

# TECHNOLOGISCHE ONTWIKKELING DOOR DE BRIL VAN GOOGLE

Discoursvorming door Google bij de introductie van Glass



Masterthesis

Nieuwe Media & Digitale Cultuur

26 februari 2014

Stijn van Grol

Studentnummer: 3263924

Tutor: René Glas

Tweede lezer: Imar de Vries

## **SAMENVATTING**

Dit onderzoek belicht de wijze waarop Glass door Google wordt geïntroduceerd en het discours dat daarmee wordt neergezet. De focus ligt op de aanwezige camera van dit soort wearables en de wijze waarop dit implicaties heeft voor privacy en macht. Er wordt in kaart gebracht hoe Google vorm geeft aan het discours rondom Glass en welke aspecten daarbij worden benadrukt of juist onderbelicht. In het theoretisch kader wordt aangetoond hoe de toename van zowel surveillance als sousveillance (Mann 2003) gevolgen heeft voor privacy en macht in een maatschappij. Duidelijk wordt dat gebruikers van Glass zich onderwerpen aan corporate surveillance (Campbell & Carlsson 2002) en niet-gebruikers worden ongevraagd onderworpen aan sousveillance. Een kritische discoursanalyse laat vervolgens zien op welke wijze Google in haar communicatie spreekt over Glass en welke rol potentiële implicaties daarbij spelen. Uit de analyse volgt dat Google een duidelijk technologisch deterministisch beeld naar buiten brengt waarbij het concept privacy en het belang hiervan erg eenzijdig wordt voorgesteld. Zowel het beeld dat Google schetst als de visie van Mann op wearables om onze surveillancemaatschappij te doorbreken, behoeven dan ook enige nuance.

**Keywords:** surveillance, sousveillance, privacy, macht, Google Glass

## INHOUDSOPGAVE

Inleiding	4
1. Surveillance, sousveillance, privacy en macht	11
1.1 Van surveillance naar sousveillance	11
1.2 Van panopticon naar neo-panopticon	13
1.3 Impliciete participatie en corporate surveillance	15
1.4 Privacy in een steeds transparantere samenleving	16
2. Technologische ontwikkeling door de bril van Google	19
2.1 Google's visie op technologie	19
2.2 Gebruikers aan de macht	20
2.3 Eerst ervaren, dan oordelen	22
2.4 Technologie dichterbij en uit de weg	23
2.5 Het komt eraan, of je het nu wilt of niet	24
3. Overall ogen: opgelet of opgelucht?	28
3.1 Het Borg Complex	28
3.2 Niks te verbergen?	29
3.3 Glass & sousveillance	30
Conclusie	32
Bibliografie	34

Bijlage: brief Google over privacy Glass, 7 juni 2013

## INLEIDING

We already live in a surveillance society. Massive surveillance systems underpin modern existence, from CCTV cameras to the processing of our transactions using bank, credit and loyalty cards. These systems represent a basic, complex infrastructures which assumes that gathering and processing personal data is vital to contemporary living (Williamson 2008: 5).

Op steeds meer plekken staan 'oplettende ogen' op ons gericht. Surveillance camera's zien we onder andere in winkelstraten, scholen en op werkplekken. Door de verdeckte opstelling zijn we ons er niet altijd van bewust, maar in feite worden we op heel veel plekken gefilmd. Wat er precies gebeurt met deze data en wie er eigenlijk naar ons kijken, is voor velen onduidelijk. En waarom zouden we ons hier eigenlijk zorgen over maken, we hebben toch niks te verbergen? Het zorgt immers voor een gevoel van veiligheid en het nut van de vele camera's om ons heen wordt regelmatig bevestigd. Het gaat echter al lang niet meer alleen om surveillance camera's. De komst van de mobiele telefoon heeft ervoor gezorgd dat tegenwoordig vrijwel iedereen een (video)camera binnen handbereik heeft. Daarnaast zien we bijvoorbeeld in de sportwereld steeds meer helmcamera's en in landen als Rusland wordt al veelvuldig gebruik gemaakt van 'dashcams'.<sup>1</sup> De komst van 'wearable computing' zoals Google Glass is hierin de volgende stap. Deze 'bril' is uitgerust met een camera, die constant gericht staat op datgene waar de drager naar kijkt. Google tracht deze nieuwe technologie op een bepaalde manier aan ons voor te stellen, waarbij vanzelfsprekend bepaalde aspecten van de bril zoveel mogelijk worden benadrukt, terwijl andere aspecten weer onderbelicht blijven.

In januari van dit jaar ontstond er veel ophef in de media toen beveiligingsbeelden werden verspreid van een mishandeling door een groep van acht Belgische jongeren in Eindhoven. Deze jongeren konden snel worden opgepakt en dankzij de beveiligingscamera's was er een duidelijk beeld van wat er zich die nacht precies had afgespeeld. Naast dit soort beelden afkomstig van surveillance camera's worden dergelijke incidenten ook steeds vaker vastgelegd door omstanders. Tegenwoordig heeft bijna iedereen wel een mobieltje uitgerust met een (video)camera, waarvan de beeldkwaliteit steeds beter wordt. Regelmatig roept de politie burgers dan ook op om

---

<sup>1</sup> Dashcams zijn videocamera's die worden bevestigd aan de voor en/of achterraut van een auto. In landen als Rusland wordt het beeldmateriaal veelal ingezet als bewijsmateriaal voor verzekeringskwesties.

eventuele opnames van een incident te overhandigen. Hierdoor kan vanuit verschillende perspectieven bekeken worden wat er precies is gebeurd. Dit gebeurde bijvoorbeeld bij het onderzoek naar de rellen bij 'Project X Haren', waar de politie na oproepen via Twitter en andere media erg veel beeldmateriaal van omstanders verzamelde. Mede dankzij deze beelden kon een groot deel van de relschoppers uiteindelijk worden opgepakt en berecht. Deze opnames gemaakt door omstanders kunnen gezien worden als 'sousveillance'. Dat is eigenlijk omgekeerde surveillance, of letterlijk: 'kijken vanaf beneden' (Mann 2003: 332). Deze sousveillance staat tegenover surveillance, wat letterlijk 'kijken vanaf boven' betekent. We worden dus niet meer alleen in de gaten gehouden 'van bovenaf', maar kijken ook terug naar autoriteiten en bedrijven en houden tegelijkertijd elkaar in de gaten. Dergelijke technologieën brengen daarmee bepaalde implicaties met zich mee op het gebied van privacy en macht, en de ontwikkeling hiervan dient dan ook kritisch belicht te worden.

Mobiele en wearable technologieën zorgen ervoor dat we steeds meer en gemakkelijker foto's en video's kunnen maken in de openbare ruimte. Mobieltjes en andere camera's dienen vaak eerst nog uit een tas of broekzak gehaald te worden, maar wearables zorgen ervoor dat dit niet meer nodig is. Dit zorgt er voor dat het niet of nauwelijks meer zichtbaar is wanneer er gefilmd wordt. Zo zijn er al meerdere smartwatches te koop die zijn uitgerust met camera's en bestaat er tevens lifelogging apparatuur. Dit zijn compacte en draagbare apparaten uitgerust met een videocamera en GPS. Je bevestigt het apparaat aan je kleding of hangt het om je nek, zodat constant beelden worden opgenomen van alles wat je doet.<sup>2</sup> Hierdoor wordt er een soort tijdlijn van je leven geconstrueerd, waardoor je kunt terugkijken wat je hebt gedaan en waar je bent geweest. Erg bekend zijn dergelijke apparaten momenteel nog niet. Veel meer hoor je in de media over Glass. Hoewel dit product enkel nog verkrijgbaar is voor een select groepje mensen via het zogenaamde 'Glass Explorer Program', wordt er al veel over geschreven en gesproken. Glass is een draagbare computer in de vorm van een bril, uitgerust met een camera en een klein transparant display dat vlakbij het oog van de gebruiker geplaatst is. Dit soort displays wordt ook wel '(optical) head-mounted displays' genoemd. Glass heeft functies die ook op veel smartphones te vinden zijn: je kunt er bijvoorbeeld mee navigeren, berichten lezen of versturen en Google raadplegen. Ook stelt het gebruikers in staat om direct vanuit point-of-view (POV) perspectief te fotograferen of filmen en deze beelden

---

<sup>2</sup> Reeds verkrijgbare voorbeelden hiervan zijn de Narrative ([getnarrative.com](http://getnarrative.com)) en de Autographer ([autographer.com](http://autographer.com)). Dit zijn allebei kleine apparaten die je bevestigt aan je lichaam of kleding waarna volgens een bepaalde interval automatisch beelden gemaakt worden.

eventueel live of achteraf te delen met anderen.<sup>3</sup> Google zelf heeft enkele maanden geleden een promotievideo gemaakt die de mogelijkheden van de technologie laat zien, waarbij met name het beeld wordt geschetst van technologie als middel om ons leven leuker en makkelijker te maken (Google Glass 2013a). Vanzelfsprekend worden in dit soort video's de potentiële gevolgen op het gebied van privacy niet getoond. Maar wat betekent het eigenlijk als we straks allemaal zijn 'uitgerust' met een (video)camera en alles om ons heen vastleggen?

Het zorgt er in ieder geval voor dat het aantal camera's om ons heen verder toeneemt en dit is van direct invloed op onze privacy. We leven echter al veel langer in een maatschappij waarin we op heel veel plekken gefilmd worden. In het debat rondom privacy is er al veel wetenschappelijk onderzoek gedaan naar surveillance. Onder andere socioloog David Lyon betoogt dat we leven in een surveillance-maatschappij (Lyon 2001: 4). Theoloog en historicus M.G. Michael en filosoof Katina Michael gaan hierin nog een stap verder en waarschuwen dat we op weg zijn naar een staat van 'Überveillance' (Michael & Michael 2010: 9). Zij definiëren dit concept als: "An omnipresent electronic surveillance facilitated by technology that makes it possible to embed surveillance devices in the human body" (Michael & Michael 2009: 1094). Glass en allerlei reeds verkrijgbare technologieën zoals lifelogging apparaten en smartwatches kunnen gezien worden als een volgende stap in deze ontwikkeling. Een pionier in het denken over en gebruiken van wearables is Steve Mann, een professor aan de 'Department of Electrical and Computer Engineering' en onderzoeker op het gebied van wearable computing. Sinds het begin van de jaren zeventig heeft hij verschillende draagbare computers gecreëerd die geschikt zijn voor gebruik in het dagelijks leven (Mann & Ferenbok 2013: 21). In 1994 begon hij met het opnemen en verzenden van zijn leven, 24 uur per dag, zeven dagen per week. In 1998 startte hij een community van lifeloggers waarvan inmiddels meer dan 100.000 leden deel uitmaken (Mann & Ferenbok 2013: 27).<sup>4</sup> Hij ziet wearables als ideale mogelijkheid om de huidige surveillance-maatschappij te veranderen en stelt dat sousveillance de eenzijdige macht ten gevolge van surveillance doorbreekt, waardoor een meer evenwichtige verdeling van macht tot stand komt (Mann 2003: 347). Ook filosoof en informaticus Jean-Gabriel Ganascia (2010) omschrijft deze verschuiving. Hij introduceert hiertoe de term 'catopticon', afgeleid van het panopticon van Jeremy Bentham (1791). In tegenstelling tot het panopticon maakt de architectuur van het

---

<sup>3</sup> Meer over de werking van Glass is te vinden via de YouTube playlist 'Glass Tips': <http://www.youtube.com/playlist?list=PLyR4fvjGTgA65BkribVHAWT9luPIExw5>

<sup>4</sup> De website van de community is te vinden via [www.glogger.mobi](http://www.glogger.mobi)

catopticon het mogelijk dat iedereen met elkaar kan communiceren en ontstaat er transparantie en gelijkheid. Dit onderzoek haakt in op het wetenschappelijk debat rondom privacy met betrekking tot surveillance en sousveillance en nuanceert de voordelen die volgens onder andere Mann en Ganascia voortvloeien uit een toename van sousveillance in onze maatschappij.

