

PRIVACY IS VERDACHT

Hanneke Wetzer

~~—PRIVACY IS VERDACHT—~~

PRIVACY IS VERDACHT

Hanneke Wetzor

– Faculteit Illustratieve Vormgeving –

– Hogeschool voor de Kunsten Utrecht –

– April 2010 –

-VRAAGSTELLING	8
-INLEIDING	9
-H 1 BIOMETRIE ALS ZEGEN EN ALS VLOEK	10
-H 2 NIEUWE MEDIA EN CONTROLESYSTEMEN IN DE KUNST	16
-H 3 EEN INZOOM OP DE URGENTIE	35
-H 4 AFSTUDEERPROJECT	42
-NAWOORD	51
-BIJLAGE	56
-LITERATUUR	59

Hoe kunnen kunstenaars vorm geven aan de angstgevoelens die de nieuwe ontwikkelingen oproepen op het gebied van biometrische technologieën om terrorisme te bestrijden?

Het is mij opgevallen dat er tegenwoordig vele tentoonstellingen en festivals worden georganiseerd waarbij een groot aantal kunstenaars betrokken is dat zich bezighoudt met nieuwe media als kunstvorm in combinatie met biometrie als thema (zie bijlage). Meest recent is het festival GLOW in Eindhoven van afgelopen november. Verder heeft MAMA - Showroom for Media and Moving Art Rotterdam - zojuist een expositie afgerond met de welluidende titel 'For Security Reasons' en organiseerde het Rathenau Instituut het festival 'Het Glazen Lichaam' in het kader van de informatie-maatschappij. Bij verder onderzoek naar kunstenaars die zich met het thema biometrie bezighouden werd ik door V2 -Instituut voor Onstabiele Media, een interdisciplinair centrum voor kunst en mediatechnologie in Rotterdam- verwezen naar de website www.we-make-money-not-art.com, die een apart hoofdstuk bevat voor kunstenaars die zich over de gehele wereld bezighouden met nieuwe media en biometrie. V2 zelf biedt ook vele kunstenaars in zijn archief die zich met dit thema hebben beziggehouden. In deze scriptie verhelder ik allereerst het begrip 'biometrie' en geef ik aan wat de voor- en nadelen hiervan zijn. Vervolgens ga ik dieper in op een selectie van kunstwerken van kunstenaars die bezig zijn met volg- en/of controlesystemen en veelal werken met nieuwe media technologie. Kennelijk maken deze kunstenaars zich druk om biometrie als door de overheid ingezette techniek in het kader van de terrorismebestrijding. Zij pogen een bewustmakingsproces op gang te brengen bij de beschouwer. Een bewustmakingsproces waarvan? Wat is er zo urgent? En hoe komt mijn eigen gevoel van urgentie tot uiting in mijn afstudeerproject?

Hoofdstuk 1 Biometrie als zegen en als vloek

Allereerst is het belangrijk de term 'biometrie' te verhelderen, zodat er begrip ontstaat van wat biometrie precies inhoudt, welke toepassingen er bestaan, en wat de voor- en nadelen zijn.

— Wat is biometrie? —

“Biometrie is het gebruik van lichaamskenmerken of gedragseigenschappen om de identiteit van iemand te verifiëren of vast te stellen”.¹ Het is een techniek waarbij persoonsidentificatie plaats vindt op basis van de unieke menselijke karakteristieken, zoals een vingerafdruk, een deel van de iris of bepaald gedrag. Door dit kenmerk elektronisch op te slaan, is er vergelijking mogelijk met een versie die op een ander tijdstip is verkregen.

Bij ieder biometrisch systeem zijn authenticatie, identificatie, verificatie en autorisatie aan de orde. Authenticatie is het vaststellen van iemands identiteit. Identificatie is het bepalen wie iemand is door een verzameling persoonsgegevens te controleren. Bij verificatie wordt gecontroleerd of de persoon inderdaad degene is die recht van toegang heeft tot een bepaalde voorziening. Autorisatie is het iemand verlenen van de betreffende bevoegdheid.²

Er bestaan tegenwoordig heel wat biometrische technologieën. Sommige hiervan kijken naar onbewust gedrag, maar het overgrote deel van deze technologieën baseren zich op specifieke lichaams-eigenschappen. Bij hand- of vingergeometrie wordt de geometrie van de hand of de vingers gebruikt voor authenticatie, maar dit is niet echt een betrouwbare optie. De vingerafdruk wordt het meest gebruikt omdat het al meer dan een eeuw bekend is door het ge-

¹ Biometrieforum. “Definitie biometrie”, bezocht op 5 oktober 2009 (internet, <http://www.biometrieforum.nl/Definitie-biometrie>)

² COSMO Time & Security Systems. Wat is biometrie? Biometrie: whitepaper, p. 5-6.

bruik bij het oplossen van misdrijven door politie en justitie en het een uniek kenmerk betreft. Nadeel is dat een klein gedeelte van de bevolking geen duidelijke vingerafdruk bezit door bijvoorbeeld slijtage, waardoor de meting minder betrouwbaar wordt. Ook wordt de associatie met verdachten vaak als negatief ervaren. Irisherkenning is daarentegen wel erg betrouwbaar, omdat zelfs bij eenige tweelingen elke iris uniek is. Nadelig is dat mensen een ogenscan vaak te verontrustend ervaren. Nog betrouwbaarder is retina- of netvliesherkenning, omdat het bloedvatenpatroon achterin het oog bij iedereen uniek is en aardig stabiel blijft gedurende het gehele leven, maar echt gebruiksvriendelijk is deze procedure niet. Gezichtsherkenning heeft als voordeel dat het heimelijk ingezet kan worden. Wordt het duidelijk ingezet, dan ervaren mensen dit als minder bedreigend, omdat het kijken in de camera voor de meesten een natuurlijke handeling is. Biometrische systemen die nog worden uitgetest zijn systemen waarbij er wordt gekeken naar bloedvaten in de hand, het oor, DNA, de geur of een gezichtsthermogram.³

Er zijn vandaag de dag een aantal surveillance technologieën in opmars ter ondersteuning van biometrie, waardoor de toepassing breder getrokken kan worden. Dit zijn het cameratoezicht, slimme camera's en de RFID-chip. Door middel van cameratoezicht kunnen mensen worden gevolgd en plaatsen nauwgezet in de gaten worden gehouden. Onderzoeksbureau TILT verwacht voor de toekomst dat naast gebruik van cameratoezicht in de openbare ruimte ook het gebruik daarvan binnenshuis zal toenemen: “ouders die hun kinderen op het kinderdagverblijf kunnen waarnemen, maar ook kinderen die hun ouders kunnen bewaken in het verzorgingstehuis.”⁴ Het Rathenau Instituut geeft aan dat slimme camera's in opmars zijn. Slimmecamera's zijn beveiligingscamera's die zijn uitgerust met software en sensoren, en gekoppeld aan databases zodat ze zelfstandig afwijkingen kunnen herkennen in van tevoren vastgestelde patronen.

