gebruiker wordt gedwongen om na te denken over zijn privacy, hoewel dat zonder de pop-ups alweer minder noodzakelijk wordt. Door een vernieuwd beleid met betrekking tot cookies kan het technologisch protocol veranderen, een internetgebruiker moest in Nederland aan het begin van 2013 eerst de cookies accepteren om daarna een site te kunnen openen. Ondanks bovenstaande problemen van de internetgebruiker met het nieuwe beleid, zullen toch heel veel internetgebruikers de cookies hebben geaccepteerd zonder tegenstand. Zij hebben zich dus moeiteloos aan het veranderde protocol aangepast. Maar nu de cookiewalls grotendeels zijn verdwenen in Nederland, is het pad dat de internetgebruiker moet afleggen weer aan het veranderen.

Hieruit is op te maken in hoeverre de internetgebruiker nog onderhevig is aan disciplinering door bedrijven en de overheid (en vanuit de technologie die zij gebruiken). Er is dus nog steeds sprake van een 'control society' (Deleuze, 1992). Hoewel er hier en daar protest oplaaide tegen het cookiebeleid, werd de internetgebruiker gedisciplineerd door het vernieuwde protocol en accepteerden de meesten de surveillance die uitgeoefend werd. Dus hoewel de internetgebruiker meer 'empowerment' (Pierson en Heyman, 2011) kan ervaren als hij zich zou verdiepen in de context van de informatie 'flow' (Nissenbaum, 2004), gebeurt dit meestal niet doordat het protocol (Galloway, 2004) gedachteloos gevolgd wordt. Alleen de kritische internetgebruiker kan door het Nederlandse beleid dus aangespoord worden om meer controle over zijn informationele privacy te vergaren. De gemiddelde gebruiker participeert aan de 'self-surveillance' (Campbell en Carlson, 2002), door de cookies te accepteren, zonder het idee te hebben dat zijn controle over privacy hiermee wordt verkleind. Veel internetgebruikers zullen dus het gevoel hebben te participeren aan een vorm van 'catopticon' (Ganascia, 2007) waarin geen sprake is van machtsrelaties of panoptische surveillance. Met panoptische surveillance bedoel ik hier 'panoptic surveillance'

in de uitleg van Elmer, dus een decentrale surveillance in een efficiënt ogend systeem (Elmer, 2003, p. 233). In het Nederlandse cookiebeleid is nog steeds sprake van zo'n vorm van surveillance, ondanks de vorderingen die zijn gemaakt door internetgebruikers de mogelijkheid te geven meer controle over hun informationele privacy te vergaren.

Het Nederlandse cookiebeleid heeft, hoewel het verre van perfect is, een begin gemaakt aan het reguleren van het cookiegebruik op internet. Door de wetgeving kan de Nederlandse burger zijn privacy, als hij dat wil, meer controleren en krijgt de burger meer inzicht in de verwerking van zijn persoonsgegevens. Hoewel het nog zoeken is naar de juiste balans om zowel informationele privacy te beschermen als ruimte te behouden voor economische groei en innovatie, heeft Nederland een goede eerste stap gezet.

Conclusie

Om te bepalen in hoeverre controle over privacy mogelijk is op internet als het gaat om de persoonlijke informatie die websites opslaan met behulp van cookies heb ik eerst naar de surveillance in de huidige maatschappij gekeken. Het bleek dat onze maatschappij nog steeds getypeerd kan worden als een 'control society' (Deleuze, 1992) waarin bepaalde aspecten van de 'disciplinary societies' (Foucault, 1977) nog aanwezig zijn. Dit houdt in dat er in de maatschappij sprake is van een gedistribueerde vorm van surveillance in een decentraal netwerk. De surveillance wordt uitgeoefend door de overheid en door bedrijven.