Wearables als Glass kunnen van grote invloed zijn op de praktijk van sousveillance. Dit maakt het interessant om te onderzoeken hoe Google een product als Glass presenteert. Met andere woorden, hoe ze ons de technologie 'verkopen'. In dit theoretisch-analytisch onderzoek wordt gekeken hoe een machtig en discoursbepalend bedrijf als Google dit doet. Glass wordt als casestudy gebruikt en door middel van een discoursanalyse wordt de introductie van deze nieuwe technologie in kaart gebracht. Ook zal zichtbaar worden of zaken als privacy en eventuele machtsverschuivingen niet onderbelicht blijven. Met het discours wordt in dit onderzoek een bepaalde manier van spreken bedoeld, zoals Foucault dit omschrijft in *The Archeology of Knowledge and the Discourse on Language* (1972). Hierin spreekt hij over een discoursanalyse naar het seksuele gedrag van mensen, een analyse die later terugkomt in *The History of Sexuality* (1978):

It would reveal, not of course as the ultimate truth of sexuality, but as one of the dimensions in accordance with which one can describe it, a certain 'way of speaking'; and one would show how this way of speaking is invested not in scientific discourses, but in a system of prohibitions and values. An analysis that would be carried out not in the direction of the episteme, but in that of what we might call the ethical (Foucault 1972: 193).

De benadering van Foucault ziet het discours dus als een bepaalde manier waarop gesproken wordt over de werkelijkheid. Het benadrukken van bepaalde aspecten en onderbelichten van andere aspecten geeft vorm aan deze werkelijkheid. Een discoursanalyse volgend de Foucauldiaanse traditie richt zich doorgaans namelijk op de invloed van taal op machtsstructuren en de relatie tussen macht en taal (Foucault 1972; Given 2008: 249). Foucault benadert discourses als:

Systems of thoughts composed of ideas, attitudes, courses of actions, beliefs and practices that systematically construct the subjects and the worlds of which they speak. He traces the role of discourses in wider social processes of legitimation and power, emphasizing the constitution of current truths, how they are maintained and what power relations they carry with them (Lessa 2006: 285).

Het discours en de macht die hiermee wordt uitgeoefend omvat volgens Foucault dus veel meer dan slechts het tekstuele aspect. Dit wordt benadrukt door Derek Hook (2001), onderzoeker op het gebied van psychologie en auteur van verschillende wetenschappelijke artikelen over Foucault en zijn methode van discoursanalyse. Hoewel hij betoogt dat er geen vaststaande Foucauldiaanse discoursanalyse bestaat (Hook 2011: 36), kunnen er volgens hem wel een aantal eigenschappen gedefinieerd worden die een analyse meer binnen de Foucauldiaanse traditie plaatsen (Hook 2011: 37). Allereerst is het van belang om de historische context van het discours te betrekken bij de analyse. In het geval van Glass heeft dit niet slechts betrekking op de wijze waarop in het verleden technologieën geïntroduceerd zijn. Het is tevens relevant om Glass te plaatsen in de al veel langer bestaande opkomst van surveillance en sousveillance en de discussie rondom privacy die hiermee gepaard gaat. Hieruit voortvloeiend stelt Hook dat er gekeken moet worden naar de sociale, historische en politieke voorwaarden van waaruit bepaalde uitspraken als waar of onwaar gezien worden (Hook 2011: 37). Ook moet er bij een analyse in de Foucauldiaanse traditie rekening gehouden worden met de 'materialiteit' van een uitspraak (Hook 2011: 38). Foucault stelt over deze materialiteit: "It is constitutive of the statement itself: a statement must have a substance, a support, a place, and a date. And when these requisites change, it too changes identity" (Foucault 1972: 101). Samengevat stelt Hook over deze drie eigenschappen: "The analysis of discourse, according to a Foucauldian perspective, cannot remain simply *within* the text, but needs to move, in Said's (1983) formulation, both in and out of the text" (Hook 2011: 38). Deze methodologische eigenschappen vormen niet de directe leidraad voor de uitgevoerde analyse in dit onderzoek, maar zijn vooral bedoeld om de lezer de juiste 'bril' op te laten zetten.

Een Foucauldiaanse analyse kan specifiek inzichtelijk maken hoe Google spreekt over concepten als privacy en hoe via het discours macht wordt uitgeoefend. De manier waarop Glass door Google wordt gepresenteerd kan beïnvloeden wat vervolgens door consumenten en andere media wordt gezien als waarheid. De analyse laat niet zien wat de gevolgen zijn van het door Google neergezette denkkader op de manier waarop



bijvoorbeeld grote technologie-blogs schrijven over Glass, maar wel op welke wijze Google dit denkkader vormt via het gebezigde discours. Hiermee richt dit onderzoek zich dus onder andere op hetgeen Google als norm of waarheid neerzet, welke aspecten worden benadrukt of onderbelicht en welke belangen daarbij een rol spelen. De volgende vraag is centraal gesteld:

*Hoe geeft Google in haar externe communicatie vorm aan het discours rondom Glass en welke aspecten worden hiertoe benadrukt of juist onderbelicht?*

Het eerste hoofdstuk vormt het theoretisch kader waarin aangetoond wordt hoe de toename van zowel surveillance als sousveillance gevolgen heeft voor privacy en macht in een maatschappij. Met dit hoofdstuk wordt tevens de historische context rondom de introductie van Glass in kaart gebracht. Aan de hand van het panopticon wordt de werking van macht uitgelegd (Foucault 1977) en wordt duidelijk dat het panopticon ook nog relevant is in onze huidige samenleving. Mann (2003) noemt dit neo-panopticons, aangezien er een groot verschil is in de manier waarop de data worden verzameld en geanalyseerd. Dit komt niet alleen voort uit toezicht door autoriteiten, maar tevens door middel van corporate surveillance (Campbell & Carlson 2002). Betoogd wordt dat de toename van camera's en wearables als Glass een conditionerend effect op de gebruikers en omgeving tot stand kan brengen, waardoor we steeds meer terecht komen in een 'control society' (Deleuze 1992). Privacy lijkt voor Google van ondergeschikt belang en wordt zelfs gebruikt als synoniem voor het willen verbergen van illegale of negatieve informatie. Het wordt daarmee echter op een eenzijdige manier benaderd terwijl het belang van privacy al vaak is onderschreven (Rachels 1975; Reiman 1976; Solove 2008). In dit hoofdstuk wordt uiteindelijk duidelijk in hoeverre wearables als Glass gevolgen hebben voor de praktijk van surveillance en sousveillance, en op welke manier dit weer implicaties met zich meebrengt op het gebied van privacy en macht.

In het tweede hoofdstuk wordt gekeken hoe er door Google over Glass wordt gesproken. Gekeken wordt of hierbij de gevolgen worden betrokken die naar voren zijn gekomen in het eerste hoofdstuk. Aan de hand van Thad Starner, een expert en pionier op het gebied van wearables en werkzaam als 'Technical Lead/Manager' voor Google Glass, wordt de visie van Google op technologie geïntroduceerd. Door middel van een Foucauldianse discoursanalyse wordt vervolgens in kaart gebracht hoe Google spreekt over Glass en op welke manier het discours rondom deze nieuwe technologie wordt gevormd. De analyse beperkt zich niet slechts tot geschreven taal, er wordt tevens

gekeken naar video's van het officiële YouTube-kanaal van Glass. Hoewel er namelijk erg veel wordt geschreven over Glass, komt er nog maar weinig officiële communicatie naar buiten vanuit Google. Dit lijkt een bewuste keuze en kan dan ook gezien worden als onderdeel van de discoursvorming over Glass. Het bedrijf laat het hiermee aan anderen over om te speculeren over Glass. De beperkte hoeveelheid informatie die naar buiten wordt gebracht, heeft tevens tot gevolg dat het meteen enorm breed wordt uitgelicht in de media wanneer er wel iets wordt gecommuniceerd. Er wordt daarom ingezoomd op een aantal belangrijke bronnen. Centraal staat een brief waarin Google reageert op de zorgen rondom privacy (zie bijlage). Ook worden introductievideo's van Glass belicht en worden uitspraken van Google-medewerkers met betrekking tot privacy besproken.

Deze analyse maakt het vervolgens mogelijk om in het derde hoofdstuk een meer genuanceerd beeld te vormen over de implicaties die volgen uit de opkomst van technologieën als Glass. Dit hoofdstuk vormt dus een reflectie op de verkregen onderzoeksresultaten uit het tweede hoofdstuk. Uit de manier waarop Glass wordt geïntroduceerd blijkt dat technologische ontwikkelingen zoals Glass door Google worden genormaliseerd. Dit terwijl er op het gebied van macht duidelijke gevolgen zijn, waaronder de conditionerende macht die een dergelijke technologie met zich meebrengt. Ook zijn er duidelijke implicaties op het gebied van privacy en blijkt dat Google zelf een erg eenzijdig beeld neerzet van dit concept en het maatschappelijk belang ervan. Tot slot wordt betoogd dat zowel het beeld dat Google neerzet als de visie van Steve Mann op sousveillance enige nuance behoeven.

## 1. SURVEILLANCE, SOUSVEILLANCE, PRIVACY EN MACHT

Dankzij mobiele en draagbare technologieën krijgen we steeds meer mogelijkheden om onze omgeving op elk gewenst moment vast te leggen, terwijl ook de surveillance om ons heen toeneemt. Wearables als Glass maken sousveillance steeds laagdrempeliger, aangezien ze bevestigd worden aan ons lichaam en direct geactiveerd kunnen worden. Sommigen zien deze nieuwe technologie als ideaal middel om onze surveillance-maatschappij te doorbreken. Toch zorgt het tegelijkertijd voor een verdere toename van het aantal camera's om ons heen. Dit heeft directe gevolgen voor onze privacy en je kunt je daarom afvragen of technologieën als Glass wel wenselijk zijn. In dit hoofdstuk wordt duidelijk op welke manier surveillance en sousveillance zich momenteel ontwikkelen en wat hiervan implicaties zijn op het gebied van privacy en macht. Dit kan vervolgens vergeleken worden met de bevindingen uit de discoursanalyse in het tweede hoofdstuk, waarbij gekeken wordt op welke manier Google dit benadert bij de introductie van Glass.

### 1.1 Van surveillance naar sousveillance

Steve Mann ziet wearables als ideaal middel om 'terug te kijken' naar autoriteiten of corporaties. Hij schetst een utopisch beeld van technologieën zoals Glass, die volgens hem de potentie hebben om de kracht van surveillance tegen te gaan en hiermee een meer evenwichtige verdeling van sociale controle tot stand te brengen. Hierdoor zou een samenleving ontstaan met een constant 'dialogoog' tussen gevangenen en bewaarders, politici en burgers, en bureaucraten en mensen (Mann en Ferenbok 2013: 25). Hij stelt:

Newly developed technology allows them to surveil the surveillers. In affording all people to be simultaneously master and subject of the gaze, wearable computing devices offer a new voice in the usually one-sided dialogue of surveillance. They suggest a way towards a self-empowering sousveillance for people as they traverse their multiple and complex networks (Mann et al. 2003: 348).

Mann introduceerde daartoe de term 'sousveillance', dat letterlijk 'kijken vanaf beneden' betekent (Mann et al. 2003: 332). Dit wordt bedoeld in hiërarchische context, dus bijvoorbeeld als een gevangene een bewaarder observeert of als een burger het gedrag van de politie filmt. Op het moment dat degene die observeert zich bevindt in een hogere machtspositie ten opzichte van de geobserveerde, is er sprake van surveillance. Als de observerende persoon een lagere machtspositie heeft dan de geobserveerde, dan is er

dus sprake van sousveillance. In een recenter werk stelt hij: “Sousveillance changes the relationships between the asymmetric paradigm for social control that Foucault discussed as the formational characteristics of modern societies - what he termed the panoptic gaze” (Mann & Ferenbok 2013: 25).