Jan

“Constaert een camera een afwijking, dan begint ze automatisch met opnemen of geeft ze een alarmsignaal af aan de controlekamer, ten teken dat de bewaker naar zijn monitor moet kijken”.⁵ TILT geeft aan dat het gebruik van Radio Frequency Identification (RFID) een snelle opmars maakt, “doordat diverse grote afnemers van consumentenproducten het plaatsen van ‘tags’ op die producten ontwikkelen. Waar aanvankelijk RFID vooral wordt ingezet voor massagoederen (het volgen van containers bijvoorbeeld), zullen in de nabije toekomst individuele producten worden uitgerust met een RFID-chip. Deze ‘tags’ kunnen op afstand uitgelezen worden door speciaal daarvoor ontwikkelde apparaten.”⁶

— De voor- en nadelen van biometrie —

Jaap Spaans noemt in zijn boek ‘Biometrische Identificatie’ een aantal belangrijke voor- en nadelen van de toepassing van biometrie. Enkele voor mijn scriptie relevante voor- en nadelen wil ik hier graag noemen:

“Door een sluitend systeem van verificatie en identificatie kunnen fraude en andere vormen van criminaliteit worden voorkomen. Voor opsporingsinstanties en justitiële diensten van groot belang, omdeuit de hand lopende criminaliteit nog enigszins beheersbaar te houden.

Vreemdelingenstromen kunnen beter worden beheerst en gecontroleerd. Er kan bijvoorbeeld een doelmatige registratie van asielzoekers plaatsvinden.

Vergelijking met DNA-profielen is een uitstekend middel om zware criminelen op te sporen. Vaak gaat het om criminelen als zeden delinquenten die in herhaling kunnen vervallen. In bepaalde

⁴ TILT - Centrum voor Recht, Technologie en Samenleving, Techniek, Veiligheid en privacy in 2030: twee toekomstscenario's. Universiteit van Tilburg, 2005, p. 18-19.

⁵ Vedder, Anton, Leo van der Wees, Bert Jaap Koops en Paul de Hert, Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw. Den Haag: Rathenau Instituut, 2007; Studie, p. 42.

⁶ TILT, op. cit. (noot 4).

situaties kan inzet van dit instrument leiden tot preventief optreden en voorkoming van misdrijven.

Gelaatsherkenningssystemen kunnen worden ingezet om verdachten te traceren in een menigte en eventueel tot aanhouding over te gaan (...).

Persoonsverwisselingen kunnen worden voorkomen. Belangrijk om medische missers en slordigheden te voorkomen in ziekenhuizen en andere zorginstellingen, en om de zogenaamde ‘lookalike’ fraude van paspoorten tegen te gaan.”⁷

Er kleven echter ook vele nadelen aan biometrie. “Bij grootschalige toepassing kan ook biometrie fraudegevoelig zijn.”⁸ Biometrische kenmerken kunnen worden ontvreemd en nagemaakt. Denk aan een nagemaakte vingerafdruk van een dun laagje rubber, dat over de eigen vinger wordt gelegd, een dummyhand, of een foto van een gezicht. Als er geen goede beveiliging is kan de scanner of de database worden misleid, of templates verwisseld worden.⁹ “De praktijk heeft uitgewezen dat criminelen vaak over ruime financiële middelen beschikken en niet schromen om deskundigheid in te kopen om de fraudegevoeligheid van beveiligingssystemen te onderzoeken en deze vervolgens te gebruiken.

Het systeem is betrouwbaar, maar niet onfeilbaar. Een gering percentage personen zal bij biometrische identificatie door de apparatuur worden geweigerd. Naarmate het systeem uitgebreider wordt, zal ook de identiteitsketen ingewikkelder worden. In elke schakel van de keten kan het misgaan. Als er bij een massale toepassing van biometrie eenmaal fouten optreden, zal het moeilijk zijn deze te herstellen.

⁷ Jaap Spaans, Biometrische identificatie: digitaal brandmerk? Amsterdam: Oogstpublicaties, 2002, p. 56-57.

⁸ Ibid., p. 58-59.

⁹ COSMO, op. cit. (noot 1), p. 9.

Evenals andere computersystemen is biometrische apparatuur kwetsbaar, bijvoorbeeld als er stroomstoringen optreden of apparatuur defect raakt.

Identificatie kan worden toegepast zonder dat de betrokkene het weet. Dat geldt onder andere voor gelaatsherkenning en stemherkenning via bijvoorbeeld de telefoon.”¹⁰ Denk hierbij ook aan de pasfoto van je strakke gezichtsplooi die in ieders paspoort verplicht is gesteld. Met behulp van beveiligingscamera’s uitgerust met gezichtsherkenning is een verdachte persoon eenvoudig uit een menigte te plukken en kan direct zijn identiteit worden achterhaald wanneer deze is opgenomen in een centrale database. Ik geloof niet dat er veel mensen zijn die zich er van bewust zijn dat dit de reden is waarom zij op hun nieuwe pasfoto niet meer mogen lachen.

“Biometrie kan een bedreiging vormen voor de persoonlijke levenssfeer of privacy. Mensen kunnen meetbaar en volgbaar worden als lichaamseigen informatie op meerdere plaatsen wordt opgeslagen. Toepassing van biometrie zal leiden tot een toename van gegevensuitwisseling en koppeling van bestanden (...).

Grondrechten kunnen onder druk komen te staan. Dat geldt met name bij een centrale opslag van gegevens (...).

Het is aangetoond dat computerisering en digitalisering een samenleving niet veiliger maken. Het tegendeel is gebleken. De moderne mens individualiseert in toenemende mate en vertoont de neiging zich terug te trekken in de beveiligde en beschermde omgeving. Het is een utopie te denken dat de massale toepassing van beveiligings- en identificatiesystemen, mensen of een gehele samenleving op een hoger plan zou kunnen brengen. Criminaliteit, fraude en zelfs terrorisme zijn zaken van het hart. Door meer controle en betere identificatiemethodes kunnen deze excessen wel in

beperkte mate worden beheerst,
maar niet volledig uitgebannen.

