Vechten tegen de Bierkaai

Een kwalitatief onderzoek naar reacties op de surveillant assemblage

Rotterdam, juli 2014

Masterscriptie

Justin Klein

jklein@xs4all.nl

Studentnummer: 305359

Erasmus Universiteit Rotterdam

Faculteit der Sociale Wetenschappen

Opleiding Sociologie

Grootstedelijke Vraagstukken & Beleid

Begeleider: dr. D.W.J. Broeders

Tweede lezer: prof. dr. J.L. Uitermark

Vechten tegen de Bierkaai

Een kwalitatief onderzoek naar reacties op de *surveillant assemblage*

Rotterdam, juli 2014

Masterscriptie

Justin Klein

Woord vooraf

Voor u ligt mijn masterscriptie. Enerzijds de spreekwoordelijke kroon op mijn studie sociologie en anderzijds de grootste uitdaging bij het afronden van diezelfde studie. Het feit dat u op dit moment dit woord vooraf leest wil zeggen dat deze uitdaging tot een goed einde is gebracht. Ik ben hiervoor een aantal mensen een dankwoord verschuldigd. Zij hebben mij op allerlei manieren ondersteund bij dit proces en zo een grote bijdrage geleverd aan de totstandkoming van deze scriptie.

Op het sociale vlak wil ik mijn ouders bedanken voor het geduld, het medeleven en het geboden totaalpakket. Mijn zus voor de overlevingspakketten. Tim voor zijn belminuten en alle anderen voor de bemoedigende en motiverende woorden. Voor ieder van hen geldt dat juist op de momenten wanneer het nodig was ik kon rekenen op hun steun.

Op het inhoudelijke vlak wil ik mijn begeleider Dennis Broeders bedanken voor de vele uren die hij vrij heeft gemaakt voor onze bijeenkomsten. Zijn tijd en inzichten zijn van grote waarde geweest bij het opzetten, uitvoeren en afronden van deze scriptie. Daarnaast wil ik mijn respondenten bedanken voor hun medewerking aan mijn onderzoek en de feedback die zij hierop hebben gegeven. Bits of Freedom voor de hulp bij het uitnodigen van mijn respondenten en Justus Uitermark voor het beoordelen van het onderzoeksvoorstel en deze scriptie.

Ik wens eenieder veel plezier bij het lezen van mijn scriptie.

Was getekend,

Justin Klein
3 juli 2014

Inhoudsopgave

Hoofdstuk 1: Surveillant assemblage & maatschappelijke reacties

1.1 Inleiding

Onze hedendaagse samenleving is meer en meer een digitale. Met onze computers en smartphones hebben wij toegang tot wereldwijde netwerken en kunnen wij beschikken over grote hoeveelheden informatie. Naast dat wij in ons dagelijks leven volop gebruik maken van dergelijke informatie en de netwerken waarover die informatie zich verplaatst, produceren wij met onze dagelijkse handelingen ook gegevens die worden verzameld en gebruikt door overheden en bedrijven. Surveillance is volgens Lyon (2001: 2) elke vorm van het verzamelen en verwerken van persoonlijke gegevens met het doel om diegene waarover gegevens verzameld worden te beïnvloeden. Met de komst van het kapitalisme en moderne samenlevingen zijn dergelijke activiteiten in hoge mate gesystematiseerd (Graham & Wood, 2003: 227). Informatie over personen maakt bureaucratische administratie voor overheden mogelijk en geeft bedrijven inzicht in het gedrag van werknemers en consumenten (Lyon: 2003: 162). In de recente geschiedenis is de mate van surveillance enorm toegenomen. Zowel een verlangen naar controle, governance, veiligheid, winst en entertainment (Haggerty & Ericson, 2000: 609) alsmede technologische ontwikkelingen (Graham & Wood, 2003: 228) hebben bijgedragen aan deze toename. Het samenspel van digitale technologieën en governance brengen iedereen tegenwoordig onder een "*shared surveillance umbrella*" (Martin, van Brakel en Bernhard, 2009: 228).

Digitalisering alsmede de opkomst van nieuwe informatietechnologieën zoals het internet hebben de mogelijkheden voor het verzamelen, opslaan en verwerken van persoonlijke informatie sterk doen toenemen. Daarnaast hebben deze ontwikkelingen ervoor gezorgd dat dergelijke processen een intrinsiek deel van ons leven zijn gaan uitmaken (Lyon, 2003: 161-170). Door het samensmelten van informatie- en communicatietechnologieën worden dagelijkse sociale activiteiten op het internet meer en meer gevolgd, en zijn zo een waardevolle bron van informatie geworden om kennis over personen en groepen te vergaren (Bruno, 2012: 343).

Gary Marx (2002: 12) spreekt in dit licht van "*new surveillance"* en Haggerty & Ericson (2000: 619) zien een "*disappearance of disappearance"* waarbij het steeds lastiger is voor personen om hun anonimiteit te bewaren of te ontsnappen aan surveillance door sociale instituties. Haggerty & Ericson beschrijven de hedendaagse samenleving daarom als een "*surveillant assemblage"* (Ibid: 608). Waar surveillance voorheen vooral gericht was op specifieke groepen of personen, zijn tegenwoordig personen in het algemeen steeds vaker onderwerp van surveillance. Surveillance zet volgens Haggerty & Ericson gegevens over het (gedrag van het) menselijk lichaam om in zogenaamde "*data-doubles"* (Haggerty & Ericson, 2000: 613). Deze virtuele representatie van personen wordt vervolgens

in verschillende systemen en settings gebruikt voor zaken als analyses, management en omzetverhoging. Het feit dat de auteurs spreken van een assemblage komt volgens hen voort uit het verlangen en de mogelijkheden om dergelijke praktijken en systemen meer en meer aan elkaar te koppelen. Haggerty & Ericson leggen uit: *"We are only now beginning to appreciate that surveillance is driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole. It is this tendency which allows us to speak of surveillance as an assemblage, with such combinations providing for exponential increases in the degree of surveillance capacity.*" (Haggerty & Ericson, 2000: 610). Belangrijk om hierbij op te merken is het feit dat Haggerty & Ericson niet uitgaan van één Big Brother-achtige actor waar al deze informatie samen komt. De gegevens of "*data-doubles"* bevinden zich in verschillende systemen of databanken van overheden en bedrijven. De mogelijkheden tot het integreren, combineren en coördineren van deze verschillende systemen en componenten van surveillance zorgen echter voor de potentiële assemblage (Haggerty & Ericson, 2005: 4-5).

1.2 Aanleiding voor deze scriptie

De aanleiding voor deze scriptie is het ontstaan van maatschappelijke en wetenschappelijke reacties op de hierboven beschreven samenleving. "*Radical new technologies of surveillance, at the micro-consumer level, the international level and the global level, have triggered serious social (as well as academic) concern over such issues as power, privacy and social management*" (Green, 1999: 27). Binnen elke industriële samenleving is er tegenwoordig minimaal één groepering te vinden die zich inzet voor de bescherming van persoonlijke privacy en een lobby voert tegen intensieve surveillance praktijken (Bennett, 2008). Dergelijke organisaties verzetten zich zo tegen vergaande surveillance. En hoewel er veel wetenschappelijke aandacht is voor ontwikkelingen op het gebied van surveillance is er relatief weinig aandacht "*to the issues of resistance to these technologies.*" (Fernandes & Huey, 2009: 198). Vooral de manieren waarop individuen op nieuwe vormen van surveillance reageren, kunnen volgens Gilliom (2005) verdere wetenschappelijke aandacht gebruiken: "*Research on how people respond to surveillance has touched on things like resistance, litigation, opposition, compliance and apathy, but made relatively little progress in understanding how these dimensions are linked to different contexts, programs, and people.*" (Gilliom, 2005: 128). Met dit onderzoek tracht ik een bijdrage te leveren aan wetenschappelijke kennis over reacties op, en verzet tegen surveillance binnen de context van een surveillant assemblage. Ik richt mij daarbij op personen die zich identificeren met een dergelijke privacy organisatie en wil bekijken of, en hoe zij in het dagelijks leven reageren op deze nieuwe vormen van surveillance. Voor deze scriptie heb ik gesproken met zeventien

personen die zich identificeren[1] met de digitale burgerrechtenbeweging Bits of Freedom. Deze lobby beweging komt op voor digitale burgerrechten en verdedigt de online privacy en vrijheid van burgers[2]. Bits of Freedom kan zo gezien worden als een collectieve maatschappelijke reactie op de surveillant assemblage. Ik ben in deze scriptie echter geïnteresseerd in de meer individuele reacties op de surveillant assemblage in het dagelijks leven van personen. Welke probleemstelling ik daarvoor in deze scriptie tracht te beantwoorden wordt hieronder beschreven.

1.3 Probleemstelling

Een belangrijk kenmerk van de door Haggerty & Ericson (2000) beschreven surveillant assemblage is de veelheid aan systemen en componenten die tezamen de potentiële assemblage vormen. Voorbeelden van dergelijke componenten zijn databanken van overheden, bedrijven en organisaties. Echter bestaat de assemblage niet alleen uit dergelijke databanken. In een wereld waarin informatietechnologieën meer en meer ons dagelijks leven structureren zijn personen afhankelijk van het gebruik van hun persoonlijke gegevens *"to consume, acces things and generally act within society.*" (Green, 1999: 33). Steeds meer handelingen produceren zo digitale gegevens die opgeslagen en gemanipuleerd kunnen worden (Mulgan, 1991: 71). Of het nu gaat om pin-transacties, reisgegevens van de ov-chipkaart, klantenkaarten van winkels of de vele verbindingen die mobiele telefoons de hele dag door maken, al dit soort gegevens dragen bij aan de potentiële assemblage. Ook op het internet worden de handelingen van personen continu gevolgd en worden gegevens gebruikt voor het opstellen van profielen, het ontdekken van patronen en het voorspellen van toekomstige handelingen (Hope, 2005: 363). Zowel in het offline als online leven worden personen tegenwoordig dus "*continuously and constantly watched, monitored and documented.*" (Rapoport, 2012: 320). In dit onderzoek naar de reacties van personen op een samenleving waarin surveillance een dergelijk belangrijke en alomvattende rol inneemt, is het daarom van belang te bekijken wat precies de problemen zijn die personen ervaren. De zorgen van personen over de surveillant assemblage maken daarom het eerste deel uit van mijn probleemstelling.

Naast de zorgen die personen ervaren richt ik mij in dit onderzoek op de manier waarop zij reageren op de beschreven surveillant assemblage. Volgens Bennett (2012) zijn er drie soorten reacties op surveillance te onderscheiden. Ten eerste zijn er institutionele reacties die zich voornamelijk richten op privacy en de bescherming van persoonsgegevens binnen wetgeving. Ten tweede zijn er individuele reacties waarbij personen strategieën van verzet hanteren. Ten derde zijn er collectieve reacties zoals lobbybewegingen of sociale bewegingen die zich richten op collectieve actie (Bennett,

[1] In paragraaf 3.2 staat beschreven dat het identificeren met Bits of Freedom bestaat uit het publiekelijk, of naar eigen zeggen fan zijn van de organisatie.
[2] www.bof.nl.

2012: 412). Volgens Marx (2003: 387) richten collectieve protestbewegingen zich enerzijds op het streven naar invloed op wetgeving en anderzijds op het ondersteunen van individuele reacties door het verstrekken van middelen en kennis. Bits of Freedom kan gezien worden als een collectieve reactie. Enerzijds proberen zij (online) privacy binnen wetgeving te verbeteren[3] en anderzijds bieden zij individuen tips voor een veilig internet gebruik[4]. McAdam & Snow (1997) stellen dat collectieve vormen en individuele vormen van verzet met elkaar verbonden zijn. Zij kunnen uit elkaar ontstaan en elkaar versterken. Hoewel ik in dit onderzoek niet wil bekijken hoe collectieve reacties zoals Bits of Freedom als geheel bewegen en functioneren binnen een surveillant assemblage, ben ik wel geïnteresseerd in de rol die het collectieve aspect speelt bij reacties van personen die zich identificeren met een dergelijke organisatie. Juist omdat collectieve en individuele reacties met elkaar verbonden zijn, verwacht ik dat personen verschillende doelen zullen nastreven met hun reacties. Personen kunnen bijvoorbeeld reacties bezigen die zich richten op een collectief doel zoals het steunen van Bits of Freedom en hun lobby voor de bescherming van privacy en persoonsgegevens. Daarnaast kunnen die reacties ook gericht zijn op een individueel doel zoals bijvoorbeeld het beschermen van persoonlijke privacy. Om deze reden maak ik in deze scriptie onderscheid tussen individueel-collectieve en individuele reacties op basis van het doel van de reactie. Voor Hollander & Einwohner (2004: 536) speelt de intentie van handelingen van verzet een belangrijke rol in de uiteindelijke vorm die het verzet aanneemt. Volgens de auteurs bepaalt datgene wat personen willen bereiken met hun verzetshandeling zowel in de praktijk als op analytisch vlak de vorm van verzet. Dit idee pas ik in deze scriptie toe op het onderscheid tussen individueel-collectieve en individuele reacties. Als ik in deze scriptie spreek over individueel-collectieve reacties betreffen dat persoonlijke handelingen die een collectief doel voor ogen hebben terwijl individuele reacties zich richten op een persoonlijk doel[5]. Vanuit de bovenstaande overwegingen kom ik tot de volgende probleemstelling:

Wat zijn de zorgen van personen die zich met Bits of Freedom identificeren, en hoe reageren zij individueel en individueel-collectief op de surveillant assemblage?

Door het beantwoorden van deze probleemstelling biedt mijn onderzoek inzichten in de problemen die personen ervaren met de surveillant assemblage en de manieren waarop zij hierop reageren. Het onderzoek draagt zo bij aan wetenschappelijke kennis over reacties op surveillance in een samenleving waarin persoonlijke informatie meer en meer gekoppeld is aan dagelijkse handelingen, en waarin die gegevens gebruikt wordt door overheden, organisaties en bedrijven. Het hierboven

[3] www.bof.nl/ons-werk/onze-successen/.
[4] www.bof.nl/ons-werk/internetvrijheid-toolbox/.
[5] In paragraaf 2.2 wordt het onderscheid tussen individueel-collectieve en individuele reacties verder beschreven.

beschreven onderscheid tussen individueel-collectieve doelen en individuele doelen laat daarnaast zien of de reacties van personen zich richten op het collectief, of zich meer richten op het individu. Naast zorgen en reacties in het algemeen, schenk ik in deze scriptie ook aandacht aan de notie van verzet tegen surveillance en de rol die macht speelt in een dergelijke surveillant assemblage. Deze scriptie draagt daarom tevens bij aan theorieën over verzet en macht in de context van een surveillant assemblage.

1.4 Opbouw van de scriptie

In hoofdstuk twee worden een aantal centrale thema's, begrippen en theorieën uiteengezet die als theoretisch kader dienen voor deze scriptie. Ik maak gebruik van theorieën over macht, sociale bewegingen alsmede collectief en individueel verzet. In hoofdstuk drie wordt uiteengezet welke methoden en technieken ik in dit onderzoek heb gebruikt. Er wordt beschreven dat het om een kwalitatief onderzoek gaat op basis van zeventien diepte-interviews met fans en volgers van Bits of Freedom. In hoofdstuk vier geef ik de resultaten van de interviews weer met betrekking tot de zorgen van de respondenten over de surveillant assemblage. In hoofdstuk vijf worden vervolgens de resultaten over individueel-collectieve en individuele reacties op diezelfde assemblage besproken. Aan de hand van de analyse van de interviews wordt een ideaaltypische indeling van individuele reacties uiteengezet. Tot slot worden in hoofdstuk zes de samenvatting, conclusie en wetenschappelijke bijdrage van deze scriptie besproken.

Hoofdstuk 2: Theoretisch kader

De probleemstelling die ik in dit onderzoek wil beantwoorden bestaat uit een beschrijvend en een verklarend deel. De zorgen die respondenten hebben met betrekking tot de surveillant assemblage vallen onder het beschrijvende deel. Als het gaat om de reacties die de respondenten bezigen wil ik naast het beschrijven daarvan tevens een verklaring vinden voor diezelfde reacties en de strategieën die daarbij gebruikt worden. Om deze zoektocht te structureren, en om aanknopingspunten te bieden die kunnen helpen bij het verklaren van de resultaten, zal in dit hoofdstuk een overzicht worden gegeven van de wetenschappelijke inzichten en theorieën die in deze scriptie gebruikt worden. Ik richt mij daarbij voornamelijk op theorieën over macht, sociale bewegingen en verzet tegen surveillance.

2.1 Macht, informatie & nieuw feodalisme in de surveillant assemblage

Macht is volgens Castells de "*structural capacity of a social actor to impose its will over other social actor(s).*" (Castells, 2007:239). Daar waar surveillance plaatsvindt ontstaan machtsrelaties. In de meest simpele vorm bestaat die machtsrelatie tussen personen die kijken en personen die bekeken worden. Zeker als personen weten dat zij in de gaten gehouden worden kan dat zorgen voor veranderingen in gedrag. We kunnen dit verduidelijken door te kijken naar Jeremy Bentham's Panopticon (1791). Volgens Green (1999) is dit achttiende-eeuwse gevangenis ontwerp de ultieme metafoor geworden als het gaat om moderne surveillance activiteiten. In dit ontwerp staat een ringvormig gebouw met individuele cellen om één centrale uitkijk toren. Bewakers kunnen in dit ontwerp vanuit de toren iedere gevangene zien terwijl gevangenen de bewakers niet kunnen zien (Green, 1999:29). Volgens Foucault (1977) zorgt dit panoptisch ontwerp voor een illusie van constante en alwetende surveillance. Het feit dat bewakers in principe altijd kunnen zien wat de gevangenen doen, maakt dat de gevangenen zichzelf als het ware surveilleren en daarmee disciplineren. Het gevolg is dat de gevangenen surveillance internaliseren en op den duur zich de regels eigen zullen maken. Voor Foucault staat het panoptisch ontwerp symbool voor een moderne disciplinerende samenleving waarin macht niet meer werkt door zichtbare uitingen zoals bijvoorbeeld institutioneel geweld op een dorpsplein. Surveillance maakt dat macht, en het controleren en disciplineren van de massa, steeds meer uitgaat van subtiele, effectieve en stille vormen van dwang. Volgens Foucault zijn dit kenmerken van een moderne samenleving waarin disciplinering vooral via onopvallende wegen tot uiting komt (Foucault, 1977: 200-209). Green stelt dat de kern van Foucault's analyse een nieuwe vorm van rationaliteit behelst "*where continuous administration – at school, in hospitals, in governing and consumer activity – enables control of day-*

to-day life through a constant gaze." (Green, 1999: 30). Constante surveillance zorgt zo voor een toename van macht van grote organisaties over het individu (Marx, 1985: 32-33).

In hoofdstuk één werd duidelijk dat in de hedendaagse surveillant assemblage het verzamelen en gebruiken van persoonlijke informatie een belangrijke rol inneemt. Omdat vele handelingen van het dagelijks leven tegenwoordig gegevens produceren, of vragen om het vrijgeven van persoonlijke informatie, kunnen we spreken van vele machtsrelaties tussen overheden, bedrijven en organisaties die deze informatie verzamelen en personen waarover informatie verzameld wordt. Of het nu gaat om bewakers en gevangenen, politie en verdachten, docenten en studenten, ouders en kinderen, veiligheidsdiensten en reizigers of ondernemers en klanten: "*surveillance information tends to be one sided and is used to control, manage, affect, and make decisions about the subject.*" (Marx, 2005: 370). Disciplinering zoals werkzaam in het panopticon is zo niet meer de enige uitwerking van macht in een samenleving die gezien kan worden als een surveillant assemblage. Natuurlijk worden zaken als bewakingscamera's en flitspalen ingezet vanuit de panoptische werking. Echter meer en meer heeft de macht van surveillance tevens te maken met kennis over het gedrag van (groepen) mensen om op basis daarvan beslissingen te maken. Enerzijds betreft dat de bureaucratische organisatie van een samenleving door overheden en instituties. Anderzijds gaan die beslissingen over productie, consumptie, omzet en winst: "*Surveillance is a key part of the new technology of selling; the active gaze picks out tell-tale signs and then attempts to predict consuming temptations which can be triggered by direct mail or telesales*." (Green, 1999: 34). Informatie over het sociale gedrag van personen krijgt zo ook economische waarde omdat het naast de mogelijkheden tot governance tevens de mogelijkheden vergroot omzet te realiseren (Haggerty & Ericson, 2000; Green, 1999: 35).