Volgens Jean-Gabriel Ganascia zorgt sousveillance voor het ontstaan van het catopticon (Ganascia 2010: 497). In tegenstelling tot het panopticon gaat dit principe uit van totale transparantie van de maatschappij, fundamentele gelijkheid waardoor iedereen elkaar kan observeren en controleren, en volledige communicatie, waardoor informatie onderling tussen iedereen kan worden uitgewisseld (Ganascia 2010: 497). Hij benadrukt echter dat surveillance hierdoor niet verdwijnt, maar dat surveillance en sousveillance naast elkaar zullen blijven bestaan. Volgens Steve Mann draagt dit bij aan het bereiken van een soort evenwicht. Hij noemt dit het ‘equveillance’ (Mann 2013: 26). Dit verandert echter niks aan de wijze waarop surveillance door zowel autoriteiten als door bedrijven plaatsvindt.

De recente onthullingen van Edward Snowden over de NSA en het PRISM-programma tonen hoe relevant het door Michel Foucault (1977) omschreven panopticon en ‘panoptic gaze’ op dit moment nog is. De hele wereld heeft nu kunnen zien in hoeverre we tegenwoordig gevolgd kunnen worden door inlichtingendiensten en hoe een dergelijke instantie lange tijd ongezien en zonder enig toezicht enorme hoeveelheden informatie kan verzamelen van mensen over de hele wereld. Het panopticon werd in 1791 als architectonisch principe geïntroduceerd door de Engelse Verlichtingsfilosoof Jeremy Bentham. Foucault gebruikt het panopticon als een metafoor voor de werking van macht. Over de architectuur stelt hij:

We know the principle on which it was based: at the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other, on the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy (Foucault 1977: 200)

Hoewel het panopticon vaak direct wordt geassocieerd met een gevangenis, is dit dus zeker niet de enige manier waarop het principe kan worden ingezet. Volgens Bentham kan

het panopticon tevens gebruikt worden voor de verschillende afgesloten omgevingen als het ziekenhuis, de school of de werkplaats. Hij stelt dat de macht gebaseerd moet zijn op zichtbaarheid en onzekerheid. Foucault beschrijft dit:

Visible: the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon. Unverifiable: the inmate must never know whether he is being looked at at any one moment; but he must be sure that he may always be so (Foucault 1977: 201)

Bewoners van het panopticon weten dus nooit wanneer ze wel of niet bekeken worden en houden hiermee eigenlijk zichzelf in de gaten. Ze corrigeren hun eigen gedrag en zijn daarmee zowel gevangene als bewaarder geworden (Foucault 1977: 202-203). Het gaat dan dus niet zozeer om de werkelijke kracht van de autoriteit, maar om de potentie dat men bekeken wordt. Daarnaast draait het panopticon om het verzamelen van kennis over de bewoners, het is 'a system of intense registration and of documentary accumulation' (Foucault 1977: 189). Dit verzamelen van kennis doet niet alleen denken aan de wijze waarop de NSA en andere inlichtingendiensten dit doen, maar tevens aan bedrijven als Facebook en Google. Net als autoriteiten hebben zij er baat bij om zoveel mogelijk over ons te weten (zie ook sectie 1.3).

## **1.2 Van panopticon naar neo-panopticon**

In de huidige maatschappij zien we het panopticon overal terug in de vorm van surveillancecamera's. Dit is een typisch voorbeeld van de verschuiving van de 'disciplinary societies' naar de 'societies of control', zoals de Franse filosoof Gilles Deleuze beschrijft (Deleuze 1992: 4). De 'disciplinary societies' werden gekenmerkt door afgesloten omgevingen met ieder een eigen disciplinerende werking van macht. Voorbeelden van deze omgevingen zijn onder andere de school, de werkplaats en het gezin (Deleuze 1992: 3). Volgens Deleuze zorgde het kapitalisme ervoor dat deze gescheiden domeinen in gevaar kwamen. Door de opkomst van de 'societies of control' vervagen de grenzen tussen de verschillende gescheiden omgevingen die ons beïnvloeden en onze identiteit vormgeven (Deleuze 1992: 7). Moderne communicatiemiddelen faciliteren deze verschuiving en zorgen ervoor dat we allemaal verbonden worden middels een netwerk waarbij we constant onder controle staan. Deleuze verwijst hiervoor naar Felix Guattari, die een dystopisch toekomstbeeld schetst van een sterk gecontroleerde maatschappij:

Felix Guattari has imagined a city where one would be able to leave one's apartment, one's street, one's neighbourhood, thanks to one's (dividual)<sup>5</sup> electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position – licit or illicit – and effects a universal modulation (Deleuze 1992: 7).

De huidige ontwikkeling van mobiele en draagbare technologie zorgt ervoor dat het door Guattari geschetste beeld niet ondenkbaar is. Die elektronische kaart hebben we immers allemaal al in onze broekzak: de mobiele telefoon zorgt ervoor dat we tegenwoordig veelal verbonden zijn met het internet en ook de ingebouwde GPS-chip bepaalt onze locatie. Wearables als Glass zorgen ervoor dat deze elektronische kaart straks zelfs aan ons lichaam bevestigd zit en ongezien (video)opnames kan maken vanuit POV-perspectief. Door technologische ontwikkeling verandert ook de aard van surveillance. Mann stelt hierover: "The nature of surveillance itself has been irrevocably changed by digitization, networking and ubiquitous computing" (Mann & Ferenbok 2013: 22). Mann, Nolan en Wellman beschrijven de opkomst van neo-panopticons, die sinds het ontstaan van post-industriële samenlevingen nieuwe communicatiemiddelen uitbuiten (Mann et al. 2003: 335). Ze hekelen de onevenwichtige machtsverhouding die door technologie gemedieerde surveillance tot stand wordt gebracht, aangezien niet iedereen toegang heeft tot dergelijke technologie. Het verschil met het panopticon zit met name in de manier waarop de data worden verzameld en geanalyseerd. Waar het bij het panopticon als gevangenis draaide om toezicht via de ogen van een bewaarder, daar gaat het bij het neo-panopticon om gemediteerd toezicht dat mogelijk wordt gemaakt door technologische ontwikkeling:

Video cameras can be almost invisibly small, communication networks, directing surveillance images to monitors (both people and screens) located elsewhere, and information technology can use facial recognition software to identify likely suspects (Mann et al. 2003: 335).

Hoewel Mann erg optimistisch is over de potentie van wearables als Glass om terug te kijken, zorgt dit ook voor een nieuw soort 'panoptic gaze' in onze maatschappij. Iemand

---

<sup>5</sup> Met 'dividual' bedoelt Foucault het tegenovergestelde van 'individual'. Door moderne surveillance technologie wordt een fysieke persoon gereduceerd tot data en aan de hand hiervan gecategoriseerd tot een bepaalde groep in plaats van een individu.

die is 'uitgerust' met een camera heeft wellicht de mogelijkheid om 'terug te kijken' naar autoriteiten, maar kan tevens opnames maken van elk ander persoon in zijn of haar gezichtsveld. Voor deze omgeving kan dit een conditionerend effect tot gevolg hebben: je weet dat er de mogelijkheid is dat er opnames gemaakt worden, die in de huidige digitale maatschappij ook nog eens direct en zonder toestemming verspreid kunnen worden via het internet. Bewustwording hiervan kan ertoe leiden dat men zich anders gaat gedragen in de openbaarheid. Dit is uiteraard ook nu al het geval bij beveiligingscamera's, maar daarbij is het niet aannemelijk dat de beelden zomaar in de openbaarheid terecht komen. Daarnaast is de huidige sousveillance door bijvoorbeeld telefoons een stuk transparanter, aangezien het vaak duidelijk te zien is wanneer iemand opnames maakt met een mobiele telefoon.

### **1.3 Impliciete participatie en corporate surveillance**

In de wereld waarin we leven gaat het al lang niet meer alleen om informatieverzameling door eerder genoemde inlichtingendiensten of overheden. Er zijn ook allerlei commerciële partijen die zoveel mogelijk informatie over ons verzamelen. Op het internet laten we digitale sporen na: door bijvoorbeeld gebruik te maken van commerciële platformen als Google zorgen we vaak onbewust voor allerlei gebruikersdata. Mirko Tobias Schäfer noemt dit impliciete participatie (Schäfer 2011: 105). Dit staat tegenover expliciete participatie: het bewust participeren op bepaalde platformen, bijvoorbeeld door het toevoegen van content op YouTube of Wikipedia. Data die wordt gegenereerd uit impliciete participatie kan bijvoorbeeld gebruikt worden voor optimalisatie van zoekresultaten of het tonen van relevante advertenties. Ook door gebruik te maken van bijvoorbeeld de bonuskaart van Albert Heijn laten we onbewust waardevolle data achter waarmee ons koopgedrag wordt geregistreerd. Een ander voorbeeld betreft het inloggen op bepaalde websites via je Facebook account, waarmee je als gebruiker vaak bepaalde voordelen krijgt. In al deze voorbeelden kiezen we er eigenlijk zelf voor om ons te laten volgen door commerciële bedrijven. Mediawetenschappers John Edward Campbell en Matt Carlson stellen over deze 'corporate surveillance': "We may have feared the intrusion of Big Brother into our homes and private lives, but we open wide the door to his corporate cousins even as they reduce us to economic abstracts and marketing segments" (Campbell & Carlson 2002: 604).

Campbell en Carlson verwijzen hiermee naar het boek *1984* van George Orwell. Hierin wordt een dystopisch beeld geschetst van een totalitaire staat onder leiding van Big Brother, waarvan de inwoners onder complete surveillance door de autoriteiten verkeren.

Inmiddels lijkt onder andere door de onthullingen van Edward Snowden dat deze dystopie niet meer alleen op fictie berust. Hoewel autoriteiten en bedrijven niet dezelfde motivatie hebben om ons te volgen en dus ook uit zijn op andere informatie, gaat het in beide gevallen om dezelfde techniek: surveillance (Campbell & Carlson 2002: 587). Vanuit het perspectief van bedrijven als Google is het economisch gezien logisch dat zij trachten zoveel mogelijk gebruikersgegevens te verzamelen. Het advertentiebeleid van Google wordt namelijk steeds meer toegespitst op specifieke gebruikers. Advertenties zijn nou eenmaal effectiever wanneer ze zo goed mogelijk aansluiten bij de persoon die ze bekijkt. Om deze gebruikers te identificeren is simpelweg zoveel mogelijk informatie nodig van gebruikers. Glass zorgt ervoor dat we nog directer zijn verbonden met de technologie en maakt de stap om het te gebruiken nog kleiner. Dit maakt het voor de gebruiker gemakkelijker om bijvoorbeeld de verschillende diensten van Google op elk moment te gebruiken, waardoor men bewust of onbewust bijdraagt aan het genereren van nog meer waardevolle gebruikersdata.

#### **1.4 Privacy in een steeds transparantere samenleving**

Deze ontwikkelingen hebben echter wel gevolgen voor onze privacy. Bedrijven als Facebook en Google lijken een transparante samenleving als ideaal na te streven. Zo stelt Facebook de missie te hebben om mensen de macht te geven om te delen en om de wereld meer open en verbonden te maken (Facebook 2013). Google zegt in andere bewoordingen een soortgelijke missie na te streven, namelijk om “alle informatie ter wereld te organiseren en universeel toegankelijk en bruikbaar te maken” (Google 2013). Een meer transparante samenleving impliceert in zichzelf al gevolgen op het gebied van privacy, aangezien daarmee ook steeds meer persoonlijke informatie openbaar toegankelijk wordt. Zoals hiervoor besproken, zorgen bedrijven via corporate surveillance ook nu al dat zoveel mogelijk informatie over ons verzameld wordt. Campbell en Carlson stellen hierover:

An important component of such information transactions is that users choose-or appear to choose-to participate in commercial surveillance. Whereas involuntary surveillance is often perceived as an invasion of privacy, participatory surveillance is envisioned as mutually beneficial, what Davies (1997) identifies as a "partnership" (Campbell & Carlson 2002: 157).