Biometrische identificatie is bezig geleidelijk ingevoerd te worden. Er is echter wel sprake van een dynamisch proces in een samenleving die constant in beweging is. Omdat de technologie nog in ontwikkeling is, zullen er regelmatig nieuwe toepassingen bijkomen. Onverwachte gebeurtenissen of calamiteiten zouden het proces verder kunnen versnellen of invloed kunnen hebben op het draagvlak onder de bevolking.”¹¹ Dat dat zo werkt werd vooral duidelijk na 9/11. Het vergroten van de nationale veiligheid stond reeds op het programma van de EU wegens stijgende criminaliteit en een toenemend gevoel van onveiligheid toen plotseling de onverwachte aanslag van 9/11 een enorme prioriteitenverschuiving op gang bracht. Het vergroten van de nationale veiligheid werd onmiddellijk als prangende prioriteit op het to-do lijstje van de overheid gezet. Op het gebied van deze veiligheid maakt de overheid in steeds grotere mate gebruik van nieuwe media, met name op het gebied van de biometrische technologie.

¹⁰Jaap Spaans, op. cit. (noet 8)

Hoofdstuk 2

Nieuwe media en controlesystemen in de kunst: een aantal kunstenaars onder de loep

ACCESS

your little brother is watching you

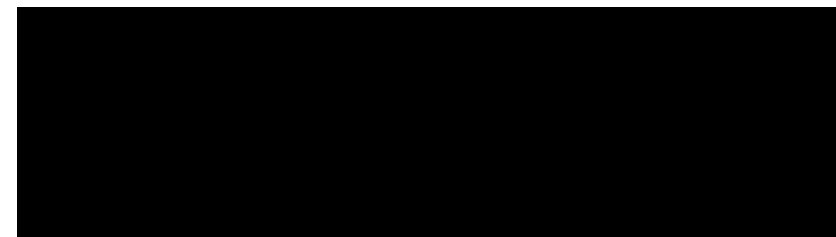
*"Beware. Some individuals may not like being monitored.
Beware. Some individuals may love the attention."¹²*



—Marie Sester, 'ACCESS', 2003—

¹² Marie Sester, "ACCESS", bezocht op 10 oktober 2009 (internet, <http://www.sester.net/projects/access/access.html>)

Marie Sester onthult door middel van haar interactieve media-kunst de dubbelzinnigheden en implicaties van verschillende technologieën, zoals de heimelijkheid ervan en de mogelijkheid tot het volgen en meten van mensen. Haar project ACCESS - beïnvloed door de schoonheid van surveillancesystemen, de onzichtbaarheid van de verzamelde gegevens, en de macht die uitgaat van surveillancepraktijken - refereert aan politieke propaganda en media-manipulatie door controlesystemen te combineren met het internet en de reclame- en Hollywoodindustrie. ACCESS roept tegengestelde emoties op: eng-grappig; obsessief-fascinerend; controleweerstand: het is onmogelijk te bepalen wie er feitelijk de controle heeft. Bij deze publieke kunstinstallatie worden internet, computer, geluid- en lichttechnologieën toegepast waarbij individuen in een publieke ruimte door internetgebruikers kunnen worden achtervolgd met een unieke robotachtige 'spotlight' en 'acoustic beamsysteem'. De achtervolgde persoon wordt automatisch door de 'spotlight' gevolgd, terwijl de 'acoustic beam' audio projecteert die alleen te horen is door diegene die in de 'spotlight' staat. De achtervolgde persoon weet niet wie kijkt of waarom hij wordt gevolgd, noch is hij zich ervan bewust dat hij de enige is die het geluid kan horen. Bovendien zijn de internetgebruikers zich er niet van bewust dat hun daden geluid opwekken naar het doelwit toe, waardoor zowel de volger als de gevolgde zich in een paradoxale communicatieloop bevinden. De inhoud van ACCESS roept op tot bewustzijn van de implicaties van surveillance, detectie, bekendheid, en het effect hiervan op de samenleving.¹³



¹³ Marie Sester, "Description and Concept", bezocht op 10 oktober 2009 (internet, <http://www.accessproject.net/concept.html>)

—Physiognomic Scrutinizer—

Ken ik jouw gezichtskenmerk niet ergens van?

'Physiognomic Scrutinizer' is een interactieve installatie van Marnix de Nijs en werd tentoongesteld gedurende het Wereld van Witte de With festival 2009. Het ontwerp is gebaseerd op de principes van de door bewakingspoortjes beveiligde publieke ruimtes. Bezoekers worden naar een fel verlichte ingang geleid, waar een camera hen vastlegt en projecteert op een LCD-monitor aan het einde van de toegangspoort. Twee luidsprekers op standaarden symboliseren bewakers. Uitgerust met biometrische systemen herkent en onderzoekt de installatie nauwkeurig de gezichten van de mensen die de expositie willen betreden. Het gaat hier echter niet om identificatie van een persoon. In plaats daarvan legt de software een link tussen de betreffende persoon en de meest overeenkomende gezichtskenmerken en karakteristieken van voorge-selecteerde personen in de database: allen uitgekozen wegens beruchte reputatie. Het genre van mensen waar we over fantaseren, maar waar we tegelijkertijd met onze vinger naar wijzen omdat er werkelijk geen ruimte is voor zulk een controversieel gedrag in onze verwende en overgecontroleerde samenleving. Vervolgens zien alle bezoekers wie de kwalijke match is en hoort iedereen een bijbehorend audio fragment. Gebaseerd op wat de software detecteert, wordt de bezoeker beschuldigd overeenkomstig de kwade naam van hun match en wordt er een met deze controversie geassocieerd audio fragment afgespeeld dat voor iedereen te horen is. De persoon die dit herkenningsproces ondergaat voelt zich over het algemeen ongemakkelijk. Ook al is hij onschuldig, hij wordt wel in deze positie geplaatst, waarbij technologie een oordeel velt en we allen weten dat technologie tevens zijn eigen logica heeft. De persoon is zich er tevens van bewust dat hij, terwijl hij wordt onderworpen aan serieuze technologische tests, zonder twijfel ergens schuldig aan zal worden verklaard. Marnix de Nijs gebruikt deze installatie als projectie van de werkelijke wereld waarin de inzet van biometrische systemen

- gebaseerd op een kruisingsmatch van het gezicht van de reiziger met dat in zijn paspoort of in gezichtsdata bases voor forensen en immigranten - de veiligheid moet vergroten.¹⁵ Hij roept net als Real Tech Support met het 'Open Biometrics Initiative' vooral vragen op over de betrouwbaarheid van biometrische systemen. Is het systeem wel altijd in staat de juiste te identificeren? En hoe voelt het om bij voorbaat te weten dat je verdacht bent?