Het panopticon van Foucault in zijn oorspronkelijke uitleg kan niet als metafoor voor de huidige informatiemaatschappij gebruikt worden. De manier waarop Campbell en Carlson het panopticon gebruiken, geeft wel een goed beeld van de werking van surveillance in onze maatschappij. Zij stellen dat er op internet sprake is van een 'participatory panopticon' waarin de geobserveerde vrijwillig aan 'self-surveillance' doet (Campbell en Carlson, 2002). Door het leveren van 'personal identifiable information' (PII) kunnen mensen gebruik maken van veel 'gratis' internetdiensten (Pierson en Heyman, 2011). Zo werkt het computer protocol voor internetgebruik (Galloway, 2004). De internetgebruiker volgt vrijwillig de meest effiënte weg die geboden wordt, maar wordt ongemerkt toch gedisciplineerd door deze uitgestippelde weg te volgen.

Naast de surveillance die uitgeoefend wordt door bedrijven, heb ik ook gekeken naar de mogelijkheden voor de geobserveerde internetgebruiker om terug te observeren. Hoewel er een beeld bestaat van een van machtsrelaties vrije, transparant internet, blijkt dat de maatschappij niet getypeerd kan worden door termen als het 'catopticon' (Ganascia, 2007), 'sousveillance society' (Mann et al., 2003; Ganascia, 2007) of 'inversed panopticon' (Elmer, 2003). Deze termen duiden het 'terugkijken' van de internetgebruiker aan, waardoor de surveillerende macht van bedrijven teniet zou worden gedaan. Toch is er geen sprake van een evenwicht tussen de 'surveillance society' en de 'sousveillance society' omdat de internetgebruiker niet volledig op de hoogte is van de 'flow' (Nissenbaum, 2004) van zijn persoonlijke informatie op het internet. Zonder deze transparantie kan er geen eerlijkere machtsverdeling tussen bedrijven en consumenten bestaan. Deze informatieassymetrie (Brief "Kabinetsvisie op e-privacy", 2013) kwam ook terug in de analyse van privacytheorie. Privacy, in dit onderzoek uitgelegd als informationele privacy, moet bekeken worden binnen de context van een situatie. Hierin heb ik de 'contextual integrity' theorie van Nissenbaum (2004) gevolgd. De 'informational norms' die gelden, kunnen per situatie verschillen en daarmee wat gepast is wat betreft het delen van informatie in die situatie (Nissenbaum, 2004). Dit is de reden dat een zwart-wit onderscheid tussen publieke informatie en privé-informatie geen basis kan vormen voor een goed privacybeleid.

Het controleren van privacy gaat in dit onderzoek over het controleren van persoonlijke gegevens op internet. In hoofdstuk twee beargumenteer ik dat een internetgebruiker pas echt controle over zijn informationele privacy kan hebben als de 'perceived context' van een privacysituatie met de 'complete context' overlapt (Pierson en Heyman, 2011). Dit houdt in dat de internetgebruiker volledig op de hoogte moet zijn van de 'flow' van informatie, dus wat er met zijn informatie gebeurt en hoe ver het 'reist' op het internet. Als dit zo is, ervaart de internetgebruiker meer 'empowerment' (Pierson en Heyman, 2011) en kan hij, als de technologische mogelijkheden er zijn, controle uitoefenen over zijn privacy.

Ten slotte heb ik een analyse gemaakt van het Nederlandse cookiebeleid waarin bovenstaande privacytheorie bevestigd wordt. In Nederland is een goede eerste stap gezet om de burger meer controle te geven over zijn informationele privacy, maar er is nog veel te doen. De handvatten die de burger in Nederland op dit moment aangereikt zijn, zijn alleen van nut als hij zelf kritisch ingesteld is en actief wil nadenken over zijn informationele

privacy. Daarnaast is de gemiddelde burger nog niet geholpen met het huidige beleid, aangezien de verplichte informatievoorziening vaak in moeilijke taal wordt gegeven en onduidelijk is (*Bits of Freedom).* Aan de internetgebruiker die wel controle wil uitoefenen over in hoeverre cookies zijn data opslaan en gebruiken, wordt nog weinig gedacht: Veel websites functioneren niet goed zonder cookies.