Vele processen van hedendaagse surveillance vinden tegenwoordig onopgemerkt plaats: "*Individuals may no longer be aware that they are the subject of surveillance. Furthermore, they may be unlikely to understand how information held on databases is used to construct consumer, worker or citizen profiles. Information derived from mundane activities such as using a store loyalty card when shopping, booking leisure activities with a credit card or even surfing on the Internet can be used to construct personal data profiles.*" (Hope, 2005: 361). Dit laat zien dat macht niet alleen traditionele controle over het lichaam behelst, maar steeds meer macht betreft op basis van informatie over het gedrag. Die informatie wordt als het ware los gemaakt van individuen en gebruikt in analyses over (groepen) personen. Haggerty en Ericson spreken in dit licht over "*data-doubles"*: "*It is not so much immediately concerned with the direct physical relocation of the human body (although this may be an ultimate consequence), but with transforming the body into pure information, such that it can be rendered more mobile and comparable.*" (Haggerty and Ericson, 2000: 613).

Voor deze veelal samengestelde en digitale profielen die een indirecte vertegenwoordiging van het individu vormen, zijn verschillende benamingen te vinden. Clarke (1994) spreekt van de "*digital persona"* en Solove (2004) van "*digital persons".* Van belang bij deze profielen is echter dat enerzijds personen de controle over hun gegevens op deze manier kwijt raken, en dat anderzijds deze gegevens vervolgens in verschillende contexten gebruikt kunnen worden. De WRR (2011) beschrijft dit proces: "*In de praktijk ontstaan van burgers verschillende profielen en zogenaamde data-doubles, dat wil zeggen een uit verschillende bronnen samengesteld profiel van een persoon dat vervolgens weer een eigen leven gaat leiden in systemen van de overheid (en/of het bedrijfsleven). Die profielen bestaan uit informatie die eerst is gedecontextualiseerd – losgemaakt uit de context waarin de informatie werd verzameld – en vervolgens wordt gehercontextualiseerd in de context van het nieuw samengesteld profiel."* (WRR, 2011: 196). De macht die zowel overheden als bedrijven over personen hebben in een surveillant assemblage is dus veelal gebaseerd op informatie over allerlei vormen van gedrag waarbij de oorspronkelijke context van die gegevens lijkt te verdwijnen.

Personen zijn daarnaast tegenwoordig ook meer en meer afhankelijk van dezelfde diensten en systemen waarmee deze informatie verzameld wordt. De informatie die personen zelf gebruiken in het dagelijks leven is namelijk steeds meer in beheer bij grote (digitale) bedrijven. Schneier (2012) spreekt in dit licht van een soort nieuw feodalisme. Deze digitale veiligheidsexpert stelt dat wij tegenwoordig meer en meer afhankelijk zijn van grote spelers binnen onze digitaal georiënteerde samenleving. Bedrijven zoals Facebook, Google, Microsoft en Apple beheren onze gegevens, agenda's, mobiele telefoons en e-mails zonder dat wij precies weten hoe zij dat doen. Het gemak dat deze bedrijven ons bieden maakt voor een groot deel dat we gebruik maken van hun diensten. Maar, stelt Schneier, zelfs als wij het zouden willen is het "*increasingly difficult to not pledge allegiance to at least one of them (...) Trust is our only option. In this system, we have no control over the security provided by our feudal lords. We don't know what sort of security methods they're using, or how they're configured.*" (Schneier. 2012: 35-36). Niet alleen zijn burgers afhankelijk van bedrijven en de manieren waarop zij met onze gegevens om gaan. Ook overheden maken steeds meer gebruik van digitale gegevens over burgers en wisselen deze uit tussen verschillende overheidsorganen en sectoren. Het ontstaan van wat de WRR (2011) beschrijft als de "iOverheid" zorgt ervoor dat volgens het rapport burgers er rekening mee moeten houden dat hun informatie zowel in publieke als private handen een eigen leven kan gaan leiden. Dit omdat enerzijds de verantwoordelijkheid voor de kwaliteit en juistheid van die informatie niet is mee geëvolueerd in de mate waarin het gebruik van die gegevens dat wel is. Anderzijds is er sprake van een vernetwerking van informatie waarbij gegevens over personen via dwarsverbanden en informatiestromen tussen verschillende organisaties

en afdelingen van de overheid zich verplaatsen, zonder dat er duidelijk is wie er verantwoordelijk is voor deze gegevens (WRR, 2011: 12-121).

De hierboven beschreven afhankelijkheid van dezelfde diensten en systemen die het dagelijks digitaal georiënteerde leven mogelijk maken, alsmede de manieren waarop deze geïntegreerd zijn in de hedendaagse samenleving zullen waarschijnlijk een rol spelen in de manieren waarop personen reageren op de surveillant assemblage. Reacties op, of verzet tegen de machtsrelaties die voortkomen uit de assemblage zullen zo van invloed zijn op de manier waarop personen in het dagelijks leven zich bewegen in een dergelijke samenleving. Voordat ik bespreek welke theorieën over individuele reacties op surveillance ik in deze scriptie gebruik om te bekijken hoe respondenten en hun reacties zich verhouden tot deze afhankelijkheid, zal ik eerst stil staan bij de rol en invloed van sociale bewegingen op personen die zich met een dergelijke beweging identificeren.

2.2 Collectieve reacties: empowerment & gedeelde doelen

Hoewel deze scriptie zich niet richt op een analyse van sociale bewegingen zoals Bits of Freedom in een surveillant assemblage, is het wel verstandig te bekijken hoe theorieën over sociale verandering en collectieve actie kunnen bijdragen aan het begrijpen en verklaren van reacties van personen die zich met dergelijke organisaties identificeren. Volgens Blumer (1969) kunnen sociale bewegingen gezien worden als collectieve ondernemingen "*to establish a new order of life.*". Ze vinden hun oorsprong in een bepaalde vorm van onrust en halen motivatie uit enerzijds een ontevredenheid over de huidige manier van leven en anderzijds de wens en de hoop voor "*a new scheme or system of living.*" (Blumer, 1969 in Rugiero & Montagna, 2008: 64). Sociale bewegingen hebben dus een hoger of collectief doel om verandering in de samenleving te bewerkstelligen. Voor Castells (2007) zijn sociale bewegingen een permanent onderdeel van een samenleving en organiseren zij zich op dezelfde manieren waarop samenlevingen waarbinnen zij zich bevinden zich organiseren. *"(..) because power relations are structured nowadays in a global network and played out in the realm of socialized communication, social movements also act on this global network structure and enter the battle over the minds by intervening in the global communication process*." (Castells, 2007:249). Het citaat laat zien dat sociale bewegingen verweven zijn in een "*battle of the minds"* en daarbij gebruik maken van dezelfde communicatie netwerken die de hedendaagse machtsrelaties structureren. Naast het creëren van een achterban gebruiken sociale bewegingen dergelijke netwerken ook om de leden van hun beweging te mobiliseren en te activeren. We zagen in hoofdstuk één al dat collectieve reacties met individuele reacties van verzet op een dergelijke manier verbonden zijn. Deze verbondenheid heeft in de context van surveillance betrekking op het bieden van middelen en kennis waarmee individuen kunnen reageren of zich kunnen verzetten (Marx, 2003; McAdam & Snow, 1997).

Empowerment van individuen is daarmee tevens een onderdeel van sociale bewegingen. Dit verstrekken van kennis en middelen is een onderdeel van wat Eyerman & Jamison (1991) zien als de cognitieve praxis. Het gaat daarbij om het proces waarbij het genereren van bepaalde ideeën en kennis zorgt voor eenheid binnen sociale bewegingen. Sociale bewegingen nemen niet alleen ideologische posities in, ze creëren kennis en daarmee culturele verandering. Er zijn drie dimensies van de cognitieve praxis: ten eerste het wereldbeeld van de beweging en hun doelen, ten tweede de manier waarop ze relateren aan het gebruik van technologie, en ten derde de organisatie en activiteiten van de beweging (Eyerman & Jamison, 1991 in Lindgren, 2013: 127). Dit wil niet meteen zeggen dat personen die zich identificeren met een dergelijke beweging als homogene groep kunnen worden gezien. Wel laat het laat zien dat er bepaalde gedeelde ideeën, opvattingen en doelen te vinden zijn binnen die groep. Voor Diani (1992) is een sociale beweging namelijk: "*a network of informal interactions between a plurality of individuals, groups and/or organizations, engaged in a political or cultural conflict, on the basis of a shared collective identity.*" (Diani, 1992 in Rugiero & Montagna, 2008: 271).

In het geval van deze scriptie heeft dat gedeelde conflict betrekking op machtsrelaties die voortkomen uit de surveillant assemblage. De gedeelde identiteit die Diani hierboven noemt is tevens van belang omdat een dergelijke gedeelde identiteit tot veranderingen kan leiden in opvattingen en de manier van leven. Want: "*The collective identity formation that takes place in social movements is a central catalyst of broader changes in values, ideas, and way of life.*" (Eyerman & Jamison, 1998: 7). Ik verwacht dat een deel van de manieren waarop respondenten reageren op de surveillant assemblage in dienst staan van het hierboven beschreven collectieve doel, de gedeelde identiteit of het gedeelde conflict waar Bits of Freedom zich op richt. En hoewel de vorm van dergelijke reacties niet georganiseerd hoeft te zijn en de daadwerkelijke handeling wellicht puur een individuele is, is het dit doel op basis waarvan ik dergelijke reacties als individueel-collectief zal beschouwen. Individuele reacties zoals ik die bespreek in deze scriptie hebben dan vooral een persoonlijk doel. Het is verstandig om hier middels een schema inzichtelijk te maken hoe het hierboven, en in hoofdstuk één beschreven onderscheid tussen collectieve, individueel-collectieve en individuele reacties op surveillance wordt gezien in deze scriptie.

Figuur 1: Schematisch overzicht van soorten reacties op surveillance	
Collectieve reacties	Sociale georganiseerde bewegingen Collectieve doelen en gedeelde identiteiten
Individueel-collectieve reacties	Individuele handelingen Gericht op collectieve doelen
Individuele reacties	Individuele handelingen Gericht op persoonlijke doelen

Hoewel collectieve reacties in dit onderzoek van belang zijn omdat het de context waarin en waaruit personen reageren op de surveillant assemblage duidelijk maakt, richt ik mij met de probleemstelling in dit onderzoek op de onderste twee reacties. Het onderscheid tussen individueel-collectieve en individuele reacties wordt gebruikt om te bekijken of reacties van personen een collectief of individueel doel hebben.

Voordat ik mij richt op enkele theoretische denkbeelden over individuele reacties op surveillance is er nog één begrip wat ik in dit licht wil behandelen. Enerzijds omdat het een belangrijk concept is bij het mobiliseren van sociale verandering. Het beschrijft een bewustzijn van gedeelde opvattingen, identiteiten of conflicten van waaruit personen kennis en middelen mobiliseren om op collectief niveau verandering te bewerkstelligen, en op individueel niveau zich te verzetten. Anderzijds is het begrip van belang omdat het de theoretische achtergrond is die de respondenten in dit onderzoek delen. Gilliom (2005: 122-128) spreekt van "*oppositional consciousness"* als hij ervaringen, kennis en reacties met betrekking tot surveillance bespreekt. Gilliom licht het concept niet verder toe, maar stelt wel dat het inzichten kan bieden in de manieren waarop personen over surveillance spreken en denken. In de literatuur over sociale actie is oppositioneel bewustzijn een centraal concept. Volgens Waite (2001) behelst een oppositioneel bewustzijn (...)"*an empowering mental state that prepares members of an oppressed group to act to undermine, reform, overthrow a system of human domination. That mental state includes identifying with members of a group, recognizing and opposing injustices done to that group, and recognizing a group common interest in ending those injustices*" (Waite, 2001: 173).

Hoewel het in de context van surveillance niet per definitie gaat om *human domination* maar om machtsrelaties die voortkomen uit surveillance is het concept toch bruikbaar. In deze scriptie gebruik

ik het concept oppositioneel bewustzijn om te verwijzen naar gedeelde opvattingen, identiteiten en conflicten met betrekking tot de surveillant assemblage van waaruit personen een noodzaak ervaren om individueel-collectief of individueel in actie te komen. De bovenstaande paragraaf geeft inzichten in de mogelijke collectieve aspecten van dergelijke reacties. In de volgende paragraaf zal ik aandacht besteden aan de meer individuele aspecten van reacties op surveillance. Ik doe dat aan de hand van een aantal theoretische denkbeelden over de manieren waarop individuen reageren op, en zich verzetten tegen surveillance.

2.3 Individuele reacties: alledaags verzet tegen de surveillant assemblage

Een veel voorkomende individuele reactie op surveillance is dat personen niets doen. "*Vast majorities consciously or unconsciously acquiesce to the new systems of power.*" (Gilliom, 2005: 114). Daarbij wordt in de context van de informatiesamenleving vaak het "*nothing to hide*" argument gebruikt. Deze stelt dat als je niets strafbaars doet, je niets te vrezen hebt van dataverzameling en surveillance. Omdat personen niets te verbergen hebben verzetten zij zich daarom niet tegen surveillance (Solove, 2007: 744-745). Hoewel er sterke aanwijzingen zijn dat iedereen tegenwoordig onder surveillance staat, gaan veel personen er nog steeds van uit dat surveillance vooral gericht is op "*miscreants and wrongdoers."* (Bennett: 2008:97-98). Als het gaat om personen die zich met Bits of Freedom identificeren verwacht ik wel dat zij zullen reageren op de surveillant assemblage. Dit omdat het waarschijnlijk is dat zij in meer of mindere mate een oppositioneel bewustzijn hebben, en gebruik maken van de kennis en middelen die Bits of Freedom faciliteert. Voordat ik mij richt op de manieren waarop personen zich tegen surveillance kunnen verzetten zal ik eerst bekijken wat verzet vanuit een breder sociologisch oogpunt behelst.

We zagen in paragraaf 2.1 dat surveillance te maken heeft met macht. Voor Foucault gaat macht altijd gepaard met verzet: "*Where there is power, there is resistance, and yet, or rather consequently, this resistance is never in a position of exteriority in relation to power.*" (Foucault, 1978: 95). Verzet is echter een breed begrip. Hollander en Einwohner (2004) stellen dat hoewel verzet binnen de sociologie veel aandacht krijgt, er weinig consensus is over wat sociologen precies onder dit begrip verstaan. Dit komt volgens de auteurs omdat vooral de schaal, coördinatie, mikpunten en doelen van verzet verschillende vormen aan kunnen nemen. Aan de hand van een literatuurstudie met als doel de analytische kracht van het concept te verbeteren komen de auteurs tot een aantal bevindingen. Ten eerste zien ze dat "*(…) resistance is not a quality of an actor or a state of being, but involves some active behavior, whether verbal, cognitive or physical.*". Daarnaast zien ze dat dit gedrag uitgaat van een "*sense of opposition*" (Hollander en Einwohner, 2004: 538). Volgens Hollander en Einwohner zijn *actie* en *oppositie* centrale kenmerken van verzet. Echter stellen de auteurs ook dat er discussie is

over de *herkenning* en *intentie* van verzet. Een centraal punt is hierbij dat de zichtbaarheid van verzet kan variëren omdat het doel verschillende vormen kan aannemen. We zien hier wederom dat het doel van verzet van invloed is op de vorm. In deze scriptie gebruik ik het doel van de reacties van personen om te bekijken of het om individueel-collectieve of individuele reacties gaat. Wat wij verder uit het bovenstaande kunnen leren is dat wij kunnen spreken van verzet als er een mate van verbale, cognitieve of fysieke actie vanuit een oppositioneel oogpunt te vinden is bij de reacties van personen.

Als het gaat om verzet tegen surveillance stelt Marx dat personen regels zullen overtreden als zij surveillance zien als "*unacceptable or illegitimate, untrustworthy or invalid, demeaning, unnecessary, or irrelevant.*" (Marx, 2003: 372-373). De mogelijkheden om verzet te plegen zijn echter in grote mate afhankelijk van kennis die personen over de surveillance systemen hebben (Haggerty & Ericson, 2005: 20). Volgens Martin, van Brakel en Bernhard (2009) is de rol van personen binnen een surveillance relatie daarnaast van groot belang voor de middelen en mogelijkheden tot verzet: "*Emanating from the position that roles condition means, we find instead that different actors are more likely to resist at certain stages than others, using their unique role based means to do so.*" (Martin, van Brakel & Bernhard. 2009: 227). Gilliom stelt ongeveer hetzelfde als hij zegt dat het uitmaakt wie je bent, wat je middelen zijn en hoe bedreigend surveillance voor je is (Gilliom, 2005: 125). We kunnen een aantal voorbeelden aanhalen die het belang van deze rollen inzichtelijk maakt. In een klassieke studie spreekt Scott (1985) van "*everyday forms of peasant resistance*" (1985: 29). Daarmee beschrijft hij de mogelijkheden die machteloze groepen hebben om zich te verzetten tegen surveillance. Scott onderzocht de individuele strategieën van arme boeren in een klein Maleisisch dorp om uitbuiting met betrekking tot arbeid, voedsel en belastingen door autoriteiten te voorkomen. Hij vond *"(...) the ordinary weapons of relatively powerless groups: foot dragging, dissimulation, false compliance, pilfering, feigned ignorance, slander, arson, sabotage and so forth*" (Scott, 1985: 29). Het betreffen hier volgens Scott kleine handelingen die vooral gericht zijn op het behalen van directe en concrete voordelen. Ook Gilliom (2001) identificeerde dergelijke patronen van alledaags verzet. Hij vond manieren waarop bijstandsmoeders uit de greep van overheidssurveillance probeerde te blijven. Hoewel deze handelingen vooral gemotiveerd waren om kleine financiële voordelen te behalen die de regels van de bijstand zouden verbieden was er volgens Gilliom sprake van verzet. Niet zozeer vanuit een ideologie, maar vanuit de wil te overleven. De auteur stelt dat (kans)arme personen vaak de middelen missen om georganiseerd formeel protest en verzet te bezigen. In plaats daarvan gebruiken zij ad hoc technieken zoals het vervalsen van voedselbonnen en het achterhouden van informatie. Gilliom spreekt van een "*widespread pattern of complaint, evasion and resistance, as welfare mothers struggle with the system that defines their condition.*" (Gilliom, 2001: 112).

De bovenstaande voorbeelden leren ons dat vormen van verzet tegen surveillance bij relatief machteloze groepen vooral gericht zijn op het behalen van kleine voordelen binnen de afhankelijkheid van de machtsrelatie in kwestie. De rol van de boeren en bijstandsmoeders verschilt echter op een aantal punten met die van personen die zich met een Bits of Freedom identificeren. Die verschillen komen vooral voort uit de context waarin de personen zich bevinden. Zo plegen de boeren en bijstandsmoeders voornamelijk verzet om een direct voordeel te behalen of een direct nadeel te beperken. In de surveillant assemblage zijn de gevolgen van surveillance veel meer indirecte gevolgen, of spelen de processen zich 'achter de schermen' af. Mogelijk verzet hiertegen zal zich dus waarschijnlijk richten op deze meer onzichtbare processen of op ideologische denkbeelden daarover. Daarnaast zorgt de surveillant assemblage ervoor dat er een veelheid aan machtsrelaties bestaan met daarbij een hoge mate van integratie van surveillance in het dagelijks leven. Dit in tegenstelling tot de enkele systemen van surveillance waartegen de boeren en bijstandsmoeders zich verzetten. Echter is er ook een overeenkomst te zien. Deze heeft te maken met de afhankelijkheid van de surveillance systemen in de hedendaagse samenleving en het gedwongen vertrouwen dat wij bij Schneier (2012) zagen. Het maakt dat personen in een surveillant assemblage, zoals de boeren en bijstandsmoeders, wellicht ook te maken hebben met een bepaalde machteloosheid. En hoewel de oorzaak van die machteloosheid verschilt stelt Marx (2003) dat: "*Powerless takes on a new meaning (beyond its usual association with lower social class or minority status) when we consider the demands of the modern organization for personal information.*" (Marx, 2003: 372).