—Marnix de Nijs, 'Physiognomic Scrutinizer', 2008—

¹⁵ Marnix de Nijs, 'Physiognomic Scrutinizer, 2008/2009', bezocht op 11 oktober 2009 (interceptie: http://www.marnixdenijs.nl/physiognomic_scrutinizer.html)



San Francisco Emotion Map
by Christian Nold

Street-mapping apps normally show maps with labels and markers. The Emotion Map is a different kind of map. It shows the emotional response of people walking through the city. The map is a grid of streets, with colored dots representing emotional data points. The dots are color-coded by Galvanic Skin Response (GSR) levels, ranging from dark red (low) to bright yellow (high). The map includes labels for streets like Colores St, Valencia St, Mission St, and parks like Golden Gate Park and Bernal Heights. A legend in the top left corner explains the color coding and includes a north arrow and a scale bar.

Biomapping
Opgewonden dansje op de brug

Een andere kunstenaar die met zijn project de focus legt op de onzuiverheid van biometrische technologieën is Christian Nold. De San Francisco Emotion Map is het resultaat van zijn residentie gedurende vijf weken in San Fransisco, waar hij 98 participanten betrok bij zijn kunstproject. Deze mensen verkenden de buurt, uitgerust met een innovatieve techniek die de Galvanic Skin Response (GSR) van de drager meet, hetgeen een simpele indicator is voor de staat van emotionele opwinding in samenhang met de geografische ligging. Het resultaat van deze wandelingen is op de kaart aangegeven door middel van gekleurde stippen en persoonlijke aantekeningen van de participanten. De San Francisco Emotion Map is een collectieve poging een emotioneel portret van een buurt te creëren en biedt nieuw gereedschap dat mensen toestaat hun eigen biodata te delen en interpreteren. Zijn strategieën kunnen terug worden herleid naar de derivé's van de Situationisten, de praktijk van het dwalen door openbare ruimtes, en psychogeografie, de studie naar de effecten van de geografische omgeving en de emoties en het gedrag van individuen.¹⁶

Bio Mapping is een bewuste reactie op de alom aanwezige beveiligingscamera's. In een interview door Anna Benthkowska-Kafel geeft Nold aan dat CCTV camera's een zeer visueel en tastbaar voorbeeld zijn van surveillance technologie. Controle over hun eigen acties en herinneringen geeft Nold de mensen niet. Zij kunnen het apparaat niet zelf aan of uitzetten. Zelf heeft hij de sleutel. Nold vindt het een prettig idee performatieve technologie te gebruiken die de gebruiker bewust maakt van de apparatuur die hij gebruikt. Zelf dirigeert hij hun leven op een bepaalde manier. Hij vraagt de participanten na te denken over de politieke en sociale

¹⁶ Christian Nold (2004, januari) "Bio Mapping" bezocht op 25 oktober 2009 (internet, <http://www.biomapping.net/>)

implicaties van deze technologie en hoe het gebruikt zou kunnen worden op grote schaal.¹⁷

De leugendetector is ons allen reeds langer bekend, de beveiligingscamera ook. Er zijn nu echter ook al programma's ontwikkeld waarmee iemands emotionele toestand door middel van gezichts-herkenning is af te lezen vanaf een beveiligingscamera. Christian Nold koppelt bekende technieken aan elkaar om een emotioneel portret van een buurt te verkrijgen. Hij heeft een leugendetector aan een GPS gekoppeld, zodat lokatie en staat van opwinding tegelijkertijd gemeten kunnen worden. Hierdoor is hij in staat bepaalde lokaties aan bepaalde emotionele toestanden van opwinding te koppelen en kan hierover gepraat worden. Mensen krijgen de gelegenheid hun ervaringen tijdens een wandeling te uiten en te interpreteren. Het maakt mensen bewust van wat ze ervaren, iets waar normaal geen aandacht aan wordt geschonken, tenzij de opwinding zo hoog is dat je er niet meer omheen kunt. Mensen worden nu gewezen op wanneer ze opwinding voelen en krijgen zo de gelegenheid bij zichzelf te ontdekken wat dat veroorzaakt heeft. Ook worden ze uitgenodigd te reflecteren op het hele gebeuren. Wat zij ervaren, kan dus ook door een bewakingscamera worden gedetecteerd. Op Google Earth zijn de projecten ook goed zichtbaar, compleet met gemaakte opmerkingen en pieken in opwindingsniveau. Hoogte van de piek is hierbij een indicatie voor opwinding en het gebruik van verschillende kleuren voor verschillende wandelingen van mensen. Mooi vond ik de piek bij een snelweg. Er bleek zich een brug te bevinden, waar iemand heerlijk op heeft gedanst. De interpretatie is dus even belangrijk als de 'pseudo'wetenschappelijke data. Ze vullen elkaar aan, het een verklaart het ander in woorden. Als je in de openbare ruimte wordt aangehouden omdat je negatieve stemming of grote opwinding is gedetecteerd door een camera heb je echter geen gelegenheid om

je emotionele toestand uit te leggen. Blijdschap kan ineens verdacht worden. Dansen op een brug al helemaal.

In het eerder genoemde interview geeft Nold aan dat mensen ook met de apparatuur proberen te rommelen. "Ze spelen ermee: springen tegen elkaar op of in een meer met water. Mensen beseffen dat het gaat om het onderwerp controle en proberen hier mee om te gaan. Bio Mapping is niet een manier om mensen over hun emoties te vertellen. Als je denkt aan Foucault, is het lichaam de plek waar alle controle wordt uitgeoefend. Het lichaam wordt politiek gecontroleerd door fysieke middelen maar ook door onze verbeelding, emoties, fantasieën en verlangens. Bio Mapping is een manier om het lichaam te overdenken. Mensen gaan meer nadenken over hoe hun lichaam aan hun geest is gerelateerd."¹⁸ Nold vertelt dat sommige mensen weigeren mee te doen omdat het een behoorlijk krachtige representatie is. "Het lijkt bijna alsof alles voor je in kaart is gebracht, maar door middel van discussies komen we terug op het punt waar we kunnen zien dat biometrische technologieën je niet alles vertellen. Ze geven ons wat abstracte hints en deze vereisen interpretatie. Persoonlijke interpretatie maakt het pas interessant en betekenisvol."¹⁹

Nold toont dus op zijn eigen manier dat technologie niet zo zuiver is. Hij belicht de bizarre en tegenstrijdige aspecten van technologie, hoe voorwerpen bezig zijn onze omgang met de wereld te veranderen.