De kwalitatieve literatuurstudie en de kritische discoursanalyse die ik heb gebruikt in dit onderzoek gaven mij de mogelijkheid om de fenomenen privacy en surveillance zowel vanuit de theorie als de praktijk te benaderen. Met de literatuurstudie heb ik een theoretisch kader opgebouwd waarin verschillende theorieën overheersen waarin ik heb beargumenteerd waarom deze tot beantwoording van de hoofdvraag zouden leiden. Zo kon ik de huidige maatschappij duiden als 'control society' (Deleuze, 1992) waarin surveillance nog steeds een belangrijke rol speelt en privacy behandelen als informationele privacy waarbij de context belangrijk is en kan verschillen voor verschillende partijen. De daaropvolgende kritische discoursanalyse maakte het discours rondom de Nederlandse cookiewet inzichtelijk en verduidelijkte hoe de cookiewet voor verschillende partijen, zoals de burger en de overheid, een verschillende betekenis draagt. Door deze verbinding tussen het theoretisch kader en de casestudy te maken, werd de theorie tastbaarder en kon ik een zo accuraat mogelijke benadering van de mogelijke controle over privacy maken.

Andere mogelijke methoden die ik had kunnen gebruiken voor dit onderzoek zouden meer gericht kunnen zijn op de receptie van internetgebruikers. Ik had receptieonderzoek kunnen doen met behulp van een enquête of interviews. Daarnaast had een kwantitatieve onderzoeksmethode van nut kunnen zijn, waarin bijvoorbeeld het gedrag van internetgebruikers met betrekking tot cookies gemeten wordt. Deze methoden hadden een nog duidelijker beeld kunnen geven van de rol van de burger als het gaat om controle over privacy.

Met het Nederlandse cookiebeleid is dus een begin gemaakt aan het geven van controle over privacy aan de Nederlandse internetgebruiker. Toch valt ook de Nederlandse maatschappij nog steeds te typeren als een 'control society' (Deleuze, 1992) waarin de internetgebruiker gedisciplineerd wordt door het protocol (Galloway, 2004). Door zowel internetgebruikers die op de hoogte zijn van de gevolgen voor informationele privacy als diegenen die dat niet zijn, wordt vrijwillig meegedaan aan het 'participatory panopticon' (Campbell en Carlson, 2002). De controle over informationele privacy die internetgebruikers hebben kan dus variëren, maar kan nooit volledig zijn. Hoeveel controle de internetgebruiker binnen het systeem van surveillance kan hebben hangt af van de informatieassymetrie tussen de gebruiker en het bedrijf, de alternatieve mogelijkheden om het internet te gebruiken na invloed uitgeoefend te hebben op het cookiegebruik en de welwillendheid van de internetgebruiker zelf.

Bibliografie

Wetenschappelijke bronnen

Bélanger, France, en Robert E. Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35.4 (2011): 1017-41.

Berg, Harry van den. “Discoursanalyse.” *KWALON* 26.2 (2004): 29-39.

Berg, Harry van den. “Discoursanalyse in de praktijk, de discursieve constructie van sociale categorieën.” *KWALON* 27.3 (2004): 27-34.

Boeije, Hennie. *Analysis in Qualitative Research.* SAGE Publications, 2010.

Campbell, John Edward, and Matt Carlson. "Panopticon.Com: Online Surveillance and the Commodification of Privacy." *Journal of Broadcasting & Electronic Media* 46.4 (2002): 586-606.

Christiansen, Linda. "Personal Privacy and Internet Marketing: An Impossible Conflict or a Marriage Made in Heaven?" *Business Horizons* 54 (2011): 509-14.

Clarke, Roger A. "Information Technology and Dataveillance." *Communications of the ACM* 31.5 (1988): 498-512.

Dawes, Simon. "Privacy and the Public/Private Dichotomy." *Thesis Eleven* 107.1 (2011): 115-24.

Deleuze, Gilles. "Postscript on the Societies of Control." *October* 59 (1992): 3-7.

Elmer, Greg. "A Diagram of Panoptic Surveillance." *New Media & Society* 5.2 (2003): 231-47.

Foucault, Michel. "Panopticism." Trans. Sheridan, Alan. *Discipline & Punish: The Birth of the Prison*. 1995 ed. New York: Vintage Books, 1977.

Galloway, Alexander R. *Protocol, How Control Exists after Decentralization.* Ed. Malina, Roger F. Londen: The MIT Press, 2004.

Ganascia, Jean-Gabriel. "The Generalized Sousveillance Society." *Social Science Information* 49.3 (2010): 489-507.