Hoewel de context en daarmee de rollen van personen die zich met Bits of Freedom identificeren verschillen met die van de boeren en bijstandsmoeders, leren wij van Marx dat verzet tegen een surveillant assemblage gekenmerkt kan worden door eenzelfde soort machteloosheid. Voor Marx komt die machteloosheid voort uit de afhankelijkheid van het gebruik van persoonlijke informatie in ons dagelijks leven. Ook Graham & Wood (2003) en Gilliom & Monahan (2012) wijzen indirect op een dergelijke machteloosheid als zij stellen dat de mogelijkheden tot verzet in een surveillant assemblage beperkt zijn. Desalniettemin zien Gilliom & Monahan (2012) wat zij noemen "*everyday resistance*". Zij bouwen voort op de ideeën van Scott (1985) en Gilliom (2001) en stellen dat: "*The central characteristics of everyday resistance practices are that they are unorganized, not explicitly tied to broader ideological critiques, and originate from direct concerns in daily life. Everyday resistance is a unique subset of resistance and opposition to surveillance: the category specifically excludes organized movements, traditional ideology, and public confrontations*." (Gilliom & Monahan, 2012: 405). Alledaags verzet gaat volgens de auteurs dus vooral uit van ongeorganiseerde handelingen die voortkomen uit directe zorgen in het alledaagse leven. De auteurs benadrukken tevens dat dergelijke reacties verschillen van de meer georganiseerde en traditioneel ideologische

reacties. Dit onderscheid heeft raakvlakken met het onderscheid tussen individueel-collectieve en individuele reacties waar ik mij in deze scriptie op richt. Omdat ik verwacht bij de respondenten naast individueel-collectieve tevens dergelijke individuele reacties te vinden, zal ik nu kort aandacht besteden aan de mogelijke manieren en vormen van alledaags verzet tegen surveillance.

Marx (2003) geeft een overzicht van de vormen van verzet die hij tijdens zijn wetenschappelijke loopbaan tegen is gekomen. *Discovery moves* hebben als doel het ontdekken van surveillance. *Avoidance moves* behelzen het ontlopen van surveillance. *Piggybacking moves* ontwijken controle of beschermen informatie door gebruik te maken van objecten of personen die legitiem lijken bij surveillance. *Switching moves* gaan uit van het verwisselen van gesurveilleerde objecten of personen. *Distorting moves* manipuleren de verzamelde surveillance-informatie waardoor technisch valide resultaten zichtbaar worden terwijl ze dat niet zijn. *Blocking moves* behelzen het fysiek tegengaan van surveillance. *Masking moves* gaan ook uit van het tegengaan van surveillance, maar geven daarvoor misleidende informatie. *Breaking moves* hebben betrekking op het onklaar maken van surveillancetechnieken. *Refusal moves* legt Marx uit als het negeren van vragen over persoonlijke informatie ten behoeve van surveillance. *Cooperative moves* zijn manieren om surveillance tegen te gaan in samenwerking met, of vanuit een organisatie die zelf gebruik maakt van surveillance. *Counter-surveillance moves* behelzen het omdraaien van surveillance: het surveilleren van diegene die normaal surveillance uitvoeren (Marx, 2003: 374-384). In deze beschrijving worden zowel online als offline handelingen beschreven, zowel specifieke als algemene doelen van verzet gevonden en wordt er geen onderscheid gemaakt tussen verzet vanuit ideologie en verzet vanuit meer praktische motivaties. Vooral de beschreven context van de surveillant assemblage die centraal staat in deze scriptie, ontbreekt in deze beschrijving. Marx zelf vraagt zich in zijn conclusie af hoe generaliseerbaar deze handelingen zijn, en of deze bruikbaar zijn binnen andere contexten van informatieverzameling en surveillance. Verderop zal duidelijk worden in welke mate dit in de context van de surveillant assemblage, zoals beschreven in deze scriptie, het geval is. Om echter helder te krijgen hoe de beschreven theorieën en denkbeelden uit dit hoofdstuk gebruikt worden in het empirische deel van deze scriptie, zal ik hieronder een korte conclusie uiteenzetten.

2.4 Conclusie: de afhankelijkheid van de surveillant assemblage

Hoewel al het bovenstaande van belang is bij het analyseren en het interpreteren van de empirische gegevens uit dit onderzoek, zijn er een aantal onderdelen die als centrale aandachtspunten gebruikt worden bij het verklaren van de resultaten van dit onderzoek. Deze punten worden hier kort besproken. In de beschreven surveillant assemblage spelen vele, vaak indirecte en onzichtbare machtsrelaties een belangrijke rol. Deze machtsrelaties komen voornamelijk voort uit het

bureaucratisch alsmede economisch gebruik van persoonsgegevens. Ze bestaan tussen burgers en consumenten aan de ene kant, en bedrijven en overheden die allerhande persoonsgegevens verzamelen aan de andere kant. Binnen de machtsrelaties lijken personen enerzijds steeds minder controle te hebben over hun persoonlijke gegevens en de manieren waarop overheden en bedrijven deze gegevens hercontextualiseren. Anderzijds lijken personen in hun dagelijks leven veelal afhankelijk te zijn van dezelfde systemen en diensten die deze gegevens verzamelen. Als het gaat om de reacties op de surveillant assemblage heb ik onderscheid gemaakt tussen individueel-collectieve en individuele reacties. Er wordt in deze scriptie niet gekeken naar georganiseerde collectieve reacties zoals sociale bewegingen als geheel. Omdat dergelijke collectieve reacties echter wel verbonden zijn met individuele reacties, verwacht ik dat individuele reacties zowel persoonlijke als collectieve doelen zullen hebben. Anders gezegd kunnen reacties van personen gemotiveerd zijn vanuit het doel bepaalde veranderingen te bewerkstelligen in de manier waarop bedrijven en overheden omgaan met persoonsgegevens en macht binnen de samenleving. Daarnaast kunnen reacties van personen tevens gemotiveerd zijn vanuit het doel om in het dagelijks leven persoonlijke en directe voordelen te behalen binnen de machtsrelaties. Deze doelen van reacties worden daarom gebruikt om het beschreven onderscheid tussen de soorten reacties te operationaliseren. Als het gaat om verzet tegen surveillance in de context van de surveillant assemblage komt naar voren dat er rekening gehouden moet worden met een bepaalde mate van machteloosheid. Juist omdat het gebruik van persoonsgegevens zo geïntegreerd is in de organisatie van de hedendaagse samenleving en de manieren waarop personen zich daarbinnen bewegen, valt te verwachten dat verzet hiertegen niet altijd gemakkelijk te realiseren zal zijn. Hoewel er theoretische aanwijzingen te vinden zijn voor de mogelijkheid tot alledaags verzet tegen deze vormen van surveillance, moet dat verzet daarom worden bezien vanuit de context en de rollen die de personen innemen binnen de machtsrelaties. Vooral de besproken integratie en afhankelijkheid van dezelfde systemen en componenten die enerzijds de surveillant assemblage vormen, en anderzijds het moderne dagelijks leven mogelijk maken, moeten daarbij in acht worden genomen.

Hoofdstuk 3: Methoden & technieken

3.1 Kwalitatief onderzoek

Om de in hoofdstuk één beschreven probleemstelling te beantwoorden heb ik gebruik gemaakt van een kwalitatief onderzoek. Kwalitatief onderzoek is een goede methode om het handelen, de betekenisgeving en de zienswijze van personen in een bepaalde context te onderzoeken (Flick, 2009: 16-17). In deze scriptie tracht ik de sociale werkelijkheid alsmede het handelen van personen die zich met Bits of Freedom identificeren in de context van een surveillant assemblage te achterhalen. Door de zorgen en reacties van respondenten te beschrijven, en waar mogelijk te verklaren, probeer ik een ideaaltypische indeling van individuele reacties op de surveillant assemblage te construeren. Naast dat dit onderzoek beschrijvende en verklarende kenmerken heeft, richt het zich tevens op het vormen van theorie. Het is van belang te vermelden dat in een ideaaltype bepaalde aspecten van de werkelijkheid kunnen worden benadrukt, terwijl andere aspecten kunnen worden veronachtzaamd. Dit komt omdat een ideaaltype een afspiegeling is van de werkelijkheid, die logisch geconstrueerd is en van kunstmatige en analytische aard zijn. Op deze manier is een vergelijking tussen de ideaaltypen mogelijk (Zijderveld, 1990: 45-47). Dit kan echter betekenen dat geen van de respondenten precies in een ideaaltype in te delen is, en dat zij zich waarschijnlijk niet (volledig) zullen herkennen in deze sociologische constructie.

3.2 Respondenten

Voor dit onderzoek heb ik zeventien diepte-interviews gehouden met personen die zich identificeren met Bits of Freedom. Ik heb daarbij gebruik gemaakt van doelgerichte selectie (purposive sampling) van de onderzoekseenheden. Volgens Boeije (2005) worden bij deze vorm van selectie doelgericht onderzoekseenheden uit een populatie geselecteerd die bepaalde kenmerken representeren. Het doel is hierbij de diverse uitingsvormen van een verschijnsel in de onderzoeksgroep weer te geven. De kenmerken van de populatie zijn daarbij de basis voor de selectie (Boeije, 2005: 50). Het kenmerk op basis waarvan de respondenten in dit onderzoek zijn gekozen betreft het identificeren met een georganiseerde collectieve reactie op de surveillant assemblage. Hoewel hiermee geen statistische representativiteit wordt gerealiseerd, geeft het wel de mogelijkheid om de verschillende uitingsvormen van reacties bij deze populatie te onderzoeken. De populatie in deze scriptie bestaat daarmee uit personen die zich identificeren met Bits of Freedom. Onder de respondenten zijn er twee vormen van dit identificeren te onderscheiden: fans en volgers. Tien respondenten zijn 'fan' van Bits of Freedom. Zij staan op een webpagina van Bits of Freedom[6] publiekelijk vermeld als fan van de beweging. Om op deze pagina als fan te komen moeten personen zichzelf aanmelden. Het zelf

[6] www.bof.nl/over-ons/de-beweging/.

aanmelden als fan zie ik in deze scriptie als het identificeren met Bits of Freedom. Omdat het wegens toegankelijkheidsproblemen niet mogelijk bleek om met voldoende fans te spreken, is er op mijn verzoek een bericht vanuit Bits of Freedom naar hun sociale media volgers uit gegaan. Via dat bericht kwam men op een Facebook-pagina waarin ik personen vroeg om hun medewerking aan mijn onderzoek. De kop van het bericht was de volgende: *Ben jij fan van Bits of Freedom? Of steun je de standpunten en het werk van Bits of Freedom? Dan wil ik in het kader van mijn afstudeeronderzoek graag met jou spreken*[7]. De personen die hebben gereageerd op dit verzoek zijn de zeven resterende respondenten. Deze zeven 'volgers' hebben danwel via Facebook, danwel via Twitter aangegeven sociale media berichten van Bits of Freedom te willen ontvangen. Deze handeling samen met het feit dat personen hebben gereageerd op mijn verzoek, en zo hebben aangegeven fan te zijn of het werk van Bits of Freedom te steunen, maakt dat ik in deze scriptie ervan uit ga dat deze personen zich tevens met Bits of Freedom identificeren. Omdat de respondenten als fan of volger zich identificeren met Bits of Freedom, was mijn verwachting dat er in meer of mindere mate sprake zou zijn van het eerder genoemde oppositioneel bewustzijn. Hoe dat oppositioneel bewustzijn er precies uit zou zien was vooraf aan het onderzoek niet vast te stellen. Wel gaf het identificeren met Bits of Freedom aanleiding te verwachten dat er bij de respondenten sprake leek te zijn van een gedeeld ervaren probleem en een gedeelde wil daar iets aan te veranderen. Omdat er een verschil bestaat tussen de twee groepen heb ik tijdens de verzameling alsmede analyse van de onderzoeksgegevens bekeken of er verschillen in denkbeelden en reacties te vinden waren. Vanuit de theoretische context waaruit in dit onderzoek naar de respondenten wordt gekeken bleek dit niet het geval.

Om de privacy van de respondenten zo goed mogelijk te waarborgen zijn de namen van de respondenten in deze scriptie geanonimiseerd. Vijf respondenten waren tussen de 19 en 24 jaar, zeven respondenten tussen de 30 en 37 jaar en vijf respondenten tussen de 40 en 44 jaar oud. Drie respondenten waren vrouw en veertien respondenten man. Het opleidingsniveau van de respondenten betrof in elf gevallen WO en in zes gevallen HBO. De studierichtingen van de respondenten betroffen: Civiele techniek, Human Technology, Geschiedenis, Informatica, Technische Informatica, Bio Informatica, Filosofie, Lerarenopleiding, Rechten, Bedrijfskader en Politicologie. Vier respondenten waren ten tijde van het onderzoek nog bezig met hun studie, de rest van de respondenten waren voornamelijk werkzaam in een ICT en internet gerelateerde sector, en hielden zich daarbij bezig met marketing, design, consultancy, beveiliging en freelance werk.

[7] Voor de gehele uitnodiging verwijs ik u naar de bijlage.

3.3 Structuur van de interviews

In de maanden april en mei van 2013 hebben de zeventien interviews plaats gevonden. Negen interviews hebben plaats gevonden bij de respondenten thuis, drie interviews op het werk van de respondenten en vijf interviews vonden plaats in een café of restaurant. Het startpunt van ieder gesprek was de reden van de respondent om zich bezig te gaan houden met Bits of Freedom en zaken als online privacy en de bescherming van persoonsgegevens. Door het stellen van deze vraag werd enerzijds duidelijk vanuit welke achtergrond de respondenten met Bits of Freedom in aanraking zijn gekomen en anderzijds een eerste indicatie duidelijk over de mogelijke zorgen op dit gebied. In de gesprekken heb ik de respondenten aangemoedigd zo vrij en uitgebreid mogelijk te spreken over hun denkbeelden. Hoewel het verloop van de gesprekken niet vast lag, heb ik in het interview gebruik gemaakt van een topiclijst die als leidraad heeft gediend voor het interview. Deze onderwerpen kwamen afhankelijk van het verloop van het gesprek in willekeurige volgorde aan bod. Daar waar bepaalde onderwerpen niet vanzelf in het gesprek langs kwamen heb ik het gesprek zo gestuurd dat deze dat wel kwamen. Op de eerder genoemde topiclijst kwamen de volgende punten voor:

Achtergrond: Hoe en waarom is de respondent in aanraking gekomen met Bits of Freedom? Liggen daar bepaalde gebeurtenissen of denkbeelden aan ten grondslag? Hoe ziet de respondent de rol van Bits of Freedom op dit gebied?

Zorgen: Is er sprake van zorgen bij de respondent? Wat zijn de risico's en wie of wat is het probleem? Hebben deze zorgen alleen betrekking op het internet? Heeft de respondent zelf iets meegemaakt op dit gebied?

Privacy: Wat is privacy volgens de respondent? Is privacy mogelijk? Moet privacy beschermd worden? Maakt de respondent onderscheid in bepaalde (persoons)gegevens?

Reacties: Wat is de invloed van deze thematiek op het dagelijks leven van de respondent? Doet of laat de respondent bepaalde zaken in zijn dagelijks (sociale) leven? Voelt de respondent zich onderdeel van een beweging? Is er een verschil tussen online en offline? Is het een individuele aangelegenheid of is het collectief van belang?

Slot: Is er volgens de respondent iets niet besproken wat in het licht van deze onderwerpen wel besproken moet worden? Is de respondent het eens met de samenvatting van het gesprek gegeven door de onderzoeker?

3.4 Analyse

De analyse die ik heb gebruikt in dit onderzoek laat zich omschrijven als de constant vergelijkende methode. Deze methode maakt de vorming en afbakening van categorieën mogelijk (Boeije, 2005: 75). Door continu te kijken naar de verschillen en overeenkomsten in de zorgen en reacties van de respondenten, zijn patronen naar voren gekomen op basis waarvan ik een typologie van reacties heb kunnen opstellen. Deze ideaaltypische indeling geeft inzicht in de verschillende reacties van de respondenten en maakt het mogelijk te bekijken welke omstandigheden een rol spelen bij de manieren waarop deze reacties zich manifesteren. Daarnaast laat het tevens zien vanuit welk doel respondenten reacties bezigen en welke factoren van invloed zijn bij de keuze en mogelijkheden voor deze reacties. Om de validiteit zo goed mogelijk te waarborgen zijn alle gesprekken opgenomen en op een later tijdstip getranscribeerd. Aan het einde van de gesprekken heb ik de belangrijkste denkbeelden en bevindingen uit het gesprek kort besproken met de respondent om na te gaan of de respondent zich hierin kon vinden.

Betrouwbaarheid binnen kwalitatief onderzoek is vaak afhankelijk van de beoordelingen die de onderzoeker tijdens het onderzoek maakt (Babbie, 2007: 314). Om problemen met betrouwbaarheid te beperken heb ik getracht mij bewust te zijn van mijn eigen opvattingen en mij zoveel mogelijk te richten op enkel vergelijkende evaluaties. Volgens Boeije (2005: 150-151) is het verstandig om duidelijk weer te geven vanuit welke theoretische vooroordelen de onderzoeker het onderzoek is gestart[8] en te reflecteren over de invloed van de onderzoeker op de verzameling en analyse van de onderzoeksgegevens.

3.5 Persoonlijk perspectief onderzoeker

Hoewel ik heb getracht mij zoveel mogelijk te beperken tot vergelijkende evaluaties waarbij mijn persoonlijke opvattingen zo min mogelijk een rol spelen, is het onvermijdelijk dat mijn achtergrond en persoonlijke (voor)oordelen van invloed zijn geweest op de manier waarop ik naar het onderzoeksonderwerp heb gekeken alsmede dat deze kenmerken van invloed zijn geweest op de manier waarop de respondenten op mij hebben gereageerd (Boeije, 2005: 151). Als het gaat om het onderwerp van privacy en de bescherming van persoonsgegevens is het van belang op te merken dat ik voorafgaande aan dit onderzoek mij niet of nauwelijks bezig heb gehouden met deze onderwerpen. Ik ben voor het eerst in aanraking gekomen met Bits of Freedom in de periode van het ontwikkelen van het onderzoeksthema, de probleemstelling en het onderzoeksontwerp. Tijdens mijn studie sociologie heb ik wel een interesse ontwikkeld voor de manieren waarop technologie en het internet van invloed zijn op het (samen)leven van personen binnen een westerse en meer en meer digitale

[8] Zie hoofdstuk 2

samenleving. Centraal staat daarbij dat ik overtuigd ben van het feit dat digitalisering, technologie en het internet een belangrijke invloed hebben op dit samenleven. Mijn interesse voor deze invloed heb ik vooraf aan de interviews aan de respondenten duidelijk gemaakt als motivatie voor dit onderzoek. Mijn opvattingen over online privacy en de bescherming daarvan zijn moeilijk te omschrijven. Dit omdat ik enerzijds pas tijdens dit onderzoek ben gaan nadenken over deze onderwerpen, en anderzijds omdat ik op het moment van het schrijven van deze scriptie geen eenduidig standpunt heb ingenomen in deze discussie. Wel ben ik van mening dat het nadenken over vraagstukken omtrent (online) privacy in onze hedendaagse samenleving op het niveau van wetgeving van belang is, maar heb tijdens het onderzoek getracht dit waardeoordeel zo min mogelijk te laten mee spelen in mijn analyse. Het feit dat mijn onderzoek en analyse zich richt op de beleving en reacties van respondenten heeft er mijns inziens voor gezorgd dat in deze scriptie mijn standpunten zo min mogelijk een rol hebben gespeeld.