¹⁸idem.
¹⁹idem.

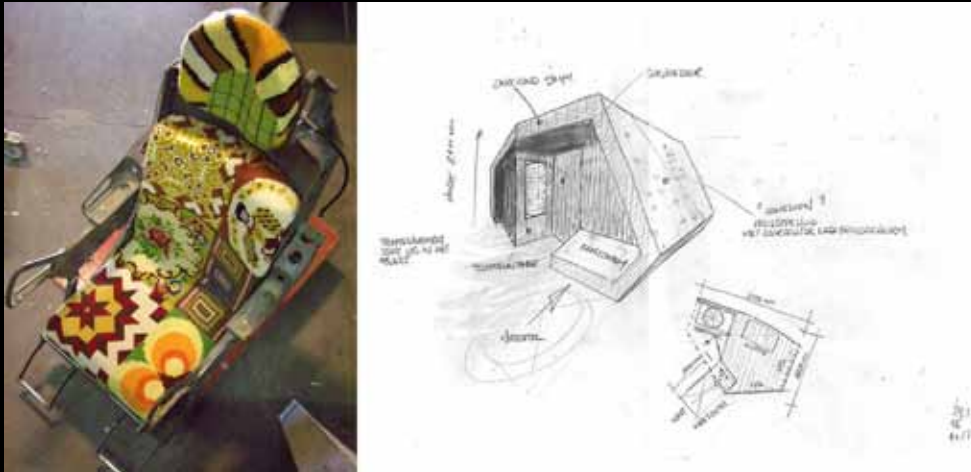
—Christian Nold, 'Biomapping', 2007—



¹⁷ Anna Benthkowska-Kafel (2006, augustus). "Christian Nold interviewed by Anna Benthkowska-Kafel". Bezocht op 25 oktober 2009 (Internet, <http://www.biomapping.net/interview.htm>)

Automeet

kunstmatige intelligentie bepaalt consumptiegedrag



CO2 Ruimtelijk Ontwerp en JWA Systems, 'AUTOMEET', 2006

De door CO2 Ruimtelijk Ontwerp en JWA Systems ontwikkelde AUTOMEET is een high tech biometrische bar. Je werpt een muntje van twee euro in het apparaat en gaat zitten in de stoel waarin meetapparatuur is verwerkt. Binnen een halve minuut wordt de fysieke conditie van de gezetelde gemeten en valt er een op basis van metingen van hersenactiviteit, bloeddruk, hartslag, alcoholpromillage, lichaamstemperatuur en het omgevingsgeluid geselecteerde versnapering in de opvangbak of wordt door de machine bereid. Naast een keuze uit een ruim assortiment van eetbare producten biedt de machine ook non-food aan in de vorm van rustgevend objecten. De interactieve machine gaat op zoek naar het uit te geven artikel dat het gunstigst is voor het verkrijgen van een 'normale', gezonde, actieve toestand van de consument. Bij een hoge hersenactiviteit en bloeddruk zal er een kalmerend middel geselecteerd worden. De meetresultaten kunnen worden ingezien en worden vertaald in een lichtspel. Het object is vervaardigd uit resthout, bekleed met gerecycled polyester, waaronder zich printplaten en 2000 LED lampjes bevinden. Binnenin het object zitten een trommelautomaat voor food en non-food, een koffieautomaat en de hardware die de vendingmachines aanstuurt verstoppt. De stoel is een omgebouwde schietstoel uit een Klu F84, waarin meetapparatuur verwerkt zit om de biometrische gegevens te meten.²⁰

De AUTOMEET is in mijn ogen een prachtig voorbeeld van waar we in de toekomst mogelijkwijs mee te maken zullen krijgen, wanneer steeds meer persoonlijke gegevens van de mens worden gemeten en gebruikt voor andere dan medische toepassingen.

²⁰ Antenne Rotterdam, "Onthulling van een biometrische bar", bezocht op 25 november 2009 (internet: http://www.antennerotterdam.nl/read/antenne_item/id/996600/templ-antenne_print.html)

—Planbperformance—

de dagelijkse praktijk van kaarten maken

"If at the end of your life, you could look at the shapes your wanderings over the earth have made, what patterns would you see? What words might be formed that take a human lifetime to write?"²¹



—Daniel Belasco Rogers, 'Planbperformance', Berlijn: five year drawing, 2003-2008.—

Daniel Belasco Rogers groeide op in London en associeerde persoonlijke herinneringen met elke bekende straat. Toen hij naar Berlijn verhuisde, een stad die hij nog nauwelijks kende, besloot hij te documenteren hoe hij deze stad leerde kennen, hoe de mentale mappen van de stad in zijn hoofd groeiden terwijl hij zijn lichaam door de straten navigeerde. Hij voelde een sterk verlangen elke trip die hij maakte te catalogiseren om zijn levensverhaal te kunnen lezen, zijn persoonlijke kaart te kunnen aanschouwen, gedurende de jaren geschreven door zijn verouderende lichaam op het oppervlak van de aarde. De tekening die een leven lang zou duren voor hij hem af zou hebben. Sinds 2003 heeft hij elke trip die hij maakte opgenomen met behulp van een GPS (Global Positioning System) en heeft hij op grote kaarten de sporen verzameld die deze trips achterlieten.²²

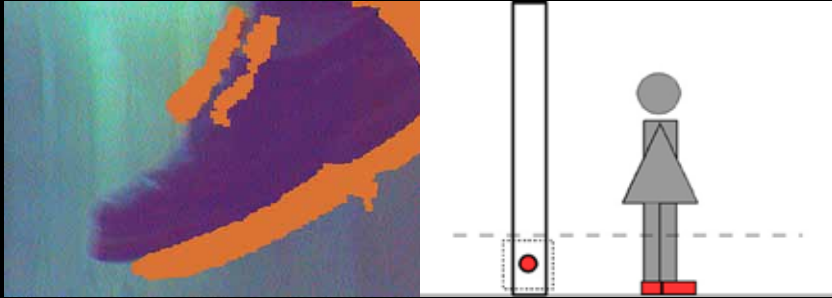
In mijn ogen heeft Daniel Belasco Rogers het GPS systeem, dat hoofdzakelijk wordt gebruikt om de gang van gedetineerden te volgen, eigen gemaakt. Hij wordt niet geobserveerd en gevolgd, hij volgt zichzelf en maakt zijn gang kenbaar aan de toeschouwer. Zijn lot ligt in eigen handen, in plaats van in die van de staat. Het volgsysteem dat hij voor zichzelf hanteert is echter wel even intensief. Hij is er iedere seconde mee bezig in zijn hoofd en in de praktijk, heeft het compleet geïnternaliseerd op vrijwillige basis. Zijn leven is een performance geworden en hij wordt bepaald door zijn eigen controlesysteem.