We lijken ons dus minder zorgen te maken over onze privacy wanneer bedrijven ons volgen, gebruikers gaan deze self-surveillance immers zelf aan. Het is echter de vraag of zij wel weten wat er precies gebeurt met deze informatie. Campbell en Carlson noemen de overeenkomst die consumenten met bedrijven aangaan dan ook een "carefully constructed illusion", aangezien we vervolgens geen inzicht krijgen in de onderliggende processen waarmee de verzamelde data geanalyseerd wordt (Campbell & Carlson 2002: 593). Voor bedrijven als Google en Facebook lijkt dit niet in lijn met hun streven naar transparantie. Hoewel veel gebruikers deze overeenkomsten niet zien als privacyschending, kunnen ze wel op die manier geïnterpreteerd worden. Dit blijkt ook uit de taxonomie van rechtsgeleerde Daniel Solove (2007), die tracht de verschillende soorten problemen en schendingen van privacy in kaart te brengen. Hij benadrukt dat het analyseren van privacy-gerelateerde kwesties lastig is, aangezien er vaak geen specifieke Big Brother aan te wijzen is (Solove 2004: 33-35). Privacy moet volgens hem niet worden gezien als een eenduidig concept, maar als een "plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other" (Solove 2007: 9).

De taxonomie van Solove is verdeeld in vier subgroepen die inzichtelijk maken hoe de praktijk van surveillance en sousveillance in verband staat met het concept privacy: 'information collection' (surveillance, interrogation); 'information processing' (aggregation, identification, insecurity, secondary use, exclusion); 'information dissemination' (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion) en 'invasion' (intrusion, decisional interference) (Solove 2007: 11). De concepten achter iedere subgroep zijn slechts voorbeelden van de problemen of schendingen die voortvloeien uit de subgroep. Wanneer gekeken wordt naar surveillance en sousveillance in de context van privacy, wordt de kwestie van informatieverzameling, informatieverwerking, informatieverbreiding en indringing duidelijk. Door bijvoorbeeld plaatsing van videocamera's of door gebruik te maken van draagbare foto- of videoapparatuur is het mogelijk om beelden te verzamelen. Deze beelden worden vervolgens opgeslagen. Vroeger gebeurde dit analoog, tegenwoordig wordt het digitaal opgeslagen op een harde schijf of 'in de cloud'. Dit kan vervolgens effect hebben op iemands privacy: de verzamelde videobeelden van een bepaalde persoon kunnen bijvoorbeeld worden gekoppeld aan andere informatie, waardoor een duidelijker profiel ontstaat. Daarmee kan deze persoon op de beelden ook geïdentificeerd worden. De volgende stap betreft het proces van verspreiding, dus wat er precies gebeurt met de beelden die zijn opgenomen en opgeslagen. Mogelijke voorbeelden van problemen die

zich voor kunnen doen bij verspreiding zijn onwenselijke zichtbaarheid via bijvoorbeeld social media, of het chanteren van individuen die erop zijn vastgelegd. Tot slot hangen de zojuist genoemde kwesties weer samen met indringing in iemands leven en kan het invloed hebben op de keuzes die deze persoon vervolgens maakt. Mensen die zich bewust zijn van dit proces kunnen zich dus anders gaan gedragen wanneer de kans bestaat dat zij gefotografeerd of gefilmd worden.

Het is in dit hoofdstuk helder geworden dat naast surveillance ook sousveillance zich steeds verder ontwikkelt in onze maatschappij. Het zijn niet alleen overheden en inlichtingendiensten die zorgen voor surveillance, maar ook allerlei bedrijven en mensen op straat. In de huidige digitale wereld is de verspreiding van informatie veel gemakkelijker en toegankelijk voor meer mensen. Wearables zorgen ervoor dat deze verspreiding nog directer kan en dankzij de aanwezige camera is het vervaardigen van beelden tevens veel laagdrempeliger. Tegelijkertijd zorgen wearables voor implicaties op het gebied van macht voor de gebruiker. Het gaat dan echter niet alleen op de wijze waarop deze kunnen worden ingezet voor de praktijk van sousveillance zoals Mann betoogt, maar tevens om de conditionerende werking voor de omgeving en de gebruiker zelf die dergelijke technologieën tot gevolg kunnen hebben (zie ook sectie 3.3). Gebruikers verkrijgen een hogere machtspositie ten opzichte van niet-gebruikers. Niet-gebruikers hebben namelijk geen directe invloed op hetgeen er precies wordt opgenomen en verspreid. Hoewel betoogd kan worden dat wearables de transparantie binnen een maatschappij ten goede komen, hebben ze grote gevolgen op het gebied van privacy. Ook heeft een technologie als Glass niet alleen gevolgen voor de praktijk van sousveillance, maar tevens voor corporate surveillance. Glass verbindt de gebruiker nog directer met de technologie, waardoor het gebruik toegankelijker wordt. Dit past in de bedrijfsstrategie van Google, die immers zoveel mogelijk over ons wil weten om hiermee steeds effectievere advertenties te kunnen bieden.

## **2. TECHNOLOGISCHE ONTWIKKELING DOOR DE BRIL VAN GOOGLE**

Aan de hand van de implicaties van wearables als Glass die naar voren zijn gekomen in het theoretisch kader, kan nu gekeken worden op welke wijze deze worden belicht in het discours van Google over Glass. Hiertoe wordt eerst het beeld dat Google schetst van technologie geïntroduceerd aan de hand van Thad Starner, een expert en pionier op het gebied van wearables en werkzaam als 'Technical Lead/Manager' voor Google Glass. Hierna wordt specifiek ingezoomd op Glass en door middel van een Foucauldiaanse discoursanalyse wordt getoond hoe Google spreekt over Glass. In bredere context wordt hiermee aangetoond op welke manier er door Google wordt gesproken over technologie en hoe concepten als privacy en macht hierbij betrokken worden. Er wordt onder andere gekeken naar hetgeen Google als norm of waarheid neerzet, welke aspecten worden benadrukt of onderbelicht en welke onderliggende belangen een rol spelen. In dit hoofdstuk staat een brief centraal die Google stuurde naar Joe Barton, een Congreslid in de Verenigde Staten, die zijn zorgen uitlet over de privacy-aspecten van Glass (zie bijlage). De brief werd verstuurd op 7 juni 2013 en is ondertekend door Susan Molinari, hoofd van de afdeling Public Policy and Government Relations. Zowel de inleidende brief als de antwoorden op de gestelde vragen zullen aan de discoursanalyse onderworpen worden. In de brief wordt verwezen naar een tweetal video's: een video op het YouTube-kanaal over Glass van Google zelf en een video van een conferentie van Google met ontwikkelaars van apps voor Glass. Ook deze video's worden daarom bij de analyse betrokken.

### **2.1 Google's visie op technologie**

Het is lastig om Google's werkelijke visie op technologie te achterhalen. Niet alleen omdat het onwaarschijnlijk is dat deze visie voor alle personen binnen het bedrijf gelijk is, maar ook omdat dit interne bedrijfsinformatie betreft. Wel kan gekeken worden naar de visie die Google uitdraagt. Een voorbeeld hiervan komt naar voren in deze uitspraak van Starner:

I believe if we reduce the time between intention and action, it causes a major change in what you can do, period. When you actually get it down to two seconds, it's a different way of thinking, and that's powerful. And so I believe, and this is what a lot of people believe in academia right now, that these on-body devices are really the next revolution in computing (Starner geciteerd in Metz 2013).

Dit geeft goed het beeld weer dat Google uitdraagt met betrekking tot de rol die wordt beoogd voor technologie in ons leven, waarbij het draait om een streven naar gemak en efficiëntie. De eerder besproken waardevolle data die gebruikers vrijgeven door impliciet te participeren op bepaalde platformen, wordt namelijk niet alleen gebruikt ten behoeve van gepersonaliseerde reclame, maar ook ten behoeve van gebruikerservaring van de verschillende diensten. Toen in 2012 de privacy-voorwaarden van Google werden aangepast, werd met name kritiek geuit op één bepaald aspect: de gebruikersgegevens van alle verschillende Google-diensten konden vanaf dat moment door Google gecombineerd worden. Door alle verzamelde data worden specifieke gebruikers steeds beter geïdentificeerd. Al deze gegevens samen kunnen vervolgens worden ingezet voor de verschillende diensten van Google, waardoor een intuïtievare ervaring geboden kan worden (Google 2012). Het is nu mogelijk om je bijvoorbeeld te waarschuwen wanneer je te laat dreigt te komen voor een afspraak die in je agenda staat, hierbij rekening houdende met je huidige GPS-locatie en de lokale verkeersomstandigheden.

Starner benadrukt in zijn uitspraak de tijdswinst die volgt uit het verkleinen van de tijd tussen intentie en actie en stelt dat je hierdoor uiteindelijk veel meer kunt doen. Een soortgelijke benadering komt naar voren wanneer we kijken naar een andere recente technologie van Google: de zelfrijdende auto. Het bedrijf gaat daarbij duidelijk uit van een positief vrijheidsperspectief en stelt dat we meer vrijheid bereiken wanneer we het autorijden overlaten aan technologie (Van Grol 2012: 11). De negatieve vrijheid wordt echter sterk beperkt, aangezien er allerlei externe factoren zijn die je handelen beïnvloeden. Bij Glass is eenzelfde effect zichtbaar: aan de ene kant zorgt een verkleining van de tijd tussen intentie en actie dat iemand meer tijd overhoudt voor andere dingen, maar tegelijkertijd is deze persoon constant onder invloed van deze technologie die hiermee een deel van het handelingsvermogen overneemt. Wat tot slot opvalt is de manier waarop Thad Starner benadrukt dat wearables toch echt de volgende revolutie zijn op het gebied van computers. Hij versterkt dit nog door te stellen dat veel mensen uit de academische wereld deze mening met hem delen. Hiermee impliceert hij een zekere vanzelfsprekendheid betreffende de komst van deze technologie en de grote veranderingen die het ons gaat brengen (zie ook sectie 2.5).

## **2.2 Google-gebruikers aan de macht**

In de brief van Google aan Joe Barton wordt direct nadruk gelegd op het hoofddoel dat Google voor ogen zegt te hebben met Glass: “Our goal with Glass is to give users control, and we have gotten very positive reactions from those with first-hand experience of the

product”. Dit doel wordt later in de brief nogmaals genoemd: “We build Glass to put users in control”. Er wordt hiermee een beeld neergezet van Glass als technologie die de macht bij gebruikers legt. Google doelt hiermee op de manier waarop gebruikers via de MyGlass-applicatie hun Glass kunnen beheren en instellingen kunnen wijzigen. Dit roept echter direct een andere vraag op waar minder nadruk op wordt gelegd in deze brief, namelijk hoe het zit met implicaties voor de macht of controle van niet-gebruikers. Het zojuist geformuleerde hoofddoel van Google maakt meteen duidelijk dat dit belang ondergeschikt is aan dat van de gebruiker. Google wijst wel op de zichtbaarheid van Glass en de ingebouwde signalen die de omgeving er bijvoorbeeld op wijzen wanneer er wordt opgenomen. Dit is alleen niet geheel in lijn met een recente ontwikkeling van Glass. Toen deze brief door Google geschreven werd, was het inderdaad enigszins zichtbaar was wanneer er gefotografeerd werd. Hiervoor moest immers het transparante scherm aan staan en het commando “OK Glass, take a picture” gegeven worden. Eind 2013 kwam echter een nieuwe versie van Glass beschikbaar die in combinatie met nieuwe firmware ervoor zorgt dat slechts een knipoog voldoende is om een foto te maken. Hierbij hoeft het scherm eveneens niet aan te staan (Adhikari 2013).