Hoofdstuk 4: Zorgen over de surveillant assemblage

In dit hoofdstuk worden de resultaten besproken met betrekking tot de zorgen van de respondenten. Eerst wordt beschreven welke ontwikkelingen ten grondslag liggen aan de zorgen van de respondenten. Vervolgens komen drie centrale zorgen aan bod. Als deze zorgen duidelijk zijn geworden, wordt de rol van privacy binnen deze zorgen besproken. Tot slot wordt in een concluderende paragraaf besproken wat deze bevindingen betekenen voor het oppositioneel bewustzijn van de respondenten.

4.1 De achtergrond van zorgen: controle & de hang naar informatie

Hoewel veel van de respondenten via hun studie of beroep zich binnen het veld van technologie, ICT en het internet bevinden, is het voornamelijk een persoonlijke interesse voor deze onderwerpen die de respondenten aandragen als reden zich bezig te houden met privacy, persoonsgegevens en Bits of Freedom. Vooral een interesse voor de uitwerking van technologie in het algemeen, en het internet in bijzonder op de manier waarop macht in de hedendaagse samenleving vorm krijgt en gebruikt wordt, speelt een belangrijke rol in de redenen voor respondenten om zich met deze thema's bezig te houden. De respondenten zijn enthousiast over wat technologie en het internet voor mogelijkheden kan bieden en maken daar ook graag gebruik van. Echter zien de respondenten ontwikkelingen op het gebied van technologie en het internet die als minder positief worden ervaren. Joris geeft een omschrijving van de groep activisten die het belang van de bescherming van privacy en persoonsgegevens duidelijk proberen te maken, en waaronder hij zichzelf schaart:

"Het is een heel technologisch gedreven groep. Het zijn mensen die goed begrijpen wat internet eigenlijk inhoudt en het zijn geen techno optimisten. Het zijn mensen die begrijpen dat je heel veel baat kunt hebben bij dingen als internet, maar die ook vaak teleurgesteld zijn. Deels. Die vroeger, halverwege de jaren '90, heel optimistisch waren over de kansen dat internet de mensheid vrij zou maken, maar daarin wel echt teleurgesteld zijn. Maar die vaak ook veel langer wel hebben gezien dat het internet ook wel veel mogelijkheden heeft om, nou, controle te verhogen basically."

Hoewel deze beschrijving zich niet alleen richt op personen die zich met Bits of Freedom identificeren, maar ook op personen die zich buiten Bits of Freedom inzetten voor deze thema's laat het wel zien welke tweedeling de meeste respondenten ervaren als het om de mogelijkheden en ontwikkelingen van technologie gaat. Technologische ontwikkelingen en het internet hebben het leven volgens de respondenten een stuk makkelijker, leuker en productiever gemaakt. Het feit dat er tegenwoordig grote hoeveelheden informatie gedeeld en geanalyseerd kunnen worden, brengt vele voordelen met zich mee. Aan de andere kant zorgt de veelheid aan gegevens er ook voor dat volgens

de respondenten de mogelijkheden tot controle toenemen. Joris gebruikt het volgende voorbeeld om uit te leggen hoe gegevens bijdragen aan die mogelijkheden:

"*Ze hebben een tool die mondiaal tracked of er griepepidemieën plaatsvinden. Dat is heel handig. Dat is natuurlijk fantastisch. Dat is big data in actie. Daar heb je op zich wat aan. Maar dat betekent dus ook dat ze allemaal individueel weten dat mensen de griep hebben*."

Als Joris spreekt over 'ze' doelt hij op overheden en bedrijven die steeds meer waarde hechten aan dergelijke gegevens, en daar tevens steeds meer gebruik van willen maken. Deze opvatting is bij andere respondenten niet anders. En hoewel deze ontwikkeling zich niet tot het internet beperkt, is het volgens de respondenten wel de plaats waar het meest zichtbaar wordt welke processen er gaande zijn. Het internet is aan het veranderen. Volgens Paul proberen overheden meer en meer grip te krijgen op het internet en de manier waarop het internet werkt. Volgens hem liggen zowel goede als minder goede bedoelingen daaraan ten grondslag. Het zijn echter vooral de onbedoelde bijeffecten die van belang zijn. Hans legt een, voor de respondenten, belangrijk bijeffect uit:

"*Want je ziet internet nu een beweging maken, of de politieke wereld maakt een beweging, dat alles op internet getraceerd zou kunnen moeten worden op personen. Dat altijd als je iets doet op internet jouw naam erbij komt te staan. Omdat je dan minder rottige dingen krijgt op internet*."

De nadruk op risicobeperking en controle wordt vooral in verband gebracht met overheden. Bedrijven dragen echter ook bij aan veranderingen die waargenomen worden op het internet. Tim stelt dat het internet steeds meer beheerst wordt door bedrijven die simpelweg geld willen verdienen. En hoewel hij daar als "*commercieel figuur*" op zich niets op tegen heeft, ziet hij wel dat het voor een bepaald accent op informatie zorgt. De nadruk op controle en risico beheersing alsmede het nieuwe belang van informatie zijn de centrale oorzaken die de respondenten aandragen voor de negatieve ontwikkelingen op het gebied van technologie en het internet. Deze ontwikkelingen hebben, zo stellen respondenten, grote gevolgen voor zaken als de vrije toegang tot informatie, de vrijheid van meningsuiting en privacy. Het voornaamste argument dat respondenten aandragen is dat hoe meer bedrijven en overheden het internet willen beheersen, en informatie willen verzamelen, hoe meer het vrije karakter van het internet alsmede de vrije toegang tot informatie in het geding komen. Vanuit deze constatering benadrukken respondenten het belang van organisaties zoals Bits of Freedom om aandacht te vragen voor de beschreven ontwikkelingen. Bits of Freedom wordt daarbij gezien als een goed doel die een nodige lobby voert. Ageeth legt uit waarom deze lobby volgens de respondenten zo nodig is:

"*Omdat het een niche is die heel erg weinig aandacht nog krijgt, terwijl het gaat over iets waar we allemaal zonder enige uitzondering 24 uur per dag mee geconfronteerd worden*."

Vanuit deze algemene achtergrond komen een drietal specifieke zorgen naar voren die ik hieronder zal beschrijven. Deze zorgen moeten worden opgevat als de voornaamste onderdelen van de ervaren problematiek met betrekking tot de verzameling van persoonsgegevens en de nadruk op risicobeperking. De zorgen zijn zowel met elkaar, als met de bovenstaande achtergrond verbonden.

4.2 Informatie is macht: de afhankelijkheid van de grote spelers

Een eerste centrale zorg die respondenten benoemen heeft betrekking op een mate van macht die de verzameling van persoonsgegevens, en de daaruit voortkomende kennis, met zich mee brengt. Overheden en bedrijven die gegevens over personen verzamelen kunnen die informatie voor vele doeleinden gebruiken. Op welke manier zij dat doen is een belangrijk onderdeel van deze zorg. Als het gaat om overheden gaan respondenten er over het algemeen vanuit dat er geen kwade opzet in het spel is. Hoewel de mate van de verzameling, alsmede de manieren waarop die verzameling onopgemerkt plaatsvindt vaak wel als problematisch wordt gezien, is de intentie van overheden om die gegevens te verzamelen volgens de respondenten niet per definitie een slechte[9]. Volgens Paul willen overheden vooral goede dingen doen met dergelijke gegevens. Echter, zo stelt hij, is er te weinig toezicht en transparantie. Paul werkt voor de overheid en geeft aan dat er pas in het begin van vorig jaar (2012) een privacyreglement is opgesteld binnen de ondernemingsraad[10]. Het gebrek aan transparantie en toezicht komt vooral voort uit de opvatting dat politici en beleidsmakers volgens de respondenten te weinig kennis bezitten op het gebied van technologie en het internet:

"Het probleem is gewoon, mensen in de Tweede Kamer hebben echt nul verstand van technologie. Die snappen echt geen flikker van wat het internet is zeg maar. En die snappen ook totaal niet, weten gewoon eigenlijk niet waar ze mee bezig zijn." (Sophie)

Als het gaat om bedrijven is het niet zozeer een gebrek aan kennis als wel een gebrek aan integriteit met betrekking tot de omgang met die gegevens wat het probleem is. De macht die voortkomt uit het beschikken over gegevens wordt volgens de respondenten vooral ingezet voor economisch gewin. Sophie gaat verder:

[9] De interviews zijn gehouden voor de onthullingen van Edward Snowden in juni 2013 en de ophef omtrent de brief van minister Plasterk en minister Hennis-Plasschaert in februari 2014 over het verzamelen van telefoonverkeer door de Nationale Sigint Organisatie (NSO).

[10] Dit privacyreglement heeft specifiek betrekking op de afdeling waar de respondent werkzaam is, en niet op de overheid als geheel.

"*Dat klinkt wat linksig misschien, maar die [bedrijven] zijn erop uit om winst te maken, en dat zullen ze doen over jouw rug als dat nodig is. Dat is wel hoe het werkt zeg maar. Tenzij burgers opstaan en zeggen: dit is de grens. Want binnen de grenzen die wij bedrijven stellen, zullen zij het spel spelen*."

Vooral de afhankelijkheid die respondenten ervaren met betrekking tot overheden die gebruik maken van persoonsgegevens komt in de gesprekken vaak naar voren. De intentie is daarbij niet zozeer het probleem. Het monopolistische karakter, en de daaruit voortkomende gedwongen afhankelijkheid is dat wel. Het invoeren van het paspoort met vingerafdruk is een veelgenoemd voorbeeld van deze ervaren gedwongen afhankelijkheid. Bedrijven zijn daarmee niet gevrijwaard van dergelijke kritiek, alleen wordt er vaak aangegeven dat consumenten tot op zekere hoogte nog de keuze hebben om wel of geen gebruik te maken van hun diensten. Als het gaat om het internet wordt er gewezen op het feit dat daar gegevens worden verzameld zonder dat personen dit merken of weten. Het feit dat bedrijven en overheden gegevens verzamelen is voor de meeste respondenten niet zozeer een probleem. Het gaat de respondenten vooral om de onnodige veelheid van de verzameling alsmede de onzichtbare en onbenullige omgang ervan.

"*Er wordt veel informatie opgeslagen waarvan ik denk van: nou, is dat nou wel, is dat nodig qua informatie? Waarom is het niet inzichtelijk wat ermee gedaan wordt?*" (Henk)

We zien op dit punt overeenkomsten met wat Schneier (2012) beschrijft als het nieuw feodalisme waarbij burgers geen inzicht hebben in de manier waarop grote spelers onze digitale gegevens beheren. Echter gaat het de respondenten niet alleen om de afhankelijkheid met betrekking tot wat Schneider noemt de *Feudal Lords*. Ook de afhankelijkheid van de gegevens zelf speelt hier een rol. Hans geeft het voorbeeld dat de politie eenvoudig kan nagaan waar zijn telefoon is. Echter wil dat volgens Hans nog niet zeggen dat hij daar dan ook is. Hans wijst hiermee op het hercontextualiseren van gegevens zoals besproken in het rapport van de WRR (2011). Jan-Willem beschrijft ook de afhankelijkheid van beslissingen en interpretaties die gemaakt kunnen worden op basis van dergelijke gehercontextualiseerde gegevens:

"*Mensen worden toch in blokjes geplaatst door zo'n computer, en dan kan je toch zomaar in het verkeerde blokje terecht komen, en dat kan dan verderop voor een ander computerprogramma weer andere gevolgen hebben*."

Een ander voorbeeld dat regelmatig gegeven wordt, is dat gegevens zoals bijvoorbeeld elektronische patiëntendossiers mogelijk gehackt kunnen worden, of via slinkse achterdeuren in de handen kunnen komen van zorgverzekeraars. Zorgverzekeraars kunnen op basis van die informatie mogelijk premies voor zorgverzekeringen verhogen, of zelfs personen weigeren. We zien hier een vergelijking met wat

de WRR als een ander gevolg van het ontstaan van de iOverheid heeft omschreven. Volgens het rapport moeten burgers er rekening mee houden dat hun gegevens, zowel in publieke als private handen, een eigen leven kunnen gaan leiden (WRR, 2011). Naast dat dit de ervaren afhankelijkheid van de omgang en bescherming van persoonsgegevens benadrukt, raakt het ook aan de tweede zorg die respondenten benoemen. Daarbij gaat het niet zozeer om het feit dat gegevens op korte termijn een eigen leven kunnen gaan leiden, maar meer om de manieren waarop de opgeslagen gegevens in de toekomst problemen kunnen opleveren.

4.3 Onbekende gevolgen: het toekomstige gevaar van de function creep

De tweede zorg die respondenten noemen heeft betrekking op de gevolgen van de opslag van persoonsgegevens voor de toekomst. De kern van deze zorgt betreft het feit dat gegevens bij overheden en bedrijven, alsmede gegevens die personen zelf toevoegen via het internet en de sociale media, volgens de respondenten nooit meer zullen verdwijnen. Dennis legt uit:

"*We zitten nu in een tijdsgewricht waar een hoop dingen aan de hand zijn, maar we zitten absoluut niet in een dictatuur. Wat dat betreft valt het allemaal wel mee. Wie zegt dat dat over 10 of 20 jaar ook zo is? Dat weten we eigenlijk helemaal niet. We zien regelmatig in de wereld dat dingen kunnen veranderen, en niet altijd ten goede. Die gegevens zijn dan niet ineens weg*."

Vooral het idee dat er bepaalde politieke opvattingen of denkbeelden kunnen veranderen maakt dat er op langere termijn risico's zitten aan de opgeslagen gegevens. Welke veranderingen dat precies zijn blijft vaak in het midden. Simpelweg omdat het volgens de respondenten niet te voorspellen is wat die verandering zal zijn. De macht en daadkracht die de overheid heeft om dergelijke gegevens te gebruiken maakt echter dat het voor de respondenten wel een reëel risico is. Volgens Stefan doet de overheid op dit moment niet zo veel met die gegevens:

"*Wel iets, maar niet heel veel. Maar de overheid verandert elke vier jaar. En dat kan best zo radicaal veranderen eigenlijk dat die data in één keer wel gebruikt wordt op een bepaalde manier. (…) En als er straks een hetze komt tegen een bepaalde groep of religie, dan heeft de overheid de middelen om daar iets mee te doen. En als dat wel geoorloofd is, omdat de meerderheid dat vindt, gaan ze dat ook doen*."

Ook hier komt naar voren dat de respondenten afhankelijk zijn van de ontwikkelingen waarop zij geen invloed hebben. Het gebrek aan invloed heeft wederom raakvlakken met de afhankelijkheid van de grote digitale spelers waarop Schneier (2012) ons wijst. Echter gaat het bij deze tweede zorg niet enkel over de manier waarop deze grote spelers de gegevens beveiligen. De zorg richt zich tevens op de manieren waarop die gegevens gebruikt kunnen gaan worden. Hans wijst op het feit dat de enige invloed die wij hebben het kiezen van de personen die ons vertegenwoordigen in het parlement

betreft. Daarna houdt het volgens hem op. Juist wat er daarna met de gegevens kan gebeuren staat bij deze tweede zorg centraal. Ageeth wijst op het idee van digitale oorlogsvoering waarbij volgens haar de mogelijkheden en kennis al bestaan dat landen op grote schaal technologische systemen 'op zwart' kunnen gooien. De controle daarop is volgens Ageeth echter minimaal. Zowel Tim en Stefan wijzen met enige nadruk op de gevoeligheid van het onderwerp op de rol die de Gemeentelijke Basis Administratie heeft gespeeld in de Tweede Wereldoorlog. Ze gebruiken dit als voorbeeld om aan te tonen hoe opgeslagen gegevens gebruikt kunnen worden op manieren waarvoor die gegevens nooit verzameld zijn. De bovenstaande zorg kent zo overeenkomsten met wat vaak "*function creep"* wordt genoemd. Volgens het Surveillance Studies Network (2006: 9) refereert function creep aan veranderingen in, en toevoegingen aan het gebruik van technologie waarbij persoonlijke gegevens verzameld voor één doel en één functie migreren naar andere doelen en functies die surveillance en de inbreuk op privacy uitbreiden en intensifiëren voorbij het eerder sociaal, ethisch en wettelijk geaccepteerd punt. Hoewel het hercontextualiseren van gegevens en de mogelijkheid tot het gaan leiden van een eigen leven van gegevens uit de eerste zorg raakvlakken heeft met de function creep, is het verschil dat bij de eerste zorg vooral de hedendaagse afhankelijkheid van fouten, beveiliging en onbenullige omgang centraal staan, terwijl de tweede zorg zich vooral richt op het moedwillig en toekomstig misbruiken van gegevens. De derde zorg richt zich niet zozeer op de gevolgen van de verzameling van persoonsgegevens, maar heeft betrekking op het onzichtbare karakter van de besproken processen en een gebrek aan alertheid daarop. Deze zorg wordt beschreven in de volgende paragraaf.

4.4 Het gebrek aan openheid & alertheid: de kikker in de pan

De derde zorg heeft betrekking op een algeheel gebrek aan alertheid op de vergaande processen van de verzameling van allerhande persoonsgegevens. We zagen eerder al dat er volgens de respondenten een gebrek aan kennis aan beleidsmakers en politici wordt toegeschreven en dat de openheid bij zowel overheden als bedrijven met betrekking tot de omgang van persoonsgegevens volgens de respondenten te wensen over laat. Juist door het feit dat niet inzichtelijk is hoe deze processen plaats vinden, stellen de respondenten dat de massa, en voor een deel ook politici, een alertheid missen op de besproken onderwerpen. Alle respondenten beschrijven dit gebrek aan alertheid. Drie respondenten gebruiken hiervoor de metafoor van de kikker in de pan. Tim legt uit:

"Wat dat betreft, nou niet zozeer incapabelheid, maar meer afwezigheid van alertheid. Er is een mooi metafoor. Zet een kikker in een pan met water en zet dan het water op laag vuur. Het water verhit heel langzaam, en de kikker blijft zitten. Uiteindelijk is het te warm en gaat de kikker dood. Maar de kikker blijft in het water zitten omdat hij eigenlijk de verandering niet merkt. Maar een kikker die je in een pan met heet water gooit springt er meteen weer uit."

Met de voorgaande metafoor wordt vooral getracht duidelijk te maken dat de massa niet merkt hoe omvangrijk de processen van de verzameling van persoonsgegevens eigenlijk zijn omdat deze vrijwel onopgemerkt, en stapje voor stapje, voortschrijden en uitbreiden. Sophie licht toe:

"In je eigen leven heb je er veel meer controle over. Als je tegenover iemand zit is het veel makkelijker om aan te voelen wat je wel en niet zegt, zeg maar. Alleen als je op internet bent, en dat is ook het nare en valse van Facebook en Google en zo, dan gaat het allemaal veel makkelijker of zo. Ik heb soms wel het gevoel dat we een kikker in de pan zijn, die langzaam aan het kapot koken is."

Het gebrek aan openheid en alertheid draagt volgens de respondenten bij aan zowel de risico's die de verzameling van persoonsgegevens met zich mee brengen alsmede de afhankelijkheid van diezelfde gegevens. De respondenten benadrukken vooral de snelheid waarmee wij onszelf hebben verbonden met technologie, het internet en onze smartphones zonder daarbij genoeg na te denken over de gevolgen daarvan en de manieren waarop gegevens die voortkomen uit deze alledaagse handelingen gebruikt worden. Hoewel die gevolgen, als we naar Bits of Freedom kijken, te maken hebben met en besproken worden in termen van privacy, is het hier niet besproken als centrale zorg van de respondenten. Waarom dat is wordt in de volgende paragraaf beschreven.