²¹ Daniel Belasco Rogers (met 2004), "The daily practice of map making", bezocht 25 oktober 2009 (internet, <http://www.planbperformance.net/dan/Texts/RadiusEdit.pdf>)

²² Idem.

—Shoeveillance—

een vriendelijk surveillancesysteem



—Marc Böhlen, 'Shoeveillance', 2006—

Marc Böhlen van wederom Real Tech Support heeft een interessante visie op de surveillance van mensen in een gebouw. Hij erkent dat surveillance noodzakelijk is in deze wereld, bijvoorbeeld om na te gaan wie er zich nog in een brandend gebouw bevindt. 'Shoeveillance' maakt het mogelijk de loop van mensen in en uit een ruimte of een gebouw te monitoren. In plaats van bewakingscamera's in de hoogte te plaatsen en gezichten te bekijken, plaatst hij ze laag en brengt hij voeten met schoenen in beeld. Tegelijkertijd telt het 'data-creep' en voorkomt data die niet verzameld hoeft te worden. De camera ziet alleen voeten en benen tot kniehoogte; het algoritme vindt alleen de richting van beweging en objecten die eruit zien als schoenen. Het idee is een surveillance systeem voor het automatisch tellen van mensen en voor veiligheid dat veel minder inbreuk doet op de privacy. Het gaat dan eigenlijk om maximale dataverzameling en een minimum aan inbreuk. "Dit is een manier om bestaande problemen op te lossen waar mensen wel blij van worden. Mensen hebben een verlangen gezien te worden, maar niet op de manier van de huidige bewakingscamera's. Liever showen ze hun kleding, of in dit geval hun schoenen. Shoeveillance maakt het mogelijk met je nieuwe schoenen te paraderen, wat een speciaal plezier is, een geaccepteerde vorm van exhibitionisme."²³

²³ We-make-money-not-art. "Interview of Marc Böhlen", bezocht op 25 oktober 2009 (internet, <http://www.we-make-money-not-art.com/archives/2006/05/interview-of-ma.php>)

—De-surveillance—

er is een ontkomen aan

'Het is onmogelijk je de Rotterdamse straatscene voor te stellen zonder surveillance camera's. Waar je ook gaat word je geobserveerd! De interactieve interventie 'de-surveillance' laat voorbijgangers verdwijnen voor het alziend oog van de bewakingscamera. Kunstenaar Sander Veenhof laat bezoekers op een speelse manier hun privacy terug nemen. Hij ontdekte dat de surveillance camera op de hoek van de Witte de Withstraat / Hartmansstraat in Rotterdam een specifiek type van de kleur blauw niet aankon, en buitte dit een kwetsbare foutje uit in de context van de 'For Security Reasons' expositie in Showroom MAMA door de camera op een ludieke wijze te hacken. Een tijdelijke 'de-surveillance service point' op dezelfde straathoek assisteerde bezoekers bij het De Wereld van Witte de With festival bij het verdwijnen voor het Rotterdam surveillance camera netwerk: door iets blauws te dragen konden zij onzichtbaar worden.²⁴



Sander Veenhof, 'De-surveillance', 2009

²⁴ SNDRV. "De-surveillance", bezocht op 23 november 2009 (internet, <http://www.sndrv.nl/de-surveillance/>)

—Perpetual Self-Dis-Infecting Machine—

Besmettelijke paranoia

“You people are pathetic fools. Do you truly believe that a virus is art? Innovative, perhaps. Interesting, maybe. But art? No. I’m not even saying what you’re doing is dangerous. It’s stupid and petty. Find yourself a real medium to work with or get a real job. ‘Cause this ain’t art.”²⁵

De kunstenaars van het collectief 0100101110101101.org ontvingen deze mail als reactie op het virus dat zij ‘tentoon hadden gesteld’ (lees: hebben verspreid) gedurende de 49ste Biennale in Venetië. Het project veroorzaakte veel commotie en irritatie, zoals blijkt uit bovenstaande reactie. Het kunstenaarscollectief wilde met het (onschuldige) virus laten zien in welke mate computervirussen worden gemediatiseerd: “We are not interested in damaging a computer, but more on the media effect viruses have.”²⁶ Op het moment dat een nieuw virus op het net verschijnt, ontstaat er een echte hysterie en worden er duizenden waarschuwingsberichten over de hele wereld verspreid.

Biennale.py is zowel een computervirus als een kunstwerk; het produkt van de organisaties epidemiC and 0100101110101101.ORG, wel bekend als mediahackers die vaak grenzen aan illegaliteit. Biennale.py werd hoofdpaginanieuws, waarmee het ineens een onaangekondigde performance werd, een controversieel kunstwerk dat laat zien hoe mediahysterie theoretisch kan worden opgewekt. Het werk toont de eindeloze aanval en tegenaanval van de virussen en antivirussen die de computingwereld infecteren. Het project brengt vele van de politieke, culturele en zakelijke kwesties aan het licht die uniek zijn voor de netwerkgemeenschap, terwijl

²⁵ V2, “Archive”, bezocht op 1 november 2009 (Internet, <http://www.v2.nl/archive/articles/sengmuller-grewenig-wirschner-stulgin-0100>)

²⁶ Idem.