Dit doet denken aan de ontwikkeling van de camera op de mobiele telefoon. De eerste mobiele telefoons die waren uitgerust met camera's waren vaak ook voorzien van een ledje waarmee het zichtbaar was wanneer er gefilmd werd, maar tegenwoordig is dit vrijwel nooit meer het geval. Bij de eerder genoemde wearables als de Narrative en Autographer is het nu al niet zichtbaar dat er beelden worden opgenomen en zijn de apparaten zelf ook nauwelijks zichtbaar. Google zegt echter te verwachten dat er vanzelf een zekere etiquette rondom het gebruik van Glass zal ontstaan, zoals dat volgens hen ook al het geval is met bestaande mobiele telefoons, laptops of camera's: “We have also built some social signals into the way Glass is used. These signals help people understand what users are doing, and give Glass users means for employing etiquette in any given situation”. Google stelt eerdere technologische ontwikkelingen hiermee als norm en betoogt dat ook bij deze producten problemen betreffende privacy verwacht werden, maar dat ze nu ook volledig in onze maatschappij geaccepteerd zijn. Maatschappelijke acceptatie betekent echter niet dat de eerdere zorgen rondom privacy als onnodig bestempeld kunnen worden. Een nieuwe technologie wordt immers niet van het ene op het andere moment overal gebruikt en deze geleidelijke introductie kan ervoor zorgen dat de kritiek uiteindelijk afneemt. Het ‘Glass Explorer Program’ lijkt hierbij een ideale manier om ons rustig te laten wennen aan een revolutionair product als Glass en de privacy-implicaties die hierbij komen kijken.

Op een vraag van Joe Barton betreffende de privacy van niet-gebruikers gebruikt Google het voorbeeld van gezichtsherkenning. Het bedrijf stelt hierop: “Google has said for several years that we won’t add facial recognition features to our products without having strong privacy protections in place. With that in mind, we won’t be approving any facial recognition Glassware at this time” (zelf onderlijning toegevoegd). Op gelijke wijze wordt de meer gerichte vraag van Joe Barton betreffende gezichtsherkenning beantwoord, waarmee Google duidelijk de mogelijkheid open laat om gezichtsherkenning uiteindelijk toe te voegen wanneer zij vinden dat de privacy voldoende gewaarborgd blijft. Er is bijvoorbeeld al een applicatie ontwikkeld die objecten live kan herkennen. Het bedrijf AlchemyAPI had al een bestaande beeldherkenningsdienst en heeft deze nu toegepast in een applicatie geschikt voor Glass (eturner303 2013). Hoewel deze functie momenteel dus nog niet wordt ingezet in Glass, geeft deze applicatie van AlchemyAPI wel aan dat de potentie ervoor zeker aanwezig is. Met de bestaande sociale netwerken waarvan tegenwoordig veel mensen deel uitmaken, lijkt de ontwikkeling van een applicatie die deze database gebruikt om live personen te herkennen een kleine stap. Ook kan er via hacks voor gezorgd worden dat dergelijke functionaliteiten al veel eerder mogelijk zijn, zoals de 23-jarige hacker Stephen Balaban al heeft aangetoond (Greenberg 2013). Ook andere recente technologieën zijn al uitgerust met gezichtsherkenning, zoals de onlangs geïntroduceerde Xbox One. Dit wordt gebruikt om specifieke spelers te herkennen en hierop zelfs getoonde advertenties af te stemmen (Vrankulj 2013). In dat geval draait het in ieder geval nog om de gebruiker zelf waarop de gezichtsherkenning is gericht. Bij Glass is de camera gericht op de omgeving en in combinatie met een sociale media als Facebook zijn er allerlei mogelijkheden denkbaar waarbij gegevens van de fysieke omgeving direct gekoppeld worden aan een bepaald profiel op internet.

### **2.3 Eerst ervaren, dan oordelen**

Google tracht ook duidelijk te maken dat een daadwerkelijke ervaring met het product van belang is. Aan het begin van de brief wordt twee keer verwezen naar de demonstratie die Joe Barton heeft gekregen waarbij hij de bril daadwerkelijk heeft kunnen gebruiken. Zo stelt Molinari: “As you saw when you wore Glass, it requires specific user actions to do things like search the Internet, find directions, or take a photo or video”. Het belang van het daadwerkelijk ervaren van Glass wordt iets later in de inleidende tekst nogmaals benadrukt: “We believe first-hand experience with Glass will continue to help shape discussions in a positive directions for users and the public”. Het belang dat Google hecht aan het zelf ervaren van Glass wordt tevens duidelijk uit de video die ze op 8 november

2013 hebben toegevoegd aan het YouTube-kanaal (Google Glass 2013b). De video laat een verslag zien uit Durham, waar Google het publiek heeft uitgenodigd om Glass zelf te komen ervaren. De voice-over benadrukt dat dit event ‘iets zegt over de manier waarop ze dit doen’, doelend op de introductie van Glass. De video laat mensen van alle etniciteiten en leeftijden zien die Google voor het eerst gebruiken, waarbij vanzelfsprekend zeer positieve ervaringen in beeld gebracht worden. Het sluit af met een jongen die benadrukt dat je bij het zien van Glass denkt “yeah, it’s cool”, maar bij het daadwerkelijk uitproberen pas ontdekt hoe “mindblowing” het is.

Voor Google is het vanzelfsprekend van belang om de revolutionaire aspecten van Glass daadwerkelijk te laten ervaren door gebruikers om ze op deze manier te enthousiasmeren voor deze nieuwe technologie. Het product lijkt zich hiervoor ook uitstekend te lenen, omdat het een geheel nieuwe ervaring biedt ten opzichte van bijvoorbeeld de mobiele telefoon. Deze ervaring kan mensen enthousiast maken en toont de mogelijkheden en potentiële toepassingen van de nieuwe technologie. Je kunt echter stellen dat dit juist leidt tot een minder objectief beeld over de uiteindelijke maatschappelijke gevolgen, waaronder implicaties op het gebied van privacy. Deze benadering zorgt er voor dat de vernieuwende aspecten zoveel mogelijk worden benadrukt, terwijl de mogelijk negatieve gevolgen zoveel mogelijk naar de achtergrond verdwijnen.

#### **2.4 Technologie dichterbij en uit de weg**

In de video waarnaar wordt verwezen in de brief, houdt Timothy Jordan een presentatie voor (potentiële) ontwikkelaars voor Glass (Google Developers 2013). Jordan is Senior Developer Advocate bij Google en werkt mee aan Project Glass. Jordan benadrukt meerdere keren in de presentatie: “By bringing technology closer, we can get it out of the way”. Hiermee gaat hij in op een voor de hand liggende kritiek op Glass, namelijk dat we hierdoor nog minder betrokken zijn bij onze omgeving en constant worden afgeleid door technologie. Deze kritiek kwam overigens niet uit de lucht vallen, want toen Google in 2012 middels een YouTube video het concept van Glass liet zien, leek het er wel degelijk op dat het scherm en de notificaties direct voor je ogen verschenen (chalitapple 2012).<sup>6</sup> Aan de hand van deze video werden ook verschillende parodieën gemaakt, die een meer dystopische visie op dit concept liet zien (Tom Scott 2012). Het uiteindelijke ontwerp wijkt hier vanaf en Jordan stelt dan ook over Glass: “It’s not in the way. It is not in my line of

---

<sup>6</sup> De desbetreffende video staat inmiddels niet meer op het YouTube-kanaal van Google zelf.

sight, but it is in my field of view. It's not between me and my life. It's not that tablet at the concert, and that I'm looking at that instead of what I'm doing". Ook in de richtlijnen voor ontwikkelaars die Jordan gedurende de presentatie bespreekt komt dit beeld naar voren. De richtlijnen die genoemd worden zijn: 'design for Glass', 'don't get in the way', 'keep it timely' en 'avoid the unexpected'. Hierin ontbreekt echter iedere verwijzing naar de aanwezige camera. Ook in het overige deel van de presentatie wordt weinig aandacht gegeven aan de camera en wordt de nadruk gelegd op de andere aspecten die Glass interessant maken. Dit is opmerkelijk, aangezien het POV-perspectief van de camera uniek is ten opzichte van bestaande mobiele technologie, zelfs wanneer we kijken naar wearables zoals smartwatches. Je zou verwachten dat het juist daarom wordt opgenomen in de door Google opgestelde richtlijnen. Zoals in hoofdstuk 1 naar voren is gekomen heeft de camera immers gevolgen voor de privacy van de omgeving van iemand die Glass draagt. Desalniettemin wordt dit aspect ook verder in de presentatie nauwelijks besproken en lijkt het bedrijf hiermee eventuele discussies betreffende implicaties op het gebied van privacy zoveel mogelijk uit de weg te gaan.

## **2.5 Het komt eraan, of je het nu wilt of niet**

Zoals eerder naar voren is gekomen zegt Google met Glass de macht te willen verschuiven naar de gebruiker. Potentiële implicaties op het gebied van privacy van niet-gebruikers blijven echter onderbelicht en in de presentatie voor ontwikkelaars wordt de aanwezige camera nauwelijks belicht. Om een goed beeld te krijgen van de manier waarop Google communiceert over Glass is het relevant om te kijken op welke manier Google reageert op kritiek. De CEO van Google, Eric Schmidt, stelt hierover: "Our goal is to make the world better. We'll take the criticism along the way, but criticisms are inevitably from people who are afraid of change or who have not figured out that there will be an adaptation of society to it" (Sacacas 2013). Deze uitspraak is opmerkelijk. Schmidt stelt hiermee mensen die kritisch zijn over Glass gelijk aan mensen die bang zijn voor verandering of nog niet begrijpen dat de samenleving zich hierop zal aanpassen. Het geschetste doel van deze technologische ontwikkeling om de wereld te verbeteren krijgt duidelijk prioriteit boven eventuele implicaties voor de samenleving, die zich volgens Schmidt toch wel aanpast. Met betrekking tot de grote veranderingen van Glass en de implicaties op het gebied van privacy betoogt hij vervolgens:



Society adapts to these new things, and wearable computing is very much a real thing, of which Glass is just one example. We have to have rules about how you use them. And that may literally be just etiquette—what’s appropriate and what’s not. There’s obviously places where Google Glass is not appropriate. [...] We’re acutely aware of those questions, so we want to be very careful that this new invention is not misused. But I’m always concerned about premature regulation based on fear, as opposed to understanding what’s possible. The people who’ve used Glass, including myself, report it as remarkable. I’d like to let it get a little bit farther off a runway before we characterize it in the obvious ways (Woodward 2013).

Behalve dat Schmidt nogmaals herhaalt dat een samenleving zich vanzelf vormt naar dit soort nieuwe technologische ontwikkelingen, betreft hij hierbij nu ook de bredere context van Glass: wearable computing. Glass is inderdaad slechts één product binnen de eerder genoemde producten die zijn aangekondigd of reeds verkrijgbaar zijn, zoals smartwatches of lifelogging apparaten. Google impliceert echter een soort onvermijdelijkheid van deze nieuwe technologie. Eenzelfde visie op technologische ontwikkeling komt naar voren in een gesprek met Mary Lou Jepsen, hoofd van de Google X display group. Over Glass zegt ze: “It’s coming. I don’t think it’s stoppable [...] If we use the automobile analogy, we believe this would be the Model T. It’s lightweight, it’s comfortable, it’s cool” (Carr 2013). Volgens Jepsen is de verdere ontwikkeling van Glass en andere wearables dus niet tegen te houden. Of je het nu wilt of niet, het komt er toch aan. In Glass ziet ze een Model T, verwijzend naar één van de eerste Fords die in massaproductie werd genomen, waarna uiteraard vele volgden. Hiermee wordt een technologisch deterministisch beeld neergezet: de technologie heeft het verloop van de geschiedenis bepaald en vormt onze toekomst, zonder dat de mens hieraan iets kan doen. Marshall McLuhan betoogt echter dat dit niet zo hoeft te zijn. Hoewel hij vaak een technologisch determinist wordt genoemd, is dit niet helemaal terecht. Zo stelt hij: “There is absolutely no inevitability as long as there is a willingness to contemplate what is happening” (McLuhan & Fiore 1967: 25). Hiermee impliceert hij dat wanneer de technologische ontwikkeling begrepen wordt, er ook iets aan gedaan kan worden. Het draait volgens McLuhan dus om een bewustwording van dit proces. In het geval van Glass draait het er dan om dat gebruikers zich bewust zijn van de technologie, omdat zij zich anders niet meer beseffen wat het allemaal doet met hun omgeving en de wijze waarop zij daar naar kijken. De visie van Jepsen gaat echter niet uit van deze bewustwording, maar benadrukt slechts de onvermijdelijkheid, waarmee het

denken over de technologische ontwikkeling en de wenselijkheid ervan direct al irrelevant wordt.