4.5 Het containerbegrip privacy

Het feit dat privacy niet als centrale zorg is opgenomen lijkt vreemd omdat het een belangrijk onderwerp is als het gaat om gevolgen van de verzameling van persoonsgegevens in het bijzonder alsmede surveillance en digitalisering in het algemeen. Hoewel de respondenten vaak het begrip privacy gebruiken bij het beschrijven van hun zorgen valt op dat de term vooral gebruikt wordt als containerbegrip om te verwijzen naar de verzameling van zorgen en problemen in relatie tot wetgeving en politieke discussies.

"Overigens ben ik wel van mening dat privacy gewaarborgd moet worden in de wet, zodat je dus met verzekeringen, met rechtszaken, met dat soort dingen, dat je daarin gewoon veilig bent. Maar in het algemene verkeer bestaat het eigenlijk gewoon niet meer." (Roderik)

Naast het feit dat het begrip privacy vooral gebruikt wordt als containerbegrip lijken er opvattingen bij de respondenten te bestaan waarin persoonlijke privacy steeds minder mogelijk wordt geacht, of simpelweg niet meer bestaat. Negen respondenten hebben dergelijke denkbeelden waarvan er vier tevens stellen dat privacy in de toekomst niet meer van belang is, of een andere betekenis zal krijgen. Volgens Paul is privacy alleen nog mogelijk als je in een geheel zelfvoorzienende grot in de rimboe gaat wonen. Als je een normaal leven wil leiden, dan zijn er volgens Paul gegevens over je bekend. Daar kan je volgens hem niet omheen. Stefan zegt over privacy op het internet het volgende:

"*Dat kan niet. Dat kan uiteindelijk niet. Want het is gewoon buiten. Je kunt ook niet zeggen: ik wil privacy buiten. Het is gewoon een open wereld. Maar natuurlijk kan je wel, je kan wel gesloten omgevingen creëren in die wereld. Maar uiteindelijk staat het ergens opgeslagen. Fysiek. Dus privacy kan je nooit garanderen, dat kan niet. Dat is onmogelijk denk ik.*"

Van de overige respondenten stellen er twee dat privacy in de toekomst wellicht mogelijk is zolang men ervoor wil betalen. De laatste zes respondenten stellen dat privacy technisch gezien wellicht mogelijk is, maar dat daarvoor grote veranderingen moeten plaatsvinden en dat het nog maar de vraag is of dat ook daadwerkelijk zal gebeuren. Ik wil hier benadrukken dat de respondenten privacy wel degelijk belangrijk vinden. Vooral in de maatschappelijke en politieke discussies zien de respondenten de waarde en relevantie van het begrip in. Op persoonlijk vlak geven vrijwel alle respondenten echter aan het moeilijk te vinden een goede definitie van privacy te geven. Drie respondenten beschrijven privacy in termen van vrijheid, met rust gelaten worden of jezelf kunnen zijn. Vier respondenten beschrijven het in termen van het hebben van een privé domein. De overige tien respondenten beschrijven privacy in termen van controle over eigen persoonsgegevens. Opvallend is dat bij de zorgen van respondenten het gebrek aan die controle een rol lijkt te spelen. Of het nu gaat om de macht die bedrijven en overheden hebben op basis van de verzameling van persoonsgegevens, de mate van afhankelijkheid van de omgang en bescherming of het gebrek aan alertheid bij de massa; het feit dat respondenten weinig invloed lijken te hebben komt bij elk van die zorgen in meer of mindere mate terug.

Bij het ontwerpen van dit onderzoek en het ontwikkelen van de probleemstelling heeft de verwachting dat personen die zich met Bits of Freedom identificeren een oppositioneel bewustzijn richting de surveillant assemblage hebben een belangrijke rol gespeeld. In de volgende paragraaf wordt uiteengezet wat de resultaten met betrekking tot de zorgen van de respondenten ons kunnen leren over dit oppositioneel bewustzijn.

4.6 Het oppositioneel bewustzijn: afhankelijkheid & een gebrek aan controle

Waite (2001: 173) beschrijft het oppositioneel bewustzijn als een mentale staat van een onderdrukte groep om een systeem van menselijke dominantie te hervormen, te verwerpen of te ondermijnen. De mentale staat bestaat uit het identificeren met leden van een groep, het herkennen van onrecht tegenover die groep alsmede het herkennen van gedeelde groepsbelangen om dat onrecht te beëindigen. In deze scriptie gebruik ik het oppositioneel bewustzijn om te verwijzen naar gedeelde opvattingen, identiteiten en conflicten met betrekking tot de surveillant assemblage van waaruit personen een noodzaak ervaren om in actie te komen. De gedeelde opvattingen van de respondenten hebben betrekking op de tweedeling tussen enerzijds de kansen en mogelijkheden van

technologie en het internet en anderzijds de manieren waarop die kansen en mogelijkheden gebruikt worden. Vooral de nadruk op risicobeperking, beheersing van het internet en het accent op persoonsgegevens die als gevolg daarvan zijn ontstaan brengen het vrije karakter van het internet en de vrije toegang tot informatie in gevaar. De conflicten of zorgen die de respondenten ervaren richten zich op de manieren waarop bedrijven en overheden met persoonsgegevens omgaan, de risico's die zowel op korte als lange termijn daaruit voortkomen en het gebrek aan alertheid en kennis bij overheden en de massa op deze ontwikkelingen. Dit alles resulteert in een gedeelde identiteit van de respondenten die zich laat kenmerken door een afhankelijkheid van de grote spelers op het gebied van de verzameling van persoonsgegevens. Privacy heeft voor de meeste respondenten betrekking op een mate van controle over persoonsgegeven. Dit is interessant omdat juist een gebrek aan controle, zowel in de omgang door derden als persoonlijke controle over eigen persoonsgegevens, in meer of mindere mate als een rode draad door de zorgen heen loopt. De noodzaak die respondenten aandragen om in actie te komen komt voort uit deze bovenstaande punten. Zij zien Bits of Freedom vooral als een goed doel dat de nodige aandacht vraagt voor deze thema's. Daarnaast geven respondenten aan zelf ook bepaalde handelingen uit te voeren vanuit het zojuist beschreven oppositioneel bewustzijn. Welke dat zijn wordt in het volgende hoofdstuk beschreven.

Hoofdstuk 5: Reacties op de surveillant assemblage

In dit hoofdstuk worden de individueel-collectieve alsmede de individuele reacties van respondenten op de surveillant assemblage beschreven. Daarnaast wordt er gewerkt naar een ideaaltypische indeling van individuele strategieën die de respondenten hanteren in het dagelijks leven. Het is aan het begin van dit hoofdstuk van belang te herinneren aan de manier waarop ik in deze scriptie individueel-collectieve en individuele reacties operationaliseer. Zoals beschreven in paragraaf 2.2 doe ik dit op basis van het doel van de reactie. Reacties die enkel een persoonlijk doel voor ogen hebben zie ik als individuele reacties. Reacties die het individuele doel overstijgen en gericht zijn op de collectieve doelen en conflicten van georganiseerde collectieve reacties zie ik als individueel-collectieve reacties. Deze individueel-collectieve reacties verschillen van de puur collectieve reacties omdat zij plaats vinden in een niet georganiseerde context en bestaan uit individuele handelingen.

In paragraaf 5.1 komen twee individueel-collectieve reacties aan bod. In deze paragraaf wordt beschreven hoe de respondenten zich in het dagelijks leven bezig houden met een *bewustwordingsmissie* en een *politieke lobby*. Paragraaf 5.2 richt zich op drie strategieën van individuele reacties. Er wordt in deze paragraaf beschreven dat de drie strategieën respectievelijk bestaan uit het zo veel mogelijk proberen te *minimaliseren* van het vrijgeven van persoonsgegevens, het *managen* van persoonsgegevens en online identiteiten of het *reflecteren* over gegevens die respondenten zelf bijdragen aan de surveillant assemblage. In paragraaf 5.3 worden de individuele reacties in een figuur weergegeven, en wordt een kanttekening geplaatst bij de ervaren invloed en effectiviteit van de beschreven reacties.

5.1 Individueel-collectieve reacties

5.1.1 De bewustwordingsmissie

De meest voorkomende individueel-collectieve reactie betreft het creëren van bewustwording over de in hoofdstuk vier behandelde onderwerpen. Op een enkeling na is iedere respondent in meer of mindere mate actief bezig om kennis en alertheid over deze thema's te verspreiden. De respondenten richten zich daarbij vooral op hun directe sociale omgeving. Zoals Karel laat zien ligt de nadruk daarbij niet zozeer op het winnen van zieltjes:

"*Als je een goeie vriend van me bent ontkom je er niet aan, zeg maar, om daar af en toe wat over te horen. Dan merk ik wel, niet dat ze me in alles gelijk geven, sommigen zeggen: ja je hebt wel gelijk maar ik vind het zelf niet zo ernstig. Prima. Maar ik vind het in ieder geval belangrijk dat de mensen het weten*."

In de sociale omgeving gaat het vooral om het verspreiden van tips om specifieke gevaren te beperken. Tim legt uit dat hij zijn familie en schoonouders een dringend verzoek heeft gedaan tot het

aanpassen van de privacyinstellingen op Facebook toen Graph Search[11] uitkwam. Volgens Tim is Graph Search redelijk eng, en vond hij het daarom belangrijk dat de instellingen ook daadwerkelijk werden aangepast. Respondenten geven aan dat het in de sociale omgeving niet altijd gemakkelijk is om de boodschap over te brengen. Volgens Hans zijn veel mensen namelijk enorm allergisch om daar over te praten, en is het voor veel mensen geen issue. De respondenten zijn daardoor over het algemeen voorzichtig om het over deze onderwerpen te hebben. Sophie legt kort en bondig uit waarom dat is:

"*Ik ben altijd een beetje bang om die vervelende zeikerd te zijn zeg maar, die altijd aan het azijn pissen is over hoe slecht alles is*."

In de professionele omgeving zijn de respondenten echter een stuk minder terughoudend. Vanuit de zorg dat de massa te weinig kennis heeft, proberen zij daar waar het kan te wijzen op de risico's en bewustwording te bewerkstelligen. Gabriëlla geeft aan hoe dat in zijn werk gaat:

"*Als ikzelf met mensen spreek, en ik heb zelf ook wat talks en workshops gegeven, heb ik ook altijd een voorlichting over: denk erom wat je op social media zet. Of je überhaupt je GPS coördinaten bijvoorbeeld meestuurt. Dat soort hele concrete voorbeelden, dat is belangrijk en ik denk ook voor jongeren op scholen bijvoorbeeld. Ik weet niet precies wat de invulling zou moeten zijn, maar voorlichting is wel belangrijk. (…) Sowieso om te zorgen dat heel veel mensen het weten, want hoe meer mensen het weten, over het algemeen, hoe meer mensen het vervelend vinden en dus hoe groter de kans is dat er ook wat aan gedaan kan worden*."

Ongeveer een kwart van de respondenten heeft een beroep waarbij zij zich vrij direct bezig houden met zaken als privacy, beveiliging van informatie technologieën en persoonsgegevens. Zij kunnen zo relatief gezien efficiënter zijn in het overbrengen van de boodschap. Dit omdat zij met personen en organisaties van doen hebben die tot op zekere hoogte invloed hebben op, of zich bezig houden met de beschreven problematiek. De overige respondenten staan wat betreft hun beroep iets verder af van het spreekwoordelijke vuur. Desalniettemin proberen zij hun steentje bij te dragen. Het complexe karakter van de problematiek, alsmede het gebrek een kennis in de professionele sfeer van deze respondenten maakt dat dit niet altijd even soepel verloopt.

[11] Graph Search van Facebook baseert zoekresultaten op alle informatie die personen met anderen hebben gedeeld op Facebook. Een gelijke zoekopdracht door twee gebruikers zal zo verschillende resultaten opleveren. Deze interne zoekfunctie geeft de mogelijkheid om naast het zoeken naar personen ook te zoeken naar bijvoorbeeld vrienden die in een bepaalde stad wonen, een specifieke activiteit leuk vinden of foto's waar bepaalde vrienden op te zien zijn.

"Ik adviseer heel veel klanten wel op het gebied van sociale media. En ik raad ze wel aan: wees oprecht, wees jezelf en pas op voor dingen. (...) Ik denk dat ik een goed beeld heb van wat er gebeurt op dit gebied, maar ik krijg het niet uitgelegd." (Roderik)

Juist omdat de respondenten naar eigen zeggen niet altijd optimaal hun boodschap over kunnen brengen, steunen zij daarnaast personen of organisaties die zich bezighouden met de politieke lobby voor privacy en de bescherming van persoonsgegevens. Hoe zij dat doen wordt in de volgende paragraaf beschreven.

5.1.2 De politieke lobby

Naast het creëren van bewustwording in de sociale en professionele sfeer ondersteunen de respondenten, zij het in iets mindere mate, organisaties en personen die zich bezig houden met privacy en de bescherming van persoonsgegevens. Als het gaat om Bits of Freedom bestaat deze steun voornamelijk uit donaties, het publiekelijk fan zijn, het beheren van een digitaal archief, het aandragen van informatie, het ontwikkelen van software en grafische ontwerpen voor de website of het controleren van beleidsstukken en brieven aan de Tweede Kamer. Bits of Freedom heeft een mailinglijst waarmee zij geregeld aan hun vrijwilligers vragen dergelijke klusjes uit te voeren. Daar waar het mogelijk is helpen de respondenten met die klusjes. Het gaat daarbij vaak om wat Jan-Willem noemt "*de kleinere klusjes*". Het doel waarmee respondenten Bits of Freedom ondersteunen is tweeledig. Enerzijds heeft het betrekking op de hierboven besproken bewustwording.

"Ik dacht: misschien kan Bits of Freedom er wat mee. En uiteindelijk hebben ze dat ook op hun website gezet inderdaad. Nou, ik dacht misschien kan dit, helpt dit ze om mensen even mee wakker te schudden." (Jan-Willem)

Naast het creëren van bewustwording gaat het de respondenten anderzijds ook om het bijstaan van Bits of Freedom in hun lobby om privacy te beschermen. Gabriëlla geeft aan Bits of Freedom te helpen om privacy te beschermen tegenover bedrijven die dat niet zo belangrijk vinden. Zij stelt dat zij zelf in bepaalde gevallen haar privacy kan beschermen, maar als de overheid bepaalt dat zij bijvoorbeeld haar vingerafdrukken moet afgeven zij daar niet zo veel aan kan doen. Vooral het idee dat Bits of Freedom daadwerkelijk verandering kan bewerkstelligen is voor de respondenten een belangrijke reden voor hun steun. Kevin licht toe:

"*In je eentje kan je niet zo heel veel doen, dus scharen achter een beweging. Het is goed dat zij plannen hebben waar ik mij als gebruiker bij aan kan sluiten*."

Een klein deel van de respondenten legt zich niet neer bij deze individuele onmacht en zoekt manieren om persoonlijk toch iets te kunnen betekenen voor de problemen die zij zien op het gebied

van privacy en persoonsgegevens. Zij voeren wat lijkt een individuele politieke lobby. Paul legt uit wat hij doet en waarom:

"Ik vind het gewoon leuk om daar vrijwilligerswerk voor te doen. Dat wel. Maar het is niet exclusief Bits of Freedom. Via Twitter heb ik ook wel contacten af en toe met anderen, daar geef ik ook weleens tips aan. Toen [naam opzettelijk weg gelaten] nog in het Europarlement zat, die deed ook vrij veel op dit gebied, dus die stuurde ik ook nog wel eens een tip toe. (…) Daar zit je wel het makkelijkst op invloed ja. Dat zijn wel mensen die er rechtstreeks mee te maken hebben en die ook daadwerkelijk wat kunnen uitoefenen op de regelgeving. (…) Ik denk dat het meer invloed heeft als ik op een gegeven moment even een linkje over datamisbruik naar een Europarlementslid stuur, of naar onze vriend van de piratenpartij, dat heeft meer invloed dan als ik heel hard ga roepen van euh ze zijn gemeen."

Ook Dennis werkt samen met een politicus. Hij is ten tijde van ons gesprek bezig met het opstellen van Kamervragen over een privacy gerelateerd onderwerp waar hij in zijn dagelijks professionele leven vaak tegen aan loopt. Vanuit zijn frustratie over dit onderwerp besloot hij iets te willen doen en te bekijken of hij in zijn eentje wat kon bereiken. De meeste respondenten houden het echter bij het creëren van bewustwording en het steunen van organisaties die zich mengen in de politieke lobby voor privacy en de bescherming van persoonsgegevens.

Omdat beide doelen van deze reacties het persoonlijke niveau overstijgen en gericht zijn op het verbeteren van de situatie voor de samenleving als geheel vanuit de collectieve doelen en de gedeelde ervaren problematiek die Bits of Freedom centraal stelt, zijn ze in deze scriptie beschreven als individueel-collectieve reacties. De opvatting dat respondenten zelf weinig invloed hebben op dit grote geheel komt meermaals naar voren als argument om organisaties of personen die dat wel hebben te steunen. Uit de gesprekken zijn echter ook reacties naar voren gekomen die zich puur richten op het individuele vlak. Het zijn manieren waarop de respondenten in het dagelijks leven omgaan met ervaren risico's en gevaren voor henzelf die voortkomen uit de surveillant assemblage. Deze reacties worden in de volgende paragraaf beschreven.

5.2 Individuele reacties

De individuele reacties die hieronder worden beschreven hebben betrekking op het dagelijks leven van de respondenten. Het zijn handelingen die respondenten doen of laten vanuit de eerder beschreven zorgen. De reacties richten zich op een breed scala van onderdelen van de surveillant assemblage. Zo kunnen reacties betrekking hebben op persoonsgegevens, de manieren waarop die verzameld worden alsmede de databanken van overheden en bedrijven waarin die gegevens opgeslagen staan. Daarnaast hebben reacties ook betrekking op het internet en sociale media, de gegevens die de respondenten daar zelf aan toevoegen en de manieren waarop die gegevens

gebruikt (kunnen) worden door anderen. De reacties worden weergegeven als ideaaltypische strategieën. Deze strategieën bestaan uit de vorm van de reacties en het doel waarmee de respondenten deze reacties bezigen. Het zal duidelijk worden dat de strategieën kunnen worden geplaatst op een schaal waarbij de intensiteit van de maatregelen alsmede de intentie van het voorkomen of beperken van het vrijgeven van persoonsgegevens afneemt. Om een en ander te verduidelijken zal aan het einde van deze paragraaf deze schaal worden weergegeven in een figuur. Omdat het hier een ideaaltypische indeling betreft, moet worden herinnerd aan het feit dat bepaalde onderdelen worden benadrukt terwijl andere onderdelen worden veronachtzaamd. Dit wil zeggen dat in de empirie deze strategieën minder duidelijk van elkaar te onderscheiden zijn en op bepaalde punten elkaar overlappen. Om een eerste indruk te krijgen van de verschillende strategieën wordt hieronder het eerste deel van de figuur weergegeven.