Hoofdstuk 3

Een inzoom op de urgentie

het aanzet tot het bevragen van onze conventionele ideeën van identiteit, originaliteit, en de rol van de kunstenaar in de tijd van anonieme technologische reproductie. Eva, 0100101110101101.ORG's woordvoerder, zegt: "As part of an organization that produces art, my only responsibility is to be irresponsible. Once you set a virus free you loose control over it, you decide on when and where the performance begins, but you'll never know when and where it'll lead. It'll spread out of control, it'll make a round-the-world trip over two minutes, it'll go where you'll never go over your entire life, chased by anti-virus cops trying to regain control over it. In this very moment it's wandering around at the speed of byte. It's an art form that finds you, you don't have to go to museums to see it, the work itself will reach you inside your house."²⁷

Biennale.py is het eerste computervirus ooit geschreven in de 'Python programming language' en benadrukt zijn 'esthetische kwaliteite' met de schoonheid van zijn eigen broncode, een 'liefdesgedicht' dat integraal onderdeel is van zijn eigen uitvoerende code. Tijdens de Biennale konden mensen de broncode lezen en de werking testen op geïnfecteerde computers. Duizenden t-shirts met een print van de broncode van het programma werden weggegeven en verkocht: *Biennale.py* verspreidt niet alleen via machines, maar zoals bij biologische virussen ook door het menselijk lichaam.²⁸

Dit virus is in mijn ogen een goed voorbeeld van hoe paranoia eenvoudig kan worden aanzet en op zeer rap tempo wereldwijd kan worden verspreid.

Het gaat de besproken kunstenaars vooral om de urgentie van de ondermijning van onze bewegingsvrijheid, door het in het kader van de nationale veiligheid door de staat inzetten van technische vernieuwingen op het gebied van controlesystemen. Zij proberen met hun nieuwe media kunst mensen bewust te maken van de controle- en volgsystemen waar iedereen vrijwel dagelijks mee te maken heeft, veelal zonder het door te hebben. De kunstprojecten ACCESS, Open Biometrics initiative, Physiognomic Scrutinize, Bio-mapping en de Automeet brengen op een ludieke en toegankelijke manier de implicaties die -naast de voordelen- ook aan de biometrische systemen en technologieën kleven onder de aandacht. De projecten Planbperformance, De-surveillance en Shoeveillance richten zich niet direct op een bewustmakingsproces van de implicaties, maar bieden mogelijke oplossingen. *Biennale.py* is een prachtig voorbeeld van hoe paranoia kan worden opgewekt en angst in rap tempo kan worden verspreid. En deze angst, daar wil ik het over hebben wanneer ik inzoom op wat in mijn eigen ogen de urgentie is.

Iedere burger draagt uit angst voor terrorisme een vrijwillig steentje bij aan de nationale veiligheid door na elke -veelal mislukte- terroristische aanslag weer een klein beetje van zijn privacy in te leveren in het kader van het algemeen belang. De overheid zet echter in 'the war on terror' in alle haast ondoordacht nieuwe biometrische technieken in met gebrek aan kennis over de gevaren. Deze technieken zijn eenvoudig aan te scherpen en uit te breiden door de wetgeving te veranderen in het kader van de veiligheid. De burgers laten het door de geleidelijke invoering gestaag over zich heen komen, als kikkers die zich in langzaam opkokend water gaar laten koken. De overheid heeft voor hen een overtuigende angstcultuur gekweekt, waarin het niet gepast is mede-

²⁷ 0100101110101101.org . "Contagious Paranoia" bezocht op 1 november 2009 (internet: <http://www.0100101110101101.org/home/biennale.py/index.html>)

²⁸ Idem

werking te weigeren in het algemeen belang. Deze angstcultuur wordt in stand gehouden door een systeem dat afgeleid is van het eeuwenoude 'panopticum' van Jeremy Bentham en de daaruit voortvloeiende ideeën over disciplineren van Michel Foucault. Het principe van een surveillancesysteem is al eeuwenoud. Eind 17^e eeuw is men begonnen met surveillance op basis van een systeem van permanente registratie om de plaag uit te bannen. Elk individu werd compleet geregistreerd en zichtbaar gemaakt. De scheiding van 'normalen' en 'abnormalen' was geboren, en is in onze tijd nog steeds aanwezig; het bestaan van een hele set aan technieken en instituten voor het meten, toezicht houden op en het corrigeren van de abnormalen brengt het disciplinerende mechanisme in het spel waar de angst voor de plaag toe aanzette. Alle mechanieken van macht die, zelfs vandaag de dag, rond het abnormale individu worden geordend, om hem te brandmerken en veranderen, komen voort uit Bentham's architectonische ontwerp voor een Panopticum:²⁹ "De te beheersen personen worden in individuele cellen geplaatst in een dubbelwandig cirkelvormig gebouw, met ramen zowel naar buiten als naar de binnenkant van de cirkel. In het midden van de cirkel staat een toren met ramen naar alle kanten, waar de opzichter zich bevindt. De opzichter ziet zonder dat hij gezien wordt, de geïsoleerde individuen worden door de opzichter ge- en herkend zonder dat ze zelf kunnen (her)kennen. Niet voor niets noemde Bentham zijn model "een nieuwe wijze om macht te krijgen van geest over geest, in een tot heden ongekende omvang". Het rendement van het panopticum zit 'm in drie principes: zichtbaarheid van elk individu afzonderlijk, herkenbaarheid van elk individu, en overzichtelijkheid van de massa of groep."³⁰ "Volgens de Franse filosoof Michel Foucault bood het panopticum van Bentham volop mogelijkheden om mensen te disciplineren(...). Het panoptisch model en de disciplineren zijn onlosmakelijk met

²⁹ Michel Foucault, "Panopticism", in *Visual Culture: the reader*, ed. Jessima Evans en Stuart Hall, p. 61, 1/11/79.
³⁰ Gerrit de Wit en Harry Westerink, "Het alziend oog", bezocht op 24 oktober 2009 (internet, <http://www.geblader.nl/00735p44.htm>)

elkaar verbonden. Het panoptisch model is de vorm, de discipline (en het gedisciplineerde individu) is de inhoud. Het model gaat in de hoofden van mensen een eigen leven leiden(...). Niet de wet zorgt voor handhaving van orde en discipline, maar disciplineren zorgt voor handhaving van de wet"³¹