Ondanks het feit dat er soortgelijke technologieën in ontwikkeling of al verkrijgbaar zijn, heeft de discussie zich vooral gevormd rondom Glass. In allerlei verschillende media wordt het eindeloos besproken. De manier waarop een machtig en discoursbepalend bedrijf als Google dit product presenteert is daarbij belangrijk, maar zeker ook de wijze waarop wordt omgegaan met kritiek. Schmidt lijkt echter eerst te willen afwachten op welke manier Glass zich precies ontwikkelt, alvorens men zich er zorgen over gaat maken. Zoals eerder gesteld zegt Google het als haar missie te zien om alle informatie ter wereld te organiseren en universeel toegankelijk en bruikbaar te maken. Wanneer dit heel letterlijk wordt opgevat zou dat betekenen dat privacy niet meer mogelijk is, aangezien alles voor iedereen inzichtelijk is. Schmidt bevestigt deze visie met betrekking tot online privacy als hij stelt: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (theyTOLDyou 2009). Hiermee gaat Schmidt eigenlijk nog een stap verder en verwerpt hij de volledige relevantie van privacy. Dit is opmerkelijk, aangezien het niet willen openbaren van bepaalde informatie niets te maken hoeft te hebben met de aard van deze informatie (zie ook sectie 3.2). Met dit argument lijkt Schmidt aan te nemen dat wanneer iemand iets verborgen wil houden, het vanzelfsprekend gaat om illegale informatie of activiteiten.

Wanneer we uitgaan van het beeld dat Google tracht neer te zetten rondom privacy, dan lijkt er inderdaad veel minder aan te merken op een samenleving waarin iedereen is uitgerust met een camera en in het openbaar opnames van elkaar kan maken en delen via sociale netwerken. Dergelijke argumenten verantwoorden de ontwikkeling van de door Foucault geschetste 'society of control', maar onderbelichten de ondoorzichtige wijze waarop we worden onderworpen aan corporate surveillance door Google zelf en in toenemende mate door sousveillance als gevolg van wearables. De technologisch deterministische houding van Google die uit de analyse naar voren komt past goed bij deze visie, aangezien binnen dat denkkader het verzetten tegen of bekritisieren van dergelijke technologieën zinloos is. Zoals bleek uit de analyse worden critici dan ook weggezet als mensen die gewoon bang zijn voor verandering. In dit hoofdstuk is verder duidelijk geworden dat Google haar gebruikers daadwerkelijk in een machtige positie plaatst. Dit gebeurt echter niet alleen op de wijze waarop zij dit zelf bedoelen, namelijk door de gebruiker de controle te geven over alle instellingen, maar tegelijkertijd ook ten koste van de omgeving die worden onderworpen aan een nieuw soort neo-panopticon. Dit

wordt onderstreept door de onlangs toegevoegde mogelijkheid om foto's te maken door te knipogen en zonder het scherm aan te zetten. Het is dan ook niet opmerkelijk dat Google de mogelijkheid voor gezichtsherkenning in de toekomst openlaat.

### 3. OVERAL OGEN: OPGELET OF OPGELUCHT?

De implicaties op het gebied van privacy en macht als gevolg van wearables als Glass die in het eerste hoofdstuk naar voren kwamen, worden duidelijk onderbelicht in de wijze waarop Google praat over Glass. In dit hoofdstuk staat de verdere interventie centraal op het beeld dat is gevormd dankzij de discoursanalyse in het vorige hoofdstuk. Het gaat dan met name om de technologisch deterministische houding van Google, alsmede om de wijze waarop Google het concept privacy toepast. Hiermee wordt een zeer beperkt denkkader neergezet en wordt verdere discussie uit de weg gegaan. Ook brengen wearables als Glass zeker implicaties voor de praktijk van sousveillance met zich mee, alleen is het nog maar de vraag in hoeverre deze gevolgen wenselijk zijn.

#### 3.1 Het Borg Complex

Google zet dus een beeld neer van Glass en andere vormen van wearable computing als een technologische ontwikkeling die niet te stoppen is en waaraan men zich dus beter gewoon kan aanpassen. Michael Sacasas, afgestudeerd in Teleologie en momenteel bezig met een PhD programma 'Texts and Technology', noemt dit het 'Borg Complex'. Hij stelt:

The implicit tone of those with a Borg Complex can be summed up by the line, "Resistance is futile." That line has entered our pop-cultural lexicon through the Star Trek franchise. I won't pretend to be an expert on Borg lore; I'll only note that the Borg always announced some variation of the following to their victims: "We will add your biological and technological distinctiveness to our own. Resistance is futile" (Sacasas 2012).

De manier waarop Google praat over critici als mensen die bang zijn voor verandering, past hier perfect bij. Sacasas stelt verder dat mensen die 'lijden' aan het Borg Complex zich beroepen op eerdere technologische ontwikkelingen, waarover in de beginfase altijd bepaalde zorgen ontstaan die achteraf vaak onnodig blijken (Sacasas 2013). Hierop wordt het argument gebaseerd dat de huidige zorgen in de toekomst ook wel onnodig zullen blijken. Deze manier van denken kwam ook sterk naar boven in de manier waarop Google praat over Glass. Er wordt echter aangenomen dat de zorgen als onterecht kunnen worden bestempeld wanneer uiteindelijk blijkt dat een bepaalde technologie gewoon wordt geaccepteerd binnen een samenleving. Dit hoeft echter niet het geval te zijn, zo benadrukt ook Sacasas: "Could it not also be the case that genuine and substantive moral

reservations were gradually eroded and then forgotten altogether. Eventual acceptance of a given state-of-affairs, after all, is no guarantee of its moral superiority” (Sacacas 2013). Wanneer iets geleidelijk in onze maatschappij terecht komt, is het aannemelijk dat we er uiteindelijk aan wennen. Dat wil alleen niet zeggen dat daarmee eerdere zorgen ongegrond kunnen worden verklaard. Google lijkt zich goed bewust van het belang om niet van de ene op de andere dag een revolutionaire technologie te introduceren. Zoals genoemd in hoofdstuk 2.2 is de manier waarop Glass wordt geïntroduceerd in dat opzicht goed gekozen. Via het ‘Glass Explorer Program’ selecteerde Google zelf 10.000 mensen die Glass voor een bedrag van 1.500 dollar mochten aanschaffen en uitproberen. Onlangs mochten deze mensen weer drie vrienden uitnodigen die ook Glass konden aanschaffen. Behalve de exclusiviteit die op deze manier tot stand wordt gebracht, geeft het andere mensen ook de kans om geleidelijk te wennen aan Glass. Tegelijkertijd biedt het Google natuurlijk de kans om te ontdekken op welke manier Google wordt ingepast in ons leven en wat er allemaal mogelijk is. Ook de nadruk die Google legt op het ervaren van het product alvorens kritiek te vormen, past goed in deze strategie. De geheel nieuwe gebruikerservaring en potentiële mogelijkheden voor bijvoorbeeld het onderwijs en de gezondheidszorg kunnen een deel van de kritiek doen afzwakken. Ook hier geldt echter dat dit niet hoeft te betekenen dat de eerdere kritiek daarom niet gegrond is.

### **3.2 Niks te verbergen?**

Behalve het door Sacacas omschreven ‘Borg Complex’ komt er ook een ander belangrijk gegeven naar boven uit de discoursanalyse. Dit omvat de manier waarop Google praat over privacy. Eric Schmidt vat deze visie samen wanneer hij stelt dat je dingen gewoon niet moet doen als je niet wilt dat deze in de openbaarheid verschijnen. Dit komt overeen met het veelgebruikte ‘nothing to hide’ argument, dat stelt dat wanneer je niks te verbergen hebt, je niet hoeft te vrezen voor bijvoorbeeld surveillance van autoriteiten. Dit impliceert echter dat privacy gaat over het verbergen van illegale of ‘slechte’ dingen, terwijl dit niet het geval hoeft te zijn. Zoals in hoofdstuk 1 al bleek uit de taxonomie van Solove betreffende privacy, omvat privacy een pluraliteit aan verschillende dingen. Solove stelt:

The deeper problem with the “nothing to hide” argument is that it myopically views privacy as a form of concealment or secrecy. But understanding privacy as a plurality of related problems demonstrates that concealment of bad things is just one among many problems caused by government programs such as the NSA surveillance and data mining. In terms of the categories in my taxonomy, several problems are implicated (Solove 2007: 16).

Solove doelt hiermee onder andere op 'chilling effects' (Solove 2007: 17). Dit houdt in dat bepaalde rechten, waaronder vrijheid van meningsuiting, bedreigd worden door potentiële gevolgen die het gebruik van deze rechten met zich mee kan brengen. Het kan er bijvoorbeeld toe leiden dat men bepaalde uitspraken toch niet doet wanneer er surveillance plaatsvindt, uit angst voor consequenties. Deze effecten zijn negatief voor een samenleving, omdat op deze manier de veelzijdigheid aan standpunten wordt aangetast en daarmee de mate van vrijheid om deel te nemen in de politiek (Solove 2007: 18). In het geval van Glass kunnen soortgelijke 'chilling effects' optreden. De recente onthullingen van Edward Snowden hebben nog sterker bevestigd dat vrijwel alle data van Google ook door autoriteiten opgevraagd kunnen worden. Dit bleek zelfs veelvuldig gebeurd te zijn zonder dat hier toestemming van Google voor was, die naar eigen zeggen alleen gegevens verstrekt over gebruikers in bepaalde gevallen (Gellman & Soltani 2013). Daarnaast is het mogelijk om via iemands webcam mee te kijken zonder dat dit merkbaar is en de FBI blijkt deze techniek al vele jaren toe te passen (Timberg & Nakashima 2013). Inlichtingendiensten doen dit naar alle waarschijnlijkheid alleen bij verdenking van ernstige misdrijven, maar onlangs bleek een achttienjarige hacker hetzelfde te doen (Huiskamp 2013). Hij maakte onder andere naaktbeelden van tienermeisjes en postte van één meisje zelfs een naaktfoto online via haar eigen Facebookpagina. Wearables als Glass zorgen ervoor dat deze mogelijkheden worden uitgebreid: inlichtingendiensten en hackers zouden nu zelfs mee kunnen kijken door de ogen van een Glass-gebruiker. Zelf wil Google ook graag meekijken: onlangs werd een patent goedgekeurd dat een technologie omschrijft waarbij oogbewegingen van een gebruiker worden gevolgd door een 'eye-tracking device' terwijl advertenties in de fysieke wereld bekeken worden (Jeffries 2013). Hiermee wordt de effectiviteit van bepaalde advertenties op specifieke gebruikers zichtbaar voor Google. Glass heeft al een ingebouwde tweede camera die oogbewegingen registreert van de gebruiker en is dus geschikt om deze techniek in de toekomst toe te passen.