Figuur 2: Overzicht individuele reacties op de surveillant assemblage

	Strategie 1	Strategie 2	Strategie 3
Vorm	Minimaliseren	Managen	Reflecteren
Intensiteit	Hoog	Gemiddeld	Laag

5.2.1 Minimaliseren van gegevens

Ongeveer één derde van de respondenten geeft aan op verschillende manieren het bijdragen of loslaten van persoonsgegevens zo veel mogelijk te minimaliseren. Dat wil niet zeggen dat de respondenten geen gebruik maken van het internet en compleet 'off the grid' leven, maar ze geven zowel in het online als offline dagelijks leven bepaalde gemakken op om zo min mogelijk digitale sporen achter te laten. Op het internet mijden deze respondenten zo veel mogelijk de grote spelers die erom bekend staan veelvuldig (persoons)gegevens te verzamelen. Gratis diensten van bedrijven als Google en Facebook worden derhalve niet gebruikt. In plaats daarvan gebruiken de respondenten alternatieve oplossingen waar de dataverzamelaars niet bij kunnen. Karel legt uit:

"*Google gebruik ik niet, ook geen webmail-achtig iets. Ik ben informaticus, ik heb mijn eigen server aan het internet hangen. Een VPS. Een virtuele server en daar staat dus mijn mail op. Op mijn eigen server waar niemand anders bij komt.*"

Andere voorbeelden zijn het versleutelen van e-mailverkeer, het gebruiken van privacy verhogende software, het uitschakelen of omzeilen van cookies en online trackers en het gebruik maken van

verbindingen zoals TOR en VPN. TOR staat voor The Onion Router en is een privacyvriendelijk manier om het internet te gebruiken. Het TOR netwerk zoekt op een willekeurige manier, gebruik makend van drievoudige versleuteling, anoniem een weg naar het internet. Het is daardoor zeer lastig om de internetgebruiker te herleiden. VPN staat voor Virtual Private Network en bestaat uit een versleutelde verbinding met een beveiligd netwerk waarmee men vervolgens het internet op kan. Een VPN is echter minder anoniem dan een TOR netwerk[12]. De respondenten bewegen zich zo anoniem mogelijk op het internet om zo de bijdrage aan dataverzameling te minimaliseren. Daarnaast worden ook in het dagelijks offline leven maatregelen getroffen om het loslaten van gegevens te beperken en de digitale sporen van dagelijkse handelingen te minimaliseren. Gabriëlla laat zien op wat voor zaken dat zoal betrekking heeft:

"*Ik reis met een anonieme OV chipkaart. Die laad ik ook alleen op met cash geld bij de balie, want anders is mijn pin eraan gekoppeld. En daarbij ga ik er nog vanuit dat de camera's niet gebruikt worden, want anders zou ik ook nog met een masker op moeten lopen. Dat doe ik dan weer net niet, maar voor zover ik weet is die chipkaart helemaal niet gekoppeld aan mij. Daarnaast heb ik een Migo telefoon en een Linux telefoon, geen Adroïd, geen Apple. Dus een groot bedrijf weet niet wat het is, en het is een Open Source. Wat dat betreft kan ik misschien bepaalde spelletjes niet spelen, maar is het wel beter voor de privacy.* "

Andere voorbeelden van offline maatregelen zijn de volgende: Jan-Willem laat soms zijn telefoon thuis, Dennis zet zijn telefoon uit als hij gevoelige gesprekken over zijn activisten verleden voert en Paul heeft zichzelf en zijn kinderen uit het EPD (Elektronisch Patiënten Dossier) gehouden. Karel geeft nog voorbeeld van de soms creatieve manieren die respondenten gebruiken:

"*Expres nadat bekend werd van dat vingerafdruk op het paspoort, en mijn paspoort was nog wel geldig, maar ik heb hem toch vernieuwd. Dus in de laatste week, en dan mijn paspoort vernieuwen. Dus ik ben nog een van de laatste mensen die een paspoort zonder vingerafdruk heeft*."

Als we kijken naar de reacties op surveillance die Marx (2003) heeft beschreven zien we in het bovenstaande voorbeelden van *avoidance*, *blocking* en *breaking moves*. Respondenten ontwijken (avoidance) online de verzameling van gegevens door die systemen min of meer onklaar (breaking) te maken met verbindingen zoals TOR en VPN. De bovenstaande offline voorbeelden maken vooral gebruik van het fysiek tegen gaan (blocking) van de verzameling van gegevens die voortkomen uit offline handelingen. Naast het minimaliseren van verschillende vormen van digitale gegevens in databanken van bedrijven en overheden zijn respondenten over het algemeen voorzichtig met hun persoonsgegevens in het dagelijks leven. Het gebruik van pseudoniemen en het simpelweg liegen over persoonsgegevens of het verstrekken van foutieve gegevens zijn daarbij veel genoemde

[12] www.bof.nl/ons-werk/internetvrijheid-toolbox/.

middelen. Vanuit Marx (2003) kunnen we hier vooral spreken van *distorting* en *refusal* moves. Gabriëlla legt uit dat zij altijd vraagt waarom personen of instanties bepaalde gegevens nodig hebben. Wanneer zij het geven van deze gegevens niet nodig acht, of er te veel risico's aan vindt kleven zal ze het weigeren (refusal). Als weigeren geen mogelijkheid is geeft Gabriëlla simpelweg een valse naam op (distorting).

De vraag waarvoor de gegevens nodig zijn wordt door de respondenten gesteld vanuit de alertheid op mogelijke risico's van die gegevens. Het beperken van die risico's is daarbij een belangrijke motivatie voor de bovenstaande handelingen. Hoe meer identificeerbaar de gegevens zijn aan de respondent, hoe belangrijker zij het vinden om deze te beschermen. Echter is er nog een tweede motivatie te vinden die centraal staat bij deze strategie. Deze betreft een ideologische. Jan-Willem legt uit:

"*Nou, het gaat ze niets aan eigenlijk. Dat is het punt een beetje. Je hebt ook altijd van die mensen die zeggen: je hebt niets te verbergen. Maar ja. Waarom moeten ze het weten zou ik dan zeggen?"*

Het citaat laat zien hoe de respondenten die deze strategie hanteren reageren op het "*nothing to hide*" argument. Dit argument stelt dat als je niets strafbaars doet, je niets te vrezen hebt van dataverzameling en surveillance. Omdat personen niets te verbergen hebben verzetten zij zich niet tegen surveillance (Solove, 2007: 744-745). De respondenten draaien het argument om en vragen zich daarbij af wat de reden is van dataverzameling of surveillance. In veel gevallen is die er volgens de respondenten simpelweg niet. Hoewel de nadruk ligt op het beschermen van persoonsgegevens om risico's te beperken en de opvatting dat het 'ze' niets aan gaat, speelt ten slotte het gevoel om 'bekeken' te worden een rol. Dat gevoel heeft enerzijds betrekking op de digitale representatie van de personen door gegevens. Anderzijds gaat het ook om het letterlijk bekeken worden.

"Ik kan Rotterdam ingaan, maar ik vind het gewoon geen prettige stad met al die camera's. Ik weet gewoon dat ik continu begluurd wordt. Als je met de auto erheen rijdt, fotootje van je nummerbord en er wordt geregistreerd dat je daar bent geweest. Ook gewoon het gevoel. Dat vind ik niet prettig. Iedereen heeft een grens. Voor de meeste is dat de buitendeur van je huis. Maar ik vind het al niet prettig als je op straat begluurd wordt." (Karel)

De zojuist beschreven strategie is in termen van bescherming en beperking van persoonsgegevens de meest strenge en intensieve van de drie. De respondenten beschrijven wat lijkt op een dagtaak. De respondenten stellen in het dagelijks leven vrijwel altijd bezig te zijn vanuit deze strategie. Omdat het echter niet altijd gemakkelijk is om de strategie te handhaven bestaat die dagtaak voor een deel uit het zoeken naar manieren om zich te onttrekken aan de verzameling van persoonsgegevens. In

bepaalde gevallen is het simpelweg volgens de respondenten niet te doen. Vooral het eerder besproken monopolistische karakter van de overheid met betrekking tot het gebruik van persoonsgegevens wordt daarbij vaak genoemd.

5.2.2 Management van persoonsgegevens & identiteit

De tweede strategie, die door iets meer dan één derde van de respondenten gehanteerd wordt, richt zich niet op het zoveel mogelijk minimaliseren van digitale sporen. De nadruk van de handelingen binnen deze strategie ligt op het selectief beschermen en managen van persoonsgegevens. Er zijn twee grote verschillen te benoemen als we deze strategie met de vorige vergelijken. Ten eerste is er minder sprake van de ideologische opvatting dat het 'ze' niets aan gaat. Dat bedrijven en overheden 'meekijken' door middel van de verzameling van persoonsgegevens is niet zozeer problematisch, wat zij met die gegevens doen echter wel. De ideologische opvatting binnen deze strategie stelt niet zozeer dat de verzameling van persoonsgegevens op zich problematisch is. Vooral is oneigenlijk gebruik of misbruik van die gegevens het probleem. Frank legt uit:

"*Ik maak mij niet zo heel erg druk over wat, over wat mensen van mij weten. Dat maakt mij niet zo heel veel uit. Ik maak mij wel druk erover op het moment dat die informatie gebruikt danwel misbruikt wordt.*"

Het tweede verschil is dat er binnen deze strategie minder sprake lijkt van een dagtaak. Daar waar de respondenten die de eerste strategie hanteren vrijwel altijd en overal zich bewust zijn van de verzameling van persoonsgegevens en deze proberen te minimaliseren, doen de respondenten die de tweede strategie hanteren dit alleen in specifieke gevallen. Ze maken daarbij gebruik van dezelfde technieken en middelen als beschreven in de eerste strategie (avoidance, blocking en breaking moves). De intensiteit van deze handelingen ligt echter een stuk lager. Hans en Sophie leggen respectievelijk uit:

"Een voorbeeld zou zijn: als ik bepaalde dingen opzoek op internet, dan zet ik even mijn VPN aan. Af en toe, als ik denk dat het zo'n mooi rood vlaggetje gaat zijn als ik het niet doe, zet ik even mijn VPN aan." (Hans)

"Bepaalde dingen zoek ik alleen op als ik op TOR zit bijvoorbeeld." (Sophie)

Het rode vlaggetje van Hans, of de bepaalde dingen van Sophie hebben vooral betrekking op gegevens die verkeerd geïnterpreteerd kunnen worden of nadelige gevolgen voor de respondenten kunnen hebben als andere partijen toegang hebben of krijgen tot die informatie. Voorbeelden van dergelijke soorten informatie zijn zoektermen op symptomen van ziektes, privé communicatie en het opzoeken van informatie over politiek gevoelige onderwerpen. Het gaat de respondenten vooral om de ontbrekende context met betrekking tot die informatie. De overheid, politie of zorgverzekeraar bijvoorbeeld, mochten zij deze informatie onder ogen krijgen, missen volgens de respondenten de

context. Denk aan het voorbeeld uit hoofdstuk vier dat de politie kan zien waar de mobiele telefoon van een persoon is, maar dat nog niet wil zeggen dat die persoon daar ook is. We zien hier dat de mogelijkheden of gevaren die de respondenten toeschrijven aan het decontextualiseren en hercontextualiseren zoals besproken door de WRR (2001) een belangrijke rol spelen bij het inzetten van deze tweede strategie. Of dergelijke instanties deze gegevens onder ogen krijgen weten de respondenten niet, het gaat de respondenten naar eigen zeggen daarom vooral om preventieve handelingen.

Naast deze preventieve en selectieve bescherming van persoonsgegevens proberen de respondenten hun gegevens op het internet te managen. De manier waarop digitale gegevens de respondenten representeren op het internet en op sociale media wordt daarbij in de gaten gehouden. Naast het managen van persoonsgegevens in de context van het hercontextualiseren proberen de respondenten zo tevens hun online identiteit te managen. Het googelen van namen is daarbij een veel gebruikte manier. De respondenten geven aan dit ongeveer maandelijks te doen, en ondernemen ook actie als ze informatie vinden die ze liever niet op het internet hebben willen staan. Ageeth geeft aan in dergelijke gevallen contact op te nemen met de persoon of het bedrijf die deze informatie gepubliceerd heeft met de vraag die gegevens te verwijderen. Henk legt het doel uit van dergelijke handelingen:

"*Ik probeer te voorkomen dat er verkeerde beelden ontstaan. Dat er geen informatie neergezet wordt die niet klopt met de werkelijkheid. Daarom is het gewoon gevaarlijk om alles los te laten en er niets mee te doen.* "

Het managen van digitale gegevens richt zich voornamelijk op informatie op het internet en sociale media, terwijl het beschermen en beperken van persoonsgegevens zich voornamelijk richt op gegevens bij bedrijven en overheden waar het ontbreken van de eerder genoemde context problemen op zou kunnen leveren. De keuze wanneer er wel of geen maatregelen worden getroffen hangt enerzijds af van dit onderscheid, en anderzijds van de bereidheid om gemakken op te geven. Binnen deze tweede strategie ligt deze bereidheid lager dan in de eerste strategie. Dennis legt uit:

"*Ik gebruik advertentieblokkers en ik gebruik een tooltje waardoor ik altijd op een veilige verbinding zit als die er is. Maar ik gebruik bijvoorbeeld geen TOR netwerk. Dat is een beetje, dat vind ik teveel gedoe. Dus ik maak er uiteindelijk zelf ook wel een makkelijke keuze in*."

De lagere bereidheid om gemakken op te geven heeft gevolgen voor de online maatregelen die de respondenten treffen. Zoals Dennis hierboven laat zien, zorgt de afweging tussen gemak en bescherming ervoor dat respondenten online niet altijd de maximale bescherming nastreven. Vooral

offline worden er echter niet of nauwelijks maatregelen getroffen. De maatregelen zoals het thuis laten van mobiele telefoons, het zo veel mogelijk met cash geld betalen of het nemen van een paspoort zonder vingerafdruk worden binnen deze strategie niet gehanteerd.

5.2.3 Zelfreflectie & gelatenheid

Iets minder dan één derde van de respondenten maakt gebruik van de derde strategie. In deze strategie gaat het niet om het minimaliseren of beperken van persoonsgegeven. Er is in lichte mate sprake van het managen van gegevens zoals besproken in de vorige strategie. Echter maken de respondenten vooral gebruik van, en vertrouwen op, een mate van zelfreflectie. Roderik legt uit wat deze zelfreflectie in de praktijk behelst:

"Ik heb voor mezelf wel bepaald wat ik zou delen, en soms schrijf ik een tweet en gooi ik die weg. (…) Ik lees hem altijd even terug, nou niet altijd maar vaak wel, bij gevoelige dingen. Ik denk dat ik ongeveer de helft van mijn tweets niet post."

Respondenten die deze strategie hanteren stellen dat het bewustzijn dat informatie die men op het internet zet publiekelijk is, en daar voor altijd zal blijven staan, van belang is. De respondenten maken volop gebruik van internetdiensten en sociale media. Ze zijn naar eigen zeggen heel open op het internet en zijn zich daar ook erg bewust van. Het feit dat de respondenten dit bewustzijn hebben, maakt volgens hen het verschil. Tevens maakt het dat ze daarnaast weinig tot geen maatregelen treffen. Stefan legt uit:

"*Kijk, ik gebruik voor mezelf mijn echte naam op het internet en ik post ook onder mijn eigen naam. Ik heb ook een mening onder mijn eigen naam. Dat vind ik niet erg omdat ik redelijk nadenk over wat ik zeg en dat ik daar gewoon voor sta. Maar kids, van 15 of zo, die maken een periode mee in hun leven waarop ze gewoon stomme dingen zeggen. Dat doe je gewoon als je puber bent. Dan doe je vreemde dingen. Daar is het gevaar veel reëler zeg maar. Voor mij persoonlijk ontwijk ik niet echt iets. Ik kan het wel, want ik ben programmeur, dus ik weet hoe ik redelijk anoniem dingen kan doen op het internet. Maar dat doe ik niet. Nee."*

Hoewel deze zelfreflectie opgevat kan worden als een lichte mate van management omdat er een selectie van gegeven plaatsvindt, onderscheidt deze strategie zich op twee punten van de vorige. Ten eerste is zelfreflectie de enige, en volgens de respondenten afdoende, maatregel. Er worden weinig tot geen maatregelen getroffen zoals het gebruik van TOR en VPN. Ten tweede heerst de opvatting binnen deze strategie dat gegevens over het individu helemaal niet zo van belang zijn in het grotere geheel. Wederom Stefan legt uit:

"*Misschien is dat wel een beetje naïef zelfs. Maar kijk: ik ben helemaal niet zo interessant verder voor iemand, maar de groep is wel interessant. Dus ik ben er zelf eigenlijk niet mee bezig, niet veel mee bezig.*"

Naast de opvatting dat zelfreflectie grotendeels afdoende is omdat het bij de verzameling van persoonsgegevens door bedrijven en overheden vooral gaat om het totaal aan die gegevens en niet zozeer om individuele stukjes daarvan, lijken de respondenten ook bewust een keuze te maken om hun leven niet te veel te laten leiden door de vraag wie er gegevens verzamelen, en wat zij daarmee doen. In tegenstelling tot de respondenten die de eerste strategie hanteren verwerpen de respondenten die deze derde strategie hanteren het "*nothing to hide*" argument (Solove, 2007) over het algemeen niet. Hoewel het een specifieke invulling van het argument betreft, dat zich wellicht beter laat omschrijven als een "*nothing to see*" argument, gebruiken de respondenten dit idee om hun keuze zich geen zorgen te maken te verdedigen. Henk laat echter nog een reden zien waarom de respondenten die gebruik maken van deze strategie zich geen zorgen willen maken:

"*Op een gegeven moment word je zo cynisch van alles wat te maken heeft met privacy wetgeving en hoe dat geïmplementeerd wordt, en hoe je gegevens opgeslagen worden. Je gaat als je er lang genoeg mee bezig bent, ga je letterlijk een grijs aluminium hoedje dragen omdat je gewoon gek wordt*."

Ook Tim geeft aan dat hij op het gebied van de verzameling van persoonsgegevens voor een deel zijn zorgen plaats heeft laten maken voor alertheid en zelfreflectie om daarmee zijn leven niet in het teken te laten staan van zijn zorgen. Hoewel hij aangeeft bepaalde maatregelen te hebben getroffen met betrekking tot het weghalen van persoonlijke informatie van het internet, maakt hij zich bewust minder druk dan vroeger:

"*Het drukte ook op mijn gemoedsrust zeg maar. Het was iets waar ik mij druk over maakte. En dat wil ik niet. Ik heb wel besloten om, en dat is wel een bewuste keuze, om mij daar niet te veel zorgen over te maken, maar meer om daar steeds alert op te zijn*."

Het mag duidelijk zijn dat het niet zo is dat de respondenten die zich bewegen rond deze derde strategie het fijn vinden dat hun gegevens en digitale voetsporen voor lange tijd ergens opgeslagen staan. De gehanteerde zelfreflectie heeft natuurlijk lichte raakvlakken met het minimaliseren of beperken van persoonsgegevens. De opvatting dat zelfreflectie afdoende is omdat het vooral om gegevens over de groep gaat, is bepalend voor het feit dat de respondenten verder niet of nauwelijks maatregelen treffen. Daarbij speelt ook de opvatting een rol dat de situatie nu eenmaal is zoals hij is en dat de respondenten verwachten dat zij in de toekomst een manier hebben gevonden om hiermee om te gaan. Roderik legt uit:

Mijn hele porno geschiedenis zal tot in de eeuwigheid te vinden zijn, dat is gewoon zo. En ja, vind ik dat leuk? Nee. Maar het is zo. En dan zou ik heel heilig kunnen gaan doen en zeggen: dan gaan we gewoon geen porno meer surfen, en vanaf dat moment was ik genezen. Nee. Ik vind dat veel te leuk. En iedereen heeft dat. Iedereens geschiedenis is opgeslagen. En hoewel we ons dat nu nog niet kunnen voorstellen, zullen we over 30 jaar nog steeds bestaan en een manier hebben gevonden om daar mee om te gaan."

De keuze van de respondenten om zich bewust geen zorgen te maken, samen met het feit dat zij verwachten dat er manieren zullen ontstaan om met de opgeslagen gegevens om te gaan, maakt dat deze derde strategie zich laat kenmerken door een mate van gelatenheid. Die gelatenheid manifesteert zich in een acceptatie van de situatie zoals hij is. Dit accepteren is daarmee tevens onderdeel van deze derde strategie.