Gee, James Paul. *Discourse Analysis. Theory and Method.* Routledge, 2010.

Lyon, David. *Surveillance Society*. Rec 28 september 2008. Lezing tijdens Festival del Diritto, Piacenza, Italië.

Mann, Steve, et al. "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." *Surveillance & Society* 1.3 (2003): 331-55.

Mitchell, Ian D. "Third Party Tracking Cookies and Data Privacy." (2012): 1-9.

Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* (2004): 101-39

Pierson, Jo, en Rob Heyman. "Social Media and Cookies: Challenges for Online Privacy." *info* 13.6 (2011): 30-42.

Queiroz, Anderson A.L., en Ruy J. G. B. de Queiroz. "Breach of Internet Privacy through the Use of Cookies." PETRA (2010): 1-5.

Rachels, James. "Why Privacy Is Important." *Philosophy & Public Affairs* 4.4 (1975): 323-33.

Rogers, Richard. "Consumer Technology after Surveillance Technology." *Mind the Screen: Media Concepts According to Thomas Elsaesser*. Amsterdam: Amsterdam University Press, 2008. 288-96.

Solove, Daniel J. "The End of Privacy?" *Scientific American* 299.3 (2008): 101-06.

Solove, Daniel J. *The Future of Reputation. Gossip, Rumor, and Privacy on the Internet*. New Haven en Londen: Yale University Press, 2007.

Solove, Daniel J. *Understanding Privacy*. Harvard University Press, 2008.

Solove, Daniel J. "Why Privacy Matters Even If You Have 'Nothing to Hide'." *The chronicle of higher education* 15 (2011).

Vedder, Anton. "Privacy, een conceptuele articulatie." *Filosofie & Praktijk* 30.5 (2009): 7-19.

Waldo, James et al. "Engaging Privacy and Information Technology in a Digital Age: Executive Summary." *Journal of Privacy and Confidentiality* 2.1 (2010): 5-18.

Overige bronnen

"Cookies, pixels en vergelijkbare technologieën". Facebook. 11 juni 2013 <https://www.facebook.com/help/cookies?ref_type=sitefooter>.

Doodewaerd, Jitty van, en Henk Bulkema. "DDMA Hanleiding Cookiewet. 'Wet en werkelijkheid'." (2013): 1-29.

Dool, Pim van den. "Kamp kijkt of expliciet toestemming geven voor cookies wel nodig is." *NRC Handelsblad* 13 februari 2013.

"Internetbezoek volgen met cookies". 2013. Rijksoverheid. 7 juni 2013. <http://www.rijksoverheid.nl/onderwerpen/ict/veilig-online-en-e-privacy/internetbezoek-volgen-met-cookies>.

Kamp, H. G. J. "Brief kabinetsvisie op e-privacy: op weg naar gerechtvaardigd vertrouwen." Ministerie van Economische Zaken. Den Haag, 24 mei 2013. 1-17.

Kamp, H.G.J. "Consultatie cookiebepaling en de beantwoording van een tweetal vragen." Ministerie van Economische Zaken. Den Haag, 20 mei 2013. 1-7.

Kool, Linda et al. *A Bite Too Big: Dilemma's bij de implementatie van de cookiewet in Nederland*: TNO, 2011.

Kraak, Haro. "Volkskrant.nl verwijdert cookiemuur." *Volkskrant* 15 februari 2013.

"Nieuwsbreak." *Volkskrant* 15 februari 2013.

"Privacy en persoonlijke data. Jouw data, jouw keuzes.". Bits of Freedom. 22-05-2013. <https://www.bof.nl/ons-werk/privacy-en-persoonlijke-data/>.

"Rijksoverheid Cookie Opt-In". Rijksoverheid. 11 juni 2013. <http://www.rijksoverheid.nl/cookies/rijksoverheid-cookie-opt-in>.

“Veelgestelde vragen over de cookieregels”. *OPTA* (onafhankelijke Post en Telecom Autoriteit), 2013.

"Consumentenbond wil andere cookiewet." *Volkskrant* 6 februari 2013.

"Wet bescherming persoonsgegevens." 11 juni 2013. <http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_11-06-2013>.

Wordle. 14 juni 2013. <http://www.wordle.net/>.