### **3.3 Glass & sousveillance**

Je kunt betogen dat gebruikers van Glass er zelf voor kiezen om zich op deze manier te laten volgen door Google en potentieel door bijvoorbeeld inlichtingendiensten en hackers. De omgeving van iemand die Glass draagt kiest echter niet zelf om gevolgd te worden. Toch kan ook het gedrag van deze omgeving worden beïnvloed, aangezien de kans bestaat dat zij gefilmd worden. De eerder besproken wearables zoals de Narrative en Autographer kunnen eenzelfde soort effect tot gevolg hebben. Toch richten deze technologieën zich alleen op het autonoom maken van opnames en lijkt het niet

aannemelijk dat dergelijke technologieën eenzelfde soort functie in ons leven krijgen als de mobiele telefoon nu bijvoorbeeld heeft. Glass kan daarentegen gezien worden als een verlengde van de mobiele telefoon die op dezelfde momenten gebruikt kan worden. Zoals Google zelf stelt zorgt Glass voor een verkleining van de tijd tussen intentie en actie, waardoor het makkelijker en sneller te gebruiken is dan de mobiele telefoon. Dit maakt het uiteraard tot een erg geschikte technologie voor sousveillance, alsmede het feit dat de opgenomen beelden direct (en zelfs live) gedeeld kunnen worden.

Uit de analyse is gebleken dat Google nauwelijks praat over de implicaties die Glass kan hebben voor de praktijk van sousveillance. Deze potentie wordt wel uitgebreid besproken door Mann, die in technologieën als Glass mogelijkheden ziet om 'terug te kijken' naar autoriteiten of corporaties. Het lijkt er alleen niet op dat sousveillance ons bevrijdt uit de door Mann omschreven neo-panopticons. Het geeft ons de mogelijkheid om terug te kijken, maar verandert daarmee niets aan de architectuur van de bestaande neo-panopticons. De samenleving mag dan misschien een stuk transparanter worden, maar de surveillance door autoriteiten en corporate surveillance wordt daarmee niet transparanter. En zoals Google zelf ook al impliceert wanneer ze aangeven dat ze 'de gebruiker macht willen geven' met Glass, zorgt dit met name dat gebruikers meer macht verkrijgen ten opzichte van niet-gebruikers. Voor niet-gebruikers ontstaat eigenlijk een nieuw soort neo-panopticon, aangezien de kans bestaat dat zij gefilmd worden door wearables als Glass. Gebruikers bepalen wanneer er gefotografeerd of gefilmd wordt, zonder dat niet-gebruikers hierop directe invloed hebben. De ontwikkeling van wearables uitgerust met camera's lijkt juist bij te dragen aan een verdere ontwikkeling van de 'society of control', waarbij iedereen elkaar in de gaten houdt. Het eerder genoemde voorbeeld van de "Project X" rellen in Haren geven al aan op welke manier mobiele telefoons een toenemende mate van sousveillance faciliteren. Wearables zorgen dat er steeds vaker en gemakkelijker ongezien gefilmd en gefotografeerd kan worden in de openbare ruimte.

## CONCLUSIE

Google praat over Glass alsof we er nu al niet meer omheen kunnen. Ondanks dat het product nog slechts verkrijgbaar is via het 'Glass Explorer Program', stelt het bedrijf dat de komst van wearables onvermijdelijk is. Michael Sacasas noemt deze technologisch deterministische houding het 'Borg Complex'. Tegelijkertijd zien wetenschappers als Steve Mann de opkomst van dergelijke wearables als ideaal middel voor sousveillance om zo onze surveillance-maatschappij te doorbreken. Zowel het discours dat Google neerzet als het utopische beeld van Mann behoeven nuance. Hoewel het inderdaad aannemelijk is dat wearables zich verder zullen ontwikkelen, is het belangrijk dat er vooraf goed wordt nagedacht over eventuele implicaties van 'revolutionaire' technologieën. Dat is precies wat Google uit de weg gaat door te stellen dat het er toch wel komt, ongeacht menselijk handelen. Critici worden daarbij weggezet als mensen die bang zijn voor verandering. Veel kritiek op Glass heeft betrekking op privacy en de eenzijdige benadering van dit begrip die volgt uit de discoursanalyse lijkt dan ook een zorgvuldig gekozen strategie om een beperkt denkkader tot stand te brengen. Dit komt met name naar voren in de visie van Eric Schmidt, die het 'nothing to hide' argument toepast en stelt dat je dingen gewoon niet moet doen wanneer je deze met niemand wilt delen. Mede hieruit blijkt de verkeerde interpretatie van privacy: er wordt geïmpliceerd dat dit gelijk staat aan het verbergen van slechte of illegale dingen. Vanuit bedrijfs perspectief is het logisch dat Google ons op deze manier tracht te laten denken over privacy. Dit geeft ze immers de mogelijkheid om zoveel mogelijk gebruikersgegevens te verzamelen, die vervolgens kunnen worden ingezet om de effectiviteit van advertenties zoveel mogelijk te optimaliseren.

Het hoofddoel dat Google met Glass wil bereiken is naar eigen zeggen het verschuiven van macht naar de gebruiker. Hoewel Google hiermee waarschijnlijk doelt op de volledige controle die de gebruiker heeft met Glass over alle instellingen, lijkt het er ook op dat de gebruiker van Glass meer macht zal verkrijgen ten opzichte van mensen in de omgeving die een dergelijke technologie niet dragen. Dit komt met name door de aanwezige camera, waardoor het gedrag van anderen in de omgeving beïnvloed kan worden. Het utopische beeld dat Steve Mann schetst met betrekking tot de mogelijkheden van wearables voor de praktijk van sousveillance, behoeft dan ook enige nuance. Het heeft namelijk zeker gevolgen voor privacy en het lijkt niet echt aannemelijk dat we hierdoor bevrijd worden uit de neo-panopticons die Mann beschrijft. De potentie van wearables om terug te kijken verandert immers niks aan de ongelijkheid die voortkomt uit de architectuur van het panopticon. Het geeft ons wellicht de macht om misstanden van



autoriteiten of corporaties vast te leggen, maar geeft ons geen inzicht in de wijze waarop informatie over ons wordt verzameld en geanalyseerd. Voor de omgeving van iemand met Glass ontstaat hiermee een nieuw soort neo-panopticon, aangezien op ieder moment beelden kunnen worden opgenomen.

Gesteld kan worden dat de manier waarop Google praat over nieuwe technologie en de gevolgen voor macht en privacy erg is toegespitst op commerciële belangen. Bij de introductie van een grensverleggende technologie kan een bewustwording van de gevolgen voor onze samenleving in relatie tot concepten als privacy en macht erg belangrijk zijn. Een machtig en discoursbepalend bedrijf als Google zou juist de verantwoordelijkheid op zich moeten nemen om deze discussie zoveel mogelijk te faciliteren. Daartoe zou het goed als Google afstapt van de technologisch deterministische visie die op dit moment uit de communicatie naar voren komt. Het bedrijf dient zich te beseffen dat dergelijke technologieën verregaande gevolgen kunnen hebben voor een samenleving. Implicaties op het gebied van privacy en macht zouden dan ook veel centraler moeten staan bij het ontwikkelen en introduceren van nieuwe en grensverleggende technologieën zoals Glass.

Toch zal er vervolgonderzoek nodig zijn voor een beter beeld betreffende de visie van Google op de rol van technologie in ons leven, aangezien dit onderzoek zich specifiek richt op één product en slechts bekijkt welke communicatie er naar buiten wordt gebracht, zonder over interne informatie te beschikken. Ten behoeve van de focus van dit onderzoek is gekeken naar een selectie van de communicatie rondom de introductie van Glass, waarbij is gekozen voor de communicatie vanuit Google zelf. Dit heeft specifiek inzichtelijk gemaakt op welke manier Google communiceert over Glass en hoe daarbij implicaties voor privacy en macht onderbelicht blijven. Zoals eerder benadrukt legt de gekozen methode echter niet bloot welke gevolgen het door Google neergezette denkkader heeft voor de wijze waarop bijvoorbeeld grote technologie-blogs schrijven over Glass, terwijl dergelijke bronnen net zo bepalend kunnen zijn. Ook zal uiteraard nog moeten blijken in welke vorm Glass uiteindelijk voor consumenten beschikbaar komt en of hierbij wellicht rekening gehouden wordt met problemen zoals die in dit onderzoek belicht zijn. Tot slot heb ik ondanks aandringen bij Google Nederland niet de kans gekregen om Glass zelf te ervaren. Hoewel de focus van dit onderzoek dit ook niet vereist, kan dit wel nieuwe inzichten bieden bij vervolgonderzoek naar de werkelijke gevolgen van Glass voor onze samenleving.

## BIBLIOGRAFIE

Adhikari, Richard. 2013. Google Glass Just Got Creepier. *TechNewsWorld*. <http://www.technewsworld.com/story/79659.html>.

Bentham, Jeremy. 1791. *Panopticon; or the Inspection House*. London: T. Payne.

Carr, Nicolas. 2013. The future's so bright I gotta wear Glass. *Rough Type*. <http://www.roughtype.com/?p=3850>.

Campbell, John Edward, en Carlson, Matt. 2002. Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media* 46 (4): 586-606.

chalitapple, 2012. *Project Glass One day Google: Yep, we're testing augmented-reality glasses* [Video bestand]. <http://youtu.be/Vb2uojqKvFM>.

Cohen, Julie E. 2008. Privacy, Visibility, Transparency, and Exposure. *University of Chicago Law Review* 75(1): 181-201.

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

eturner303. 2013. *Google Glass + Computer Vision - AlchemyAPI Demo* [Video bestand]. [http://youtu.be/6tsLMFF9\\_yU](http://youtu.be/6tsLMFF9_yU).

Facebook. 2013. *About*. <https://www.facebook.com/facebook?v=info>.

Foucault, Michel. 1972. *The Archeology of Knowledge and the Discourse on Language*. Vertaald door A.M. Sheridan Smith. New York: Pantheon Books.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. Vertaald door A.M. Sheridan. New York: Vintage.

Foucault, Michel. 1978. *The History of Sexuality. Volume 1: An introduction*. Vertaald door Robert Hurley. New York: Vintage.

Gellman, Barton, en Soltani, Ashkan. 2013. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. [http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd\\_story.html](http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html).

Ganascia, Jean-Gabriel. 2010. The generalized sousveillance society. *Social Science Information* 2010 (49): 489-507.

Grol, Stijn van. 2012. *De autonome auto van Google. Google's visie op technologie: utopie of dystopie?* [http://www.newmediastudies.nl/sites/default/files/737-istijn1/papers/filosofie\\_paper\\_stijnvangrol.pdf](http://www.newmediastudies.nl/sites/default/files/737-istijn1/papers/filosofie_paper_stijnvangrol.pdf).

Given, Lisa M. 2008. *The SAGE Encyclopedia of Qualitative Research Methods*, Volume 2. Thousand Oaks: SAGE Publications.

Google. 2012. *Google Privacy Policy Update* [Video bestand]. <http://youtu.be/KGghIPmebCY>.

Google. 2013. *Over Google*. [http://www.google.com/intl/nl\\_nl/about/](http://www.google.com/intl/nl_nl/about/).

Google Developers. 2013. Building New Experiences with Glass [Video bestand]. <http://youtu.be/JpWmGX55a40>.

Google Glass 2013a. *How it Feels [through Google Glass]* [Video bestand]. <http://youtu.be/v1uyQZNg2vE>.

Google Glass. 2013b. *Cities Through Google Glass: Durham, NC* [Video bestand]. <http://youtu.be/G4TJh1wR6hQ>.

Greenberg, Andy. 2013. Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not. *Forbes*. <http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/>.