5.3 Tegen beter weten in: de effectiviteit van reacties & strategieën

In deze laatste paragraaf van dit hoofdstuk worden de drie besproken strategieën samengevat in het onderstaande figuur. Daarnaast wordt een laatste punt besproken wat zich richt op de ervaren effectiviteit en invloed van de reacties in het algemeen, en de strategieën in het bijzonder.

Figuur 3: Drie strategieën van individuele reacties op de surveillant assemblage

	Strategie 1	Strategie 2	Strategie 3
Vorm	Minimaliseren	Managen	Reflecteren
Handelingen	Ontlopen, blokkeren, onklaar maken, verstoren, weigeren	Ontlopen en blokkeren Gegevensmanagement Identiteitsmanagement	Zelfreflectie Gelatenheid Acceptatie
Motivatie	Voorkomen verzameling van persoonsgegevens	Beperken risico's van verzameling persoonsgegevens	Niet gek worden Individu niet van belang
Intensiteit	Hoog Online en offline	Gemiddeld Online	Laag Beperkt online

Het bovenstaande figuur geeft een schematisch overzicht van de belangrijkste elementen van de drie gevonden ideaaltypische strategieën die de respondenten in het dagelijks leven hanteren in hun omgang met de surveillant assemblage in het algemeen, en de verzameling van persoonsgegevens in het bijzonder. Het moet worden opgevat als een schaal waarbij de intensiteit van de maatregelen alsmede de bereidheid om gemakken van het hedendaagse digitaal georiënteerde leven op te willen

geven af neemt. Hoewel de keuze voor een strategie in eerste instantie afhangt van het doel, de motivatie en de overtuigingen van de respondent, spelen in sommige gevallen haalbaarheidsoverwegingen een rol. Respondenten die zich bijvoorbeeld bewegen rond strategie één kunnen in gevallen waar deze strategie niet haalbaar is mogelijk uitwijken naar strategie twee. Hoewel deze strategieën duidelijk naar voren zijn gekomen, moet er bij deze bevindingen een kanttekeningen worden geplaatst. Deze kanttekening heeft betrekking op een gebrek aan invloed of effectiviteit die de respondenten toeschrijven aan hun maatregelen. Of respondenten zich nu richten op het zo veel mogelijk minimaliseren van het vrijgeven van persoonsgegevens, deze vooral proberen te managen of vooral vertrouwen op zelfreflectie, veelal worden deze maatregelen besproken in termen van 'tegen beter weten in'. Helemaal nutteloos zijn de maatregelen volgens de respondenten niet. Zeker in vergelijking met personen die zich niet bezig houden met, of niet bewust van, privacy en de bescherming van persoonsgegevens stellen de respondenten dat zij het relatief goed geregeld hebben. Echter in ieder interview werd een bepaalde machteloosheid benadrukt zoals Sophie hieronder doet:

"*Het is niet vol te houden eigenlijk. Het is net hoe graag je het wilt, maar het is best lastig. En dat is ook het nadeel aan deze problematiek, want het proces is heel onzichtbaar, en het gaat heel geleidelijk. Dus daarom gaat het ook zo makkelijk. En daarom is het ook heel moeilijk om er iets tegen te doen*."

Hoewel bij het beschrijven van deze machteloosheid de respondenten enerzijds wijzen op specifieke oorzaken zoals de mate waarin de verzameling van gegevens geïntegreerd is in de samenleving, het onzichtbare karakter van die processen alsmede het gebrek aan inzicht wie er met die gegevens 'aan de haal' gaan, spelen anderzijds meer omvattende opvattingen een rol bij de ervaren machteloosheid. Deze hebben niet zozeer betrekking op het heden en de vraag hoe om te gaan met de beschreven problematiek, maar hebben betrekking op de toekomst en de vraag hoe deze processen zich zullen ontwikkelen. Zowel op korte als lange termijn verwachten de respondenten over het algemeen niet dat er grote veranderingen zullen plaatsvinden. Een belangrijke reden die de respondenten hiervoor noemen is het idee dat dergelijke thema's geen hoge prioriteit hebben op politieke agenda's. Stefan legt uit waarom:

"*Dat is wel moeilijk, maar, omdat er gewoon, omdat de wereld gewoon nog niet klaar is voor internationale wetten. Omdat iedereen zijn eigen mening in zijn eigen land en zijn eigen belangen heeft. Internationaal komen we niet eens uit oorlogen, laat staan over zoiets kleins*."

Stefan heeft het in het bovenstaande citaat over internationale regels. En hoewel er verschillende opvattingen bij de respondenten bestaan over de beste manier om tot verbetering van de huidige situatie te komen, hebben deze allemaal betrekking op een dergelijk grote omslag. Vooral de

belangrijke rol van technologie in het algemeen, en het internet in het bijzonder in de hedendaagse samenleving maakt dat die omslag volgens de respondenten betrekking moet hebben op een denkwijze. De afhankelijkheid van technologie en het internet maakt dat de respondenten niet verwachten dat een dergelijke omslag snel zal plaatsvinden. Daarnaast speelt het feit dat deze omslag een tamelijk grote is een rol. Ageeth laat zien op welk niveau deze omslag betrekking heeft. Voor haar is het internet een hele nieuwe beschaving waar een nieuwe werkelijkheid op geplakt moet worden. Zij doelt daarmee op een noodzaak tot nieuwe regels en een nieuw rechtssysteem die het belang en de integratie van het internet inzien. Huidige opvattingen over identiteit en privacy missen volgens Ageeth dergelijke inzichten. Vooral bij beleidsmakers en politici stellen de respondenten niet tot nauwelijks aanwijzingen te zien dat zij begrijpen hoe groot de invloed is van technologie en het internet in onze samenleving. Roderik legt uit:

"*Ik denk dat cultuur bepaald wordt door twee dingen. Enerzijds techniek. De beste technische mogelijkheden worden gekozen en bepalen de cultuur, en aan de andere kant heb je wetgeving. Je kunt mensen dwingen om bepaalde dingen te doen. Alleen op dit moment is de technische ontwikkeling van het internet, is zoveel sterker dan je met wetgeving kan beperken. En heel veel politici zitten nog in die oude controle rol. En die is er niet meer*."

De machteloosheid die de respondenten ervaren lijkt enerzijds te bestaan uit de afhankelijkheid van de bedrijven en overheden die gebruik maken van persoonsgegevens en geen motivatie of kennis lijken te bezitten om veranderingen te bewerkstelligen. Vooral het gebrek aan controle over de eigen gegevens is daarbij volgens de respondenten een heikel punt. Anderzijds zorgt de mate van integratie van technologie en het internet in het dagelijks leven ervoor dat grote veranderingen niet makkelijk te realiseren zullen zijn. Een groot deel van de respondenten geeft aan dat er eerst een aantal grote incidenten zullen (moeten) plaatsvinden alvorens dergelijke veranderingen aan de orde zullen zijn.

"Ik denk dus echt wel dat er een groot incident moet gebeuren voordat het kwartje eindelijk valt zeg maar. Maar dan nog. Hoe kan je dat oplossen?" (Stefan)

"*Dat is een proces van tientallen jaren. En er gaan heel veel erge dingen gebeuren totdat die gesprekken echt gevoerd gaan worden. Misbruik, groot misbruik van data."* (Ageeth)

Tot die tijd lijken de respondenten zich te beroepen op hun gekozen strategie, en alert te blijven op de technologische ontwikkelingen. Want hoewel sommige respondenten zich meer richten op het beschermen van hun gegevens dan andere respondenten dit doen, houden ze allemaal rekening met de kracht van technologie en de invloed die het heeft op het dagelijks leven.

"*Technologie gaat gewoon door, dus dat is een neutrale kracht waar je gewoon rekening mee hebt te houden. En iedere technologie heeft voordelen en nadelen. Heeft kansen en bedreigingen. En waar je als activist voortdurend mee bezig bent is het duwen van, het vooruit duwen van de kansen en het tegenhouden van de bedreigingen. En proberen in een samenleving te komen waar je het prettig vindt toeven*." (Joris)

De zojuist beschreven kanttekening is enerzijds van belang omdat het de resultaten van dit onderzoek plaatst in de context van het gebrek aan persoonlijke invloed die centraal staat in de belevingswereld van de respondenten. Anderzijds speelt deze context en belevingswereld een belangrijke rol in de conclusie van dit onderzoek. Hoe die rol er precies uit ziet, en welke conclusies er verder getrokken kunnen worden zal in het volgende, en tevens laatste hoofdstuk worden besproken.

Hoofdstuk 6: Conclusie & wetenschappelijke bijdrage

In dit hoofdstuk worden de conclusie en de wetenschappelijke bijdrage van deze scriptie besproken. Eerst wordt in paragraaf 6.1 echter een korte samenvatting gegeven van de belangrijkste resultaten van dit onderzoek.

6.1 Samenvatting

Vanuit de constatering dat het ontstaan van de surveillant assemblage heeft gezorgd voor maatschappelijke reacties die zich bezig houden met zaken als macht, privacy en de bescherming van persoonsgegevens, heb ik in deze scriptie getracht te onderzoeken hoe personen die zich met een dergelijke organisatie identificeren in het dagelijks leven reageren op deze assemblage. De probleemstelling die ik hiervoor heb willen beantwoorden is de volgende:

Wat zijn de zorgen van personen die zich met Bits of Freedom identificeren, en hoe reageren zij individueel-collectief en individueel op de surveillant assemblage?

De zorgen van de respondenten komen voort uit twee ontwikkelingen. Ten eerste zien zij een samenleving waarin er een nadruk op risico beheersing (overheden) en consumenten controle (bedrijven) is ontstaan. Informatie over (groepen) personen wordt daardoor tegenwoordig volop verzameld. Ten tweede zien de respondenten als gevolg daarvan een nadruk op informatie en persoonsgegevens ontstaan. Vooral op het internet stellen de respondenten daar de uitwerkingen van te kunnen zien. Overheden en bedrijven lijken steeds meer vat te willen krijgen op het internet omdat het één van de belangrijkste netwerken is om gegevens over personen te verzamelen. Vanuit deze ontwikkelingen worden een drietal zorgen zichtbaar.

Ten eerste dragen de verzamelde gegevens bij aan kennis en macht bij diegene die de gegevens verzamelen. Volgens de respondenten is het moeilijk na te gaan of die gegevens correct zijn, en op welke manieren die gegevens gebruikt worden. Vooral de afhankelijkheid van de manieren waarop overheden en bedrijven omgaan met die gegevens speelt bij deze zorg een belangrijke rol. Ten tweede stellen de respondenten dat de verzamelde gegevens nooit meer zullen verdwijnen uit de databanken waarin ze opgeslagen staan. Hoewel er nu weinig aanwijzingen zijn dat die gegevens op grote schaal misbruikt worden, kan het volgens de respondenten gebeuren dat politieke veranderingen ervoor zorgen dat die gegevens wel misbruikt gaan worden. Ten derde wijzen de respondenten op een gebrek aan alertheid. Zowel politici als de massa zien volgens de respondenten te weinig in hoe omvangrijk de potentiële problemen met betrekking tot die gegevens kunnen zijn, waardoor deze processen stapje voor stapje voortschrijden en uitbreiden.

De reacties van de respondenten hebben individueel-collectieve en individuele doelen. De individueel-collectieve reacties richten zich op het creëren van bewustwording in de sociale en professionele omgeving van de respondenten. Vooral het verspreiden van kennis en middelen om persoonsgegevens te beschermen staan daarbij centraal. Daarnaast steunen de respondenten personen en organisaties die zich bezig houden met de politieke lobby voor de bescherming van privacy en persoonsgegevens binnen wetgeving. Vooral het bewerkstelligen van veranderingen waarop de respondenten persoonlijk weinig invloed hebben staan bij de individueel-collectieve reacties centraal. De individuele reacties van de respondenten zijn in deze scriptie weergegeven als drie ideaaltypische strategieën. Deze kunnen opgevat worden als een schaal waarbij de intensiteit van de maatregelen alsmede de bereidheid om gemakken in het dagelijks leven op te geven afneemt. Hoewel in de empirie deze strategieën op bepaalde onderdelen overlappen, en dus geen harde afbakening kennen, kunnen de strategieën op de volgende manier worden beschreven.

De eerste strategie betreft het zo veel mogelijk minimaliseren van het vrijgeven van persoonsgegevens. Vanuit het idee de risico's van opgeslagen gegevens zo veel mogelijk te beperken, alsmede vanuit de ideologie dat overheden en bedrijven die gegevens niet nodig hebben, geven respondenten zowel in het online als offline leven gemakken op om zo min mogelijk digitale voetsporen bij te dragen aan de assemblage. De tweede strategie richt zich op het managen van persoonsgegevens en identiteiten. Alleen in gevallen waar respondenten verwachten dat gegevens nadelige gevolgen kunnen hebben, worden online maatregelen ingezet. Offline treffen de respondenten weinig tot geen maatregelen. De derde strategie gaat uit van een mate van zelfreflectie. Deze strategie richt zich voornamelijk op het vooraf beoordelen van gegevens die respondenten zelf willen toevoegen aan het internet. Daarnaast maken de respondenten de keuze om zich verder niet of nauwelijks zorgen te maken over de beschreven problematiek. Dit doen zij om drie redenen. Ten eerste willen de respondenten hun leven er niet teveel door laten leiden. Ten tweede gaat het bij de verzameling van persoonsgegevens volgens hen niet om het individu maar om de groep. Ten derde verwachten de respondenten in de toekomst manieren te hebben gevonden om met het feit dat gegevens nu eenmaal opgeslagen staan om te gaan. Hoewel deze drie strategieën duidelijk naar voren zijn gekomen, geven alle respondenten aan dat zij de invloed die zij persoonlijk hebben op de beschreven processen als gering ervaren. De afhankelijkheid van zowel de systemen die deze gegevens verzamelen alsmede de afhankelijkheid van de omgang met die gegevens door derden, zorgt ervoor dat de respondenten de ervaren geringe invloed bespreken in termen van machteloosheid.

6.2 Conclusie: vechten tegen de bierkaai

Naast de zojuist beschreven antwoorden op de probleemstelling kunnen we uit dit onderzoek een aantal conclusies trekken. De eerste conclusie uit het onderzoek heeft te maken met de afhankelijkheid die de respondenten ervaren met betrekking tot de overheden, bedrijven en systemen die de persoonsgegevens verzamelen en beheren. In hoofdstuk twee heb ik de noties van het nieuw feodalisme (Schneier, 2012) en de iOverheid (WRR, 2011) besproken. Volgens Schneier zijn personen afhankelijk van de digitale grootheden die hun gegevens beheren, en kunnen zij vaak niet anders dan deze bedrijven vertrouwen zonder dat personen weten hoe deze bedrijven omgaan met hun gegevens. Ook het WRR rapport laat zien dat burgers afhankelijk zijn van de manieren waarop overheden hun gegevens gebruiken en hercontextualiseren, en stelt daarnaast dat burgers er rekening mee moeten houden dat hun gegevens een eigen leven kunnen gaan leiden. Omdat de respondenten over het algemeen weinig vertrouwen hebben in de intentie of de kennis van de actoren die hun gegevens verzamelen en gebruiken, lijkt de besproken afhankelijkheid te zorgen voor een ervaren afgeleide machteloosheid. Juist omdat de intentie of kennis in twijfel wordt getrokken, en de invloed en controle die de respondenten daarop hebben als gering worden ervaren, voelen de respondenten zich overgeleverd aan de grote spelers. Als het gaat om bedrijven stellen de respondenten dat zij in veel gevallen niet weten welke bedrijven gegevens verzamelen, en hoe zij daarmee om gaan. Als het gaat om overheden speelt vooral het monopolistische karakter een belangrijke rol. Overheden gebruiken nu eenmaal gegevens om hun taken uit te voeren. En hoewel de respondenten erkennen dat bepaalde gegevens nodig zijn, wijzen zij op de gevaren van de onbenullige en onzichtbare omgang met die gegevens alsmede eventuele politieke veranderingen die in de toekomst plaats kunnen vinden. De afhankelijkheid en de afgeleide machteloosheid hebben zo dus betrekking op zowel de verschillende onderdelen van de surveillant assemblage, alsmede op de integratie van de assemblage in de hedendaagse samenleving. Het gebrek aan persoonlijke controle wat daaruit voortkomt is zowel reden voor de respondenten om te reageren (strategie 1 en 2), of om dit bewust niet of nauwelijks te doen (strategie 3).

Naast dat de afhankelijkheid en machteloosheid van invloed zijn op de reacties van de respondenten, lijken deze punten ook verbonden te zijn met de tweede conclusie uit dit onderzoek. Deze tweede conclusie heeft betrekking op de manier waarop de respondenten spreken en denken over privacy. Hoewel de respondenten regelmatig verwijzen naar privacy als zij spreken over hun zorgen, lijkt het begrip in de context van de surveillant assemblage voornamelijk gebruikt te worden als een containerbegrip voor de veelheid aan onderwerpen die te maken hebben met de verzameling en het gebruik van persoonsgegevens. Persoonlijke privacy wordt enerzijds niet of nauwelijks meer mogelijk geacht en wordt anderzijds gezien als moeilijk te realiseren. Daarnaast is door het ontstaan van de

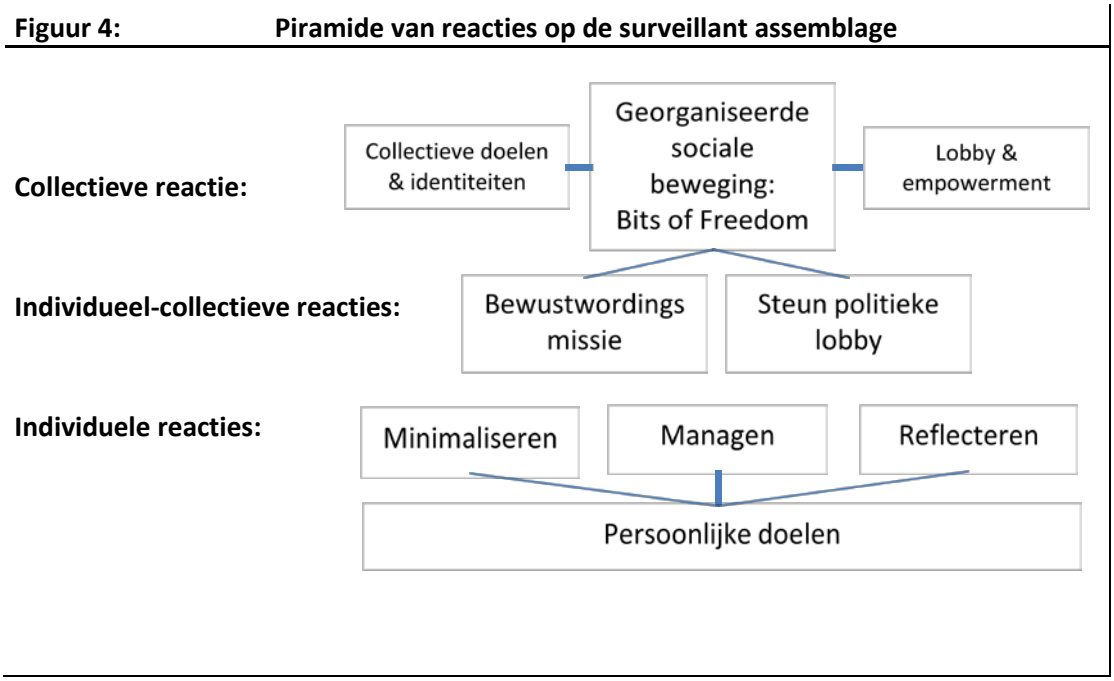
surveillant assemblage volgens de respondenten lastig te omschrijven wat privacy tegenwoordig precies is. De meeste respondenten beschrijven privacy in de context van de surveillant assemblage in termen van controle over persoonsgegevens. Het gaat daarbij erom dat respondenten zelf willen bepalen wie dergelijke gegevens mogen verzamelen, inzien of gebruiken. Hoewel privacy in termen van wetgeving nog steeds van belang is omdat het volgens de respondenten de noemer is waaronder organisaties zoals Bits of Freedom opereren, lijkt het voor de respondenten persoonlijk vooral te gaan om deze controle. Dit is in het licht van de eerste conclusie interessant omdat het gevoel van afgeleide machteloosheid, alsmede het ervaren gebrek aan controle in de surveillant assemblage zo verbonden lijken te zijn met de opvattingen van de respondenten over privacy in de hedendaagse samenleving.

De derde conclusie heeft betrekking op de manieren waarop de respondenten omgaan met dit ervaren gebrek aan controle alsmede de context waarin zij hun reacties plaatsen. Hoewel de details van de zorgen, alsmede de opvattingen over de manier waarop bedrijven en overheden met persoonsgegevens om zouden moeten gaan verschillen, is de wens tot meer invloed op dergelijke processen gemeen goed. Individueel-collectieve reacties richten zich op het steunen van personen en organisaties die zich daarvoor inzetten. Individuele reacties lijken vooral te bestaan uit de manieren waarop personen in het dagelijks leven omgaan met de beschreven afhankelijkheid en machteloosheid. Echter, of de respondenten nu hun gegevensbijdrage minimaliseren, managen of hier enkel over reflecteren; de maatregelen worden veelal geplaatst in een context van 'tegen beter weten in'. Vooral de integratie, afhankelijkheid en omvang van de surveillant assemblage in het dagelijks leven maakt dat zowel reacties met een individueel-collectief doel als reacties met een individueel doel, vanuit het oogpunt van de respondenten, kunnen worden begrepen als 'vechten tegen de bierkaai'. Dit vechten tegen de bierkaai moet worden opgevat als het uitvoeren van handelingen en maatregelen vanuit een gedachte dat de resultaten van deze ondernemingen gering zullen zijn. Net zoals de vroegere arbeiders van de Bierkade, worden de grote spelers binnen de surveillant assemblage simpelweg als te groot en te sterk ervaren. Het gevecht ertegen wordt daardoor gezien als een onwinbare strijd. Hoewel in vroegere tijden het gevecht met de arbeiders daarom veelal werd ontweken, gaan de respondenten in meer of mindere mate wel de strijd aan met de digitale bierkaai. De beschreven individueel-collectieve reacties zijn daar de meer indirecte voorbeelden van. De individuele strategieën één en twee, en in mindere mate strategie drie, zijn daar de meer directe voorbeelden van. Juist omdat de respondenten hun eigen reacties in deze context plaatsen, lijkt deze strijd op een individueel niveau niet zozeer gemotiveerd te zijn vanuit het idee dit gevecht te winnen. Het gevecht tegen de bierkaai bestaat daarom vooral uit het zo goed mogelijk omgaan met een samenleving die gezien kan worden als een surveillant assemblage.

6.3 Wetenschappelijke bijdrage

De wetenschappelijk bijdrage van deze scriptie bestaat in de eerste plaats uit de drie beschreven ideaaltypische strategieën als individuele reacties op surveillance binnen de context van de surveillant assemblage. Daarnaast hebben de resultaten uit dit onderzoek het mogelijk gemaakt deze verschillende reacties te plaatsen in de onderstaande reactiepiramide. Deze piramide maakt vooral inzichtelijk welke vormen de reacties van personen met een oppositioneel bewustzijn tegen de surveillant assemblage aannemen, vanuit welke doelen deze reacties plaats vinden en de manieren waarop deze reacties en doelen zich tot elkaar verhouden.

Figuur 4: **Piramide van reacties op de surveillant assemblage**



Naast deze piramide van reacties draagt dit onderzoek tevens bij aan kennis over reacties op, en verzet tegen surveillance in de context van de surveillant assemblage. Belangrijk om hierbij op te merken is dat de respondenten in deze scriptie zijn geselecteerd op de afhankelijke variabele. Het identificeren met, en fan zijn van Bits of Freedom kan worden gezien als een reactie op de surveillant assemblage. Hoewel dit een lichte vorm betreft is het daardoor niet mogelijk om uitspraken over reacties op, of verzet tegen surveillance te generaliseren. Wel geeft het de mogelijkheid om de specifieke context uit deze scriptie te vergelijken met die uit bestaande theorieën over reacties op, en verzet tegen surveillance en te bekijken op welke punten dit onderzoek kan bijdragen aan deze theorieën.

Om te beginnen is het interessant te bekijken of de reacties die beschreven zijn in dit onderzoek kunnen worden gezien als verzet. Als we kijken naar de beschrijving van Hollander en Einwohner

(2004) waarbij verzet gaat om verbaal, cognitief of fysiek gedrag vanuit een oppositionele opvatting, kunnen we de gevonden strategieën zien als verzet. Voor de strategieën één en twee, die zich richten op het minimaliseren en het managen van persoonsgegevens, bestaat dat verzet vooral uit de technieken die Marx (2003) heeft beschreven. Ook strategie drie, waarin respondenten enkel gebruik maken van zelfreflectie en daarnaast een keuze maken om zich verder niet al te veel zorgen te maken over de verzameling van persoonsgegevens, valt volgens de beschrijving van Hollander en Einwohner onder verzet. Hoewel in lichte vorm ondernemen de respondenten die deze strategie hanteren namelijk maatregelen vanuit een oppositionele opvatting. Het reflecteren over het loslaten van (persoons)gegevens kan daarbij als toevoeging worden gezien op de technieken die Marx heeft beschreven.

Als we meer specifiek kijken naar theorieën over verzet tegen surveillance, waarbij verzet minder algemeen wordt beschreven dan de manier waarop Hollander & Einwohner dat doen, is het van belang te kijken naar de context waarin personen reageren. Gilliom (2005) wijst namelijk op het feit dat het begrijpen van verzet tegen surveillance zich relatief weinig heeft gericht op de verschillende contexten, systemen en personen waarmee surveillance te maken heeft. Surveillance zorgt voor verschillende machtsrelaties waarin actoren verschillende rollen innemen, en verschillende mogelijkheden tot verzet bezitten als gevolg van de context waarin die machtsrelaties zich bevinden (Martin, van Brakel en Bernhard, 2009). In hoofdstuk twee zagen we dat verzet tegen surveillance beschreven door Scott (1985) en Gilliom (2001) zich laat kenmerken door enerzijds een bepaalde machteloosheid, en anderzijds een streven naar het behalen van directe voordelen vanuit de wil of noodzaak te overleven. De context van de boeren en bijstandsmoeders waarop deze kenmerken zijn gebaseerd verschilt echter van de context waarin de respondenten in dit onderzoek geplaatst kunnen worden. Daar waar de boeren en bijstandsmoeders vooral kleine ad hoc handelingen uitvoeren in relatie tot één of enkele surveillance systemen, zijn de handelingen van de respondenten in dit onderzoek gericht op de surveillant assemblage als geheel, en dus gericht op een veelheid aan surveillance systemen. Daarnaast hebben de handelingen van de respondenten vooral betrekking op het behalen van indirecte voordelen, of zelfs het beperken van nog onbekende indirecte nadelen, en speelt de noodzaak tot het overleven niet tot nauwelijks een rol. Hoewel de respondenten, net zoals de boeren en bijstandsmoeders, een bepaalde machteloosheid ervaren moet deze machteloosheid worden bezien vanuit deze verschillen in context. Voor Marx (2003) neemt machteloosheid in de context van de hedendaagse surveillant assemblage, waarin het gebruik van persoonsgegevens onderdeel is geworden van het dagelijks leven, een geheel andere betekenis aan. "*Powerless takes on a new meaning (beyond its usual association with lower social class or minority status) when we consider the demands of the modern organization for personal information*" (Marx, 2003: 372). De

resultaten van dit onderzoek laten zien dat deze machteloosheid in de context van de surveillant assemblage gezien kan worden als voornamelijk een afgeleide machteloosheid. De respondenten hebben, door gebruik te maken van de besproken strategieën, over bepaalde gegevens een lichte mate van controle. De afgeleide machteloosheid heeft echter betrekking op die gegevens waar respondenten, als gevolg van de integratie van de surveillant assemblage in de organisatie van de samenleving, geen controle over hebben. Ze zijn daarbij overgeleverd aan de kennis, intentie en zorgvuldigheid van de actoren die deze gegevens beheren en gebruiken.

Tot slot is het interessant te bekijken of de gevonden reacties van de respondenten in dit onderzoek kunnen worden gezien als alledaags verzet tegen surveillance zoals beschreven door Gilliom & Monahan (2012). Alledaags verzet wordt gezien als ongeorganiseerd, los van ideologische opvattingen en voortkomend uit directe zorgen in het dagelijks leven. Het is van nature onzichtbaar, niet confronterend gedrag waarmee personen stilletjes hun behoeften proberen te bevredigen (Gilliom & Monahan, 2012: 405-410). Hoewel de ideologische opvattingen bij de eerste strategie meer een rol spelen dan bij de tweede en derde strategie, kunnen we niet stellen dat de handelingen helemaal los staan van ideologisch opvattingen. Daarnaast komen de reacties van de respondenten voort uit zowel directe zorgen uit het alledaags leven (hercontextualiseren van persoonsgegevens) alsmede indirecte zorgen (onbekende gevolgen voor in de toekomst). Als Gilliom & Monahan hun omschrijving van alledaags verzet streng handhaven, mogen we volgens hen dus niet spreken van alledaags verzet.

Hoewel een deel van de motivatie van de respondenten voorkomt uit ideologische opvattingen lijken de individuele handelingen tevens voort te komen uit de zorgen die zij hebben over de surveillant assemblage. Gilliom & Monahan zien alledaags verzet los van ideologische opvattingen om het onderscheid tussen georganiseerde reacties op surveillance en individuele reacties op surveillance helder te krijgen: *"The category specifically excludes organized movements, traditional ideology, and public confrontations. (..) Under this definition, opposition actions such as anti-surveillance protests by labor unions, organized uprisings against video camera installations, or litigation over privacy rights are not practices of everyday resistance."* (Gilliom & Monahan, 2012: 405). De individueel-collectieve reacties uit deze scriptie kunnen tussen georganiseerde en individuele reacties in worden geplaatst. Dit vooral omdat deze reacties zich laten kenmerken door collectieve doelen, en individuele handelingen. De individuele reacties van de respondenten in dit onderzoek vallen niet onder georganiseerde vormen, en bezitten geen collectieve doelen. En hoewel ideologische opvattingen een rol spelen, beargumenteer ik om die reden dat de beschreven individuele reacties wel als alledaags verzet kunnen worden gezien. Daarbij is tevens van belang dat de respondenten in hun dagelijks leven voornamelijk bezig zijn met het voorkomen van directe en indirecte nadelen. De

opvatting van Gilliom & Monahan dat alledaags verzet tegen surveillance vooral gericht is op het behalen van directe voordelen kan, in de context van de surveillant assemblage, aan de hand van dit onderzoek worden bijgesteld. Zoals Marx (2003) ons laat zien krijgt de machteloosheid in de surveillant assemblage een andere betekenis als gevolg van de integratie ervan in het dagelijks leven. Zoals eerder besproken kan die machteloosheid worden gezien als een afgeleide machteloosheid. Op eenzelfde manier waarop machteloosheid in de surveillant assemblage een andere betekenis krijgt, lijkt alledaags verzet ook aan een dergelijke verandering onderhevig. Het ontstaan van de surveillant assemblage lijkt er in ieder geval voor te zorgen dat naast het behalen van directe voordelen, ook en vooral het beperken van directe en indirecte nadelen onderdeel zijn van de doelen die respondenten nastreven met dit alledaags verzet tegen de surveillant assemblage.

Literatuur

- Bennett, C. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.
- Bennett, C. 2012. Privacy Advocates, Privacy Advocacy and the Surveillance Society. In: Lyon, D., Ball, K., & Haggerty, K. (red). 2012. *Routledge Handbook of Surveillance Studies*. New York: Routledge, 412-419.
- Bentham, J. 1791. Outline for the Construction of a Panopticon Penitentiary House. In: M. Mack. 1969. *A Bentham Reader.* New York: Pegasus.
- Blumer, H. 1969. Social movements. In: Rugiero, V. & Montagna, N. 2008. *Social Movements. A Reader*. London: Routledge, 64-72.
- Boeije, M. 2005. *Analyseren in kwalitatief onderzoek. Denken en Doen*. Den Haag: Boom Lemma.
- Bruno, F. 2012.Surveillance and Participation on Web 2.0. In: Lyon, D., Ball, K., & Haggerty, K. (red). 2012. *Routledge Handbook of Surveillance Studies*. New York: Routledge, 343-351.
- Campbell, J. & Carlson, M. 2002. Panopticon. com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media* 46(4), 586-606.
- Castells, M. 2007. Communication, power and counter-power in the network society. *International journal of communication* 1(1), 238-266.
- Clarke, R. 1994. The digital persona and its application to data surveillance. *The Information Society* 10(2). http://www.rogerclarke.com/DV/DigPersona.html. Geraadpleegd op 01 juli 2014.
- Diani, M. 1992. The concept of social movement. *The Sociological Review* 40(1), 1-25.
- Eyerman, R. & Jamison, A. 1998. *Music and Social Movements: Mobilizing traditions in the twentieth century*. Cambridge, UK: Cambridge University Press.
- Fernandez & Huey. 2009. Is Resistance Futile? Thoughts on resisting Surveillance. *Surveillance & Society* 6(3): 198-202.
- Flick, U. 2009. *An Introduction to Qualitative Research. Edition 4*. London: Sage Publications Ltd.
- Foucault, M. 1977. *Discipline and Punish. The Birth of the Prison*. (A. Sheridan Vert.) London: Penguin Books Ltd. (oorspronkelijk werk gepubliceerd in 1975).
- Foucault, M. 1978. *The History of Sexuality* (vol. 1: R. Hurley, Vert.) New York: Random House.
- Gilliom, J. 2001. *Overseers of the Poor*. Chicago: University of Chicago Press.
- Gilliom, J. 2005. Struggling with Surveillance: Resistance, Counsciousness, and Identity. In: Haggerty, K. & Ericson, R. 2005. *The New Politics of Surveillance and Visibility*. Toronto: Toronto University Press, 111-129.
- Gilliom, J. & Monahan, T. 2012. Everyday resistance. In: Lyon, D., Ball, K., & Haggerty, K. (red). 2012. *Routledge Handbook of Surveillance Studies*. New York: Routledge, 405-411.

- Graham, S. & Wood. D. 2003. Digitizing Surveillance: Categorization, Space, Inequality. *Critical Social Policy* 23, 227-248.
- Green, S. 1999. A Plague on the Panopticon: Surveillance and Power in the Global Information Economy. *Information, Communication & Society* 2(1), 26-44.
- Haggerty, K. & Ericson, R. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4), 605-622.
- Haggerty, K. & Ericson, R. 2005. *The New Politics of Surveillance and Visibility*. Toronto: Toronto University Press.
- Hope, A. 2005. Panopticism, Play and the Resistance of Surveillance: case studies of the observation of student Internet use in UK schools. *British Journal of Sociology of Education* 26 (3).
- Lindgren, S. 2013. *New Noise. A Cultural Sociology of Digital Disruption*. New York: Peter Lang Publishing.
- Lyon, D., Ball, K., & Haggerty, K. (red). 2012. *Routledge Handbook of Surveillance Studies*. New York: Routledge.
- Lyon, D. 2003. Surveillance Technology and Surveillance Society. In: Misa, J. Brey, P & Feenberg, A. 2003. *Modernity and Technology*. Cambridge, Massachusetts: The MIT Press, 161-184.
- Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
- Martin, K. van Brakel, R. & Bernhard, D. 2009. Understanding Resistance to Digital Surveillance. Towards a Multi-disciplinary, Multi-actor framwork. *Surveillance and Society* 6 (3), 213-232.
- Marx, G. 1985. I'll Be Watching You: Reflections on the New Surveillance. *Dissent 28*, 26–34.
- Marx, G. 2002. What's New about the "New Surveillance"? Classifying for Change and Continuity. *Surveillance & Society* 1 (1), 9-29.
- Marx, G. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Isssues* 59 (2), 369-390.
- Marx, G. 2005. Seeing Hazily (But Not Darkly) through the Lens: Some Recent Empirical Studies of Surveillance Technologies. *Law & Social Inquiry* 30(2), 339-399.
- McAdam, D. & Snow, D. 1997. *Social Movements: Readings on their Emergence, Mobilization, and Dynamics*. Los Angeles: Roxbury Press.
- Mulgan, G. 1991. *Communication and Control: Networks and the New Economies of Communication.* Cambridge: Polity Press.
- Rapoport, M. 2012. The Home Under Surveillance: A Tripartite Assemblage. *Surveillance & Society* 10 (3), 320-333.
- Rugiero, V. & Montagna, N. 2008. *Social Movements. A Reader*. London: Routledge
- Schneier, B. 2012. *Carry On: Sound Advice from Schneier on Security*. Indianapolis: John Wiley & Sons, Inc.

- Scott, J. 1985. *Weapons of the Weak: Everyday Forms of Peasant Resistance*. Connecticut: Yale University Press,
- Solove, D. 2004. *The Digital Person*. New York: New York University Press.
- Solove, D. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review* 44, 745-772.
- Wood, D. , Ball, K., Lyon, D., Norris, C., & Raab, C. 2006. A Report on the Surveillance Society. *Surveillance Studies Network UK*. Office of the Information Commissioner: London. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf. Geraadpleegd op 01 juni 2014.
- Waite, L. 2001. Divided Consciousness: The impact of black elite consciousness on the 1966 Chicago Freedom movement. In Mansbridge, J. & Morris, A. (red.) 2001. *Oppositional consciousness: The subjective roots of social protest*. Chicago: University of Chicago Press, 170-203.
- W.R.R. 2011. *IOverheid*. Wetenschappelijke Raad voor het Regeringsbeleid (86). Amsterdam: Amsterdam University Press.

Geraadpleegde websites

Bits of Freedom

- http://www.bof.nl
- http://www.bof.nl/ons-werk/internetvrijheid-toolbox/
- http://www.bof.nl/ons-werk/onze-successen/
- http://www.bof.nl/over-ons/de-beweging/

Facebook

- http://www.facebook.com/about/graphsearch

Office of the Information Commissioner: London

- http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

Rijksoverheid

- http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/02/04/kamerbrief-met-reactie-op-berichtgeving-metadata-telefoonverkeer.html

Roger Clarke

- http://www.rogerclarke.com/DV/DigPersona.html

Wetenschappelijke Raad voor het Regeringsbeleid

- http://www.wrr.nl/publicaties/publicatie/article/ioverheid/

Alle geraadpleegde websites zijn op 28 juni 2014 gecontroleerd op beschikbaarheid.

Bijlage 1: Uitnodiging volgers op Facebook

Ben jij fan van Bits of Freedom? Of steun je de standpunten en het werk van Bits of Freedom? Dan wil ik in het kader van mijn afstudeeronderzoek graag met jou spreken. Klik op de info knop hieronder voor meer informatie.

Beschrijving

In het onderzoek richt ik mij op gevolgen van digitale en technologische ontwikkelingen voor de samenleving. Bedrijven, organisaties en overheden verzamelen steeds meer persoonlijke informatie. Welke sociale gevolgen dit heeft voor de personen die leven in een dergelijke samenleving, is een centrale vraag binnen mijn onderzoek.

Vanuit deze vraag zou ik graag met u willen spreken over de achtergrond van uw steun aan Bits of Freedom alsmede uw zienswijze op digitale burgerrechten en de bescherming van persoonsgegevens. Voor vragen en aanmeldingen kunt u mailen naar 305359jk@student.eur.nl of mij een bericht sturen via deze pagina.

Justin Klein

Masterstudent Sociologie

Erasmus Universiteit te Rotterdam