Huiskamp, Frank. 2013. Rotterdamse hacker opgepakt - vermoedelijke dader lek examen Frans. *NRC Handelsblad*. <http://www.nrc.nl/nieuws/2013/12/13/rotterdamse-hacker-opgepakt-vermoedelijke-dader-lek-examen-frans/>.

Hook, Derek. 2001. Discourse, knowledge, materiality, history; Foucault and discourse analysis. *Theory and psychology* 11 (4): 521-547.

Jeffries, Adrienne. 2013. Google patents 'pay-per-gaze' eye-tracking that could measure emotional response to real-world ads. *The Verge*. <http://www.theverge.com/2013/8/18/4633558/google-patents-pay-per-gaze-eye-tracking-ads>.

Lessa, Iara. 2006. Discursive Struggles Within Social Welfare: Restaging Teen Motherhood. *British Journal of Social Work* 36: 282-298.

Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Mann, Steve, Nolan, Jason, en Wellman, Barry. 2003. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1 (3): 331-355.

McLuhan, Marshall, en Fiore, Quentin. 1967. *The Medium is the Massage: An Inventory of Effects*. New York: Random House.

Mann, Steve, en Ferenbok, Joseph. 2013. New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World. *Surveillance & Society* 11 (1/2): 18-34.

Metz, Rachel. 2013. Wearable Computing Pioneer Says Google Glass Offers “Killer Existence”. *MIT Technology Review*. <http://www.technologyreview.com/qa/515681/wearable-computing-pioneer-says-google-glass-offers-killer-existence/>.

Michael, M.G. en Michael, Katina. 2009. Überveillance: Definition. In *Macquarie Dictionary: Fifth Edition* (Australia's National Dictionary, Sydney University), edited by Susan Butler, 1094.

Michael, M.G., en Michael, Katina. 2010. Toward a State of Überveillance. *IEEE Technology and Society Magazine* 29 (2): 9-16.

Rachels, James. 1975. Why Privacy is Important. *Philosophy & Public Affairs* 4 (4): 323-333.

Reiman, Jeffrey H. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs* 6 (1): 26-44.

Sacasas, Michael. 2012. *The Borg Complex*. <http://thefrailestthing.com/2012/06/18/the-borg-complex/>.

Sacasas, Michael. 2013. *Don't Worry, You'll Get Used To It*. <http://thefrailestthing.com/2013/03/13/dont-worry-youll-get-used-to-it/>.

Said, Edward W. 1983. *The World, the Text, and the Critic*. Cambridge: Harvard University Press.

Schäfer, Mirko T. 2011. *Bastard Culture! How User Participation Transforms Cultural Production*. Amsterdam University Press: Amsterdam.

Solove, Daniel J. 2004. *The Digital Person*. New York: NYU Press.

Solove, Daniel J. 2007. I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review* 44: 745-772.

Solove, Daniel J. 2008. *Understanding privacy*. Cambridge: Harvard University Press.

theyTOLDyou. 2009. *Google CEO Eric Schmidt on privacy* [Video bestand]. <http://youtu.be/A6e7wfDHzew>.

Timberg, Craig, en Nakashima, Ellen. 2013. FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance. *The Washington Post*. [http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98\\_story.html](http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html).

Tom Scott. 2012. *Google Glasses: A New Way to Hurt Yourself (parody of Google's Project Glass)* [Video bestand]. <http://youtu.be/t3TAOYXT840>.

Vrankulj, Adam. 2013. Xbox One to feature biometric targeted advertisements. *Biometric Update*. <http://www.biometricupdate.com/201307/xbox-one-to-feature-biometric-targeted-advertisements>.

Williamson, Tom. 2008. *The Handbook of Knowledge Based Policing. Current Conceptions and Future Directions*. Chichester: Wiley.

Woodward, Curt. 2013. Schmidt: Google Glass Critics "Afraid of Change," Society Will Adapt. *Xconomy*. <http://www.xconomy.com/boston/2013/04/26/schmidt-google-glass-critics-afraid-of-change-society-will-adapt/>.

**BIJLAGE: BRIEF GOOGLE OVER PRIVACY GLASS, 7 JUNI 2013**



June 7, 2013

The Honorable Joe Barton  
2107 Rayburn House Office Building  
Washington, DC 20515

Dear Congressman Barton:

Thank you for your recent letter regarding Google Glass and for the opportunity to provide an in-person demonstration of the product and its functionality. Protecting the security and privacy of our users is one of our top priorities. We recognize that new technology is going to bring up new types of questions, so we have been thinking carefully about how we design Glass from its inception.

Our goal with Glass is to give users control, and we have gotten very positive reactions from those with first-hand experience of the product. As you saw when you wore Glass, it requires specific user actions to do things like search the Internet, find directions, or take a photo or video. Users say “OK, Glass” and then state commands like “Google” to search the Internet or “Get directions to” in order to chart a path to their destination. For photos and video, users press a button on the arm of Glass or say “Take a photo” or “Record a video.” These, and other built-in signals, in turn help other people understand what Glass users are doing. This video provides a good introduction to some of the basic functionality of Glass:

<https://www.youtube.com/watch?v=4EvNxWhskf8>.

Although Glass is not yet in full consumer release and it is still early days for the product, we believe first-hand experience with Glass will continue to help shape discussions in a positive direction for users and the public. That is why we launched the Google Glass Explorer program, which includes a diverse group of individuals participating in early field trials of the product. We are thinking carefully about all this feedback as we consider next steps.

Below you will find the answers to your questions. Please note that we are still actively working on Glass, so the information provided here may change prior to our full consumer release of the product.

Sincerely,

A handwritten signature in blue ink that reads "See Molinari".

Susan Molinari  
*Vice President, Public Policy and Government Relations*  
Google Inc.



**1. In 2010, it was discovered that Google was collecting information across the globe from unencrypted wireless networks. This practice caused multiple investigations into the company along with consumers left perplexed. Google just recently agreed to pay \$7 million to settle charges with 38 states for the collection of data from unprotected Wi-Fi networks without permission. Google also admitted that they did not adequately protect the privacy of consumers and “tightened up” their systems to address the issue. While we are thankful that Google acknowledged that there was an issue and took responsible measures to address it, we would like to know how Google plans to prevent Google Glass from unintentionally collecting data about the user/non-user without consent?**

Protecting the privacy and security of our users is one of our top priorities. Because Question 2 expounds on this question, please find our detailed response below.

**2. What proactive steps is Google taking to protect the privacy of non-users when Google Glass is in use? Are product lifecycle guidelines and frameworks, such as Privacy By Design, being implemented in connection with its product design and commercialization? For example, if a Google Glass customer/user decides to resell or to dispose of their Google Glass product, would there be any product capabilities incorporated into the device to ensure that one’s personal information remains private and secure?**

In response to Questions 1 and 2:

Protecting our users is one of our top priorities. We aim to provide the world’s strongest security and privacy policies, as well as easy-to-use tools. As we do for all our products, we are carefully reviewing the design of Glass for privacy considerations as part of Google’s comprehensive privacy program. This includes designing Glass with privacy in mind and ensuring Google has obtained appropriate consent from Glass users.

We have built Glass to put users in control. Users will have access to their own “MyGlass” site ([www.google.com/myglass](http://www.google.com/myglass)) and MyGlass mobile application, which will give them a place to monitor the status of their Glass, manage settings, and decide which items or applications will appear on Glass.

We have also built some social signals into the way Glass is used. These signals help people understand what users are doing, and give Glass users means for employing etiquette in any given situation. One important feature is that Glass requires user commands to take a photo or record video — actions that also cause the Glass screen to activate, which is visible to others. As you point out in your letter, some parties have already taken measures to address the use of existing technology — such as cell phones, laptops or cameras — in certain circumstances. We expect these types of rules to continue to evolve as more wearable technologies come to market.

Our commitment to putting users in control extends to the policies we’ve created for developers making applications for Glass, also called Glassware. For example, Google has said for several years that we won’t add facial recognition features to our products without having strong privacy protections in place. With that

in mind, we won't be approving any facial recognition Glassware at this time. We also prohibit developers from disabling or turning off the display when using the camera. The display must become active when taking a picture and stay active during a video recording as part of your application.

While we ask participants in our Explorer program not to sell or transfer their Glass, users who someday transfer Glass to others will have options for removing their content from the device. Glass displays items like photos, videos, and text messages in a timeline, along with a "delete" option to remove them from that timeline. The "delete" function is one way to remove content from Glass. Also, the MyGlass site and app mentioned above will give users the ability to disable specific items (including Gmail, Google+, and Now) from Glass and to perform a factory reset, which will wipe all of their data from the device. Users who lose their Glass can likewise make use of these MyGlass site and app features.

**3. When using Google Glass, is it true that this product would be able to use Facial Recognition Technology to unveil personal information about whomever and even some inanimate objects that the user is viewing? Would a user be able to request such information? Can a non-user or human subject opt out of this collection of personal data? If so, how? If not, why not?**

Google does not provide any facial recognition capabilities in Glass, and we will not be approving any facial recognition Glassware at this time. We've consistently said that Google won't add face recognition features to our own services unless we have appropriate privacy protections in place.

**4. In Google's privacy policy, it states that the company "may reject requests that are unreasonably repetitive, require disproportionate technical effort ... risk the privacy of others, or would be extremely impractical." Please provide examples of when Google would reject requests on Google Glass that would risk the privacy of others? Would Google place limits on the technology and what type of information it can reveal about another person? If so, please explain. If not, why not?**

The portion of the Google Privacy Policy you quote relates specifically to requests from our users for "access to [their] personal information" that Google stores. This common privacy policy term, and the similarly common limitation against "unreasonably repetitive" requests, is to ensure that requests to access personal information stored by Google are legitimate and handled appropriately. As discussed above, Google gives Glass users full control over when to use the product.

**5. Given Google Glass's sensory and processing capabilities, has Google considered making any additions or refinements to its privacy policy? If so, please explain. If not, why not?**

Use of Google Glass will be governed by the terms of the Google Privacy Policy and no changes to the Google Privacy Policy are planned for Glass.

**6. In Google's privacy policy, it states that the company "may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number)."**

- a. Would this information be collected from users operating Google Glass? If so, what specific information is Google intending to collect?**
- b. Would Google Glass collect any data about the user without the user's knowledge and consent? If so, why? If not, please explain.**

Google's Privacy Policy and pertinent disclosures during Glass setup provide users with information about what data will be collected from Glass. In addition, the MyGlass site and app provide users with access to details about Google and third party applications and services that are synced with Glass. When adding applications, users are shown the device-level permissions such applications obtain when used with Glass.

**7. It was recently revealed that the *New York Times* was the first to release an app for Google Glass. To what extent was privacy considered in approving this app? Is Google planning to make privacy a priority for future app developers? If not, why not? If so, please explain.**

We are excited about the opportunity to work with developers who can create compelling and exciting applications for Glass. As we mentioned above, protecting user security and privacy is a top priority for Google and we encourage all developers to take user privacy seriously. All Glass developers have to agree to terms of service for using necessary application programming interfaces ("APIs"), as well as general Glass developer policies, which include having and following their own privacy policies.

The Glass team has been working directly with developers and engaging with them as ideas unfold for possible applications for Glass. For example, we recently held an event on this topic at our annual developers conference, Google I/O. A video of the presentation is available at [developers.google.com/events/io/sessions/332490621](https://developers.google.com/events/io/sessions/332490621).

**8.b. Will Google Glass have the capacity to store any data on the device itself? If so, will Google Glass implement some sort of user authentication system to safeguard stored data? If not, why not? If so, please explain.**

Glass does have flash memory capable of storing data. This includes storage of information that assists with the operation of the device, such as software libraries and application information. The flash memory can also be used to store user content, such as photos and video, to ensure those moments are saved even when Glass does not have an Internet connection. We are experimenting with "lock" solutions to determine what would work best for this type of device. In the event a device is misplaced or somehow compromised, users can use their Google account to login to MyGlass and initiate a remote wipe of all data stored on Glass, as described above.