—**Wie is hier nu eigenlijk de terrorist?**—

De versie van het hedendaagse panopticum is zodanig uitgebreid dat een panopticum in de vorm van een gevangenis niet meer nodig is. Niet alleen criminelen in een gevangenis worden in de gaten gehouden zodat ze zich gedragen, tegenwoordig wordt iedereen in de gaten gehouden. In de openbare ruimte hangen op een grote hoeveelheid plekken videocamera's, die werken als disciplineringsmechanisme. Bijna iedereen is het inmiddels wel gewend om op zo'n manier bekeken te worden en heeft de aanwezigheid van registrerende camera's geaccepteerd. Vooral mensen die afwijkend gedrag (willen) vertonen hebben er last van dat ze bekeken worden. Als gedisciplineerd mens schudden ze dat gevoel echter van zich af en verdringen ze het. Er blijft echter constant een waarschuwing in het achterhoofd hangen: hou je koest, anders wordt je opgepakt. Niet alleen mensen die graag afwijkend gedrag (willen) vertonen, maar ook de brave burger voelt constant de aanwezigheid van dat alziend oog. Of je het wil of niet, dat oog blijft in je rug prikken. Inmiddels zijn we zelfs zo ver dat het niet eens meer nodig is veel bewakers in te zetten. Het idee van in de gaten gehouden worden is al zo sterk in onszelf geïntegreerd, dat het geweten van het individu zelf er voor zorgt dat hij zichzelf monitort. Mensen gedragen zich 'naar' de camera. Het gevoel geobserveerd te worden zorgt voor disciplineren. Zo kan een groep mensen zo groot als de gehele wereldbevolking gestuurd worden door een relatief klein aantal 'alziende ogen'.³²

³¹ idem.
³² idem.

De term “panautomaticum”³³ is in dit opzicht zeer gepast: een eigentijdse nieuwe vorm van panoptische structuren die met behulp van automatisering een alomtegenwoordig karakter hebben gekregen “om macht te krijgen van geest over geest, in een tot op heden ongekende omvang.”³⁴ In het kader van de veiligheid en het terugdringen van het terrorisme is de overheid overgegaan tot geleidelijke maar drastische invoering van dit panautomaticum, door middel van het inprenten van angst en het invoeren van biometrische systemen. Ik vraag mij ten zeerste af of dit middel niet vele malen erger is dan de kwaal.

Een Duits filmpje op YouTube geeft op een heldere manier aan wat er nu al mogelijk is en waar bijna niemand zich van bewust is. Vanwege terreurdreiging wordt elke burger zonder uitzondering in al zijn activiteiten gevolgd en geregistreerd. Wie je belt en wanneer. Wanneer je je mobiele telefoon gebruikt en waar. Wanneer en waar je toegang hebt tot het internet. En welke sites je bezoekt. Naar wie je e-mails schrijft en waarom. En omdat iedereen ervan verdacht wordt een terrorist te zijn heeft de BKA toestemming je computer te doorzoeken.³⁵ Het filmpje vervolgt met: “We know your passwords. We can look at your pictures. We can see who you are chatting with. Or browse through your documents. We can download all the files from your computer. Change them or save completely new files.”³⁶ In Duitsland is er nog nooit een terroristische aanslag gepland, maar “we have to be careful that this doesn’t change.”³⁷ Dit heeft geleid tot een nieuwe ID, die digitaal vingerafdrukken opslaat, meer video surveillance camera’s, en meer staat ons nog te wachten, zoals naaktscanners, een ID voor in de zorg, en een internetcensuur.³⁸

³³ Idem.

³⁴ Idem.

³⁵ Alexander Lehmann, “Du bist terrorist”, bezocht op 26 november 2009 (internet, <http://www.youtube.com/watch?v=SGF2r2vewZQ>).

³⁶ Idem.

³⁷ Idem.

³⁸ Idem.

Terreur is van alle tijden. Sinds mensenheugenis bestaat het al. De technologische ontwikkeling heeft er alleen voor gezorgd dat de impact van de terreur vele malen wordt vergroot en er in één keer een groot aantal mensen er de dupe van is. Als we kijken naar de mate waarin het terrorisme kan worden teruggedrongen door de invoering van deze nieuwe systemen, dan is te verwachten dat het effect minimaal zal zijn, omdat de praktijk heeft uitgewezen dat criminelen vaak over ruime financiële middelen beschikken en niet schromen om deskundigheid in te kopen om de fraudegevoeligheid van beveiligingssystemen te onderzoeken en deze vervolgens te gebruiken. De verwoede poging de wereld door middel van computerisering en digitalisering tot een veiligere wereld te maken werkt alleen maar averechts. Mocht misbruik wel lukken, dan zal dit een grotere impact hebben.³⁹ De terrorist is echter al veel sterker komen te staan, doordat de burger de angst voor terrorisme heeft geïntegreerd in zijn wezen, in zijn bestaan. De angst zal steeds dieper geworteld raken, de terrorist zal steeds machtiger worden zonder er ook zelf maar iets voor te hoeven doen.⁴⁰

Terwijl de overheid de burger dient te beschermen tegen terrorisme zorgt zij er juist voor dat het de burger is die de meeste schade ondervindt, en wel op het vlak van de privacy. Naar mijn mening hebben de overheid en de media meegeholpen aan het volbrengen van het doel van de terrorist, door de angst voor terrorisme verder te vergroten en te verspreiden. Volgens Jeroen Boomgaard bestaat er “een curieuze verbinding tussen terreur en vertoning. De dood is nooit het enige doel van de aanslag, de terrorist hecht vaak meer belang aan zichtbaarheid. Daarbij kiest de terreur altijd voor het op dat moment dominante medium. Optimale theatraliteit gaat dan samen met maximale aandacht.”⁴¹ Naast zichtbaarheid is spektakel een belangrijk wapen van de terrorist. Zichtbaarheid en spektakel zijn eenvoudig geworden door de alom tegenwoordige

³⁹ Jeroen Boomgaard, op. cit. (noot 7), p. 58-59.

⁴⁰ Hans van Driel en Anke Coumans, ‘Het onvoorstelbare. De werkelijkheid van beeld.’

⁴¹ Jeroen Boomgaard, ‘Terreur en Kunst’, Metropolis M No 2 2005 april/mei, bezocht op 27 november 2009 (internet, <http://www.metropo1ism.org/magazine/2005-n02/terreur-en-kunst/>).

aanwezigheid van het internet, de media en de camera van de burger.⁴²

De controle speelt in op psychologische angst. Anke Coumans geeft in haar artikel 'Terreur: de produktie van traumatische beelden' aan dat "het beeld dat de terreur produceert van groter belang is dan de terroristische daad zelf(...). Het werkt diep op ons onbewuste in en laat ons zelf onze eigen beelden van terreur produceren(...). Om bevrijd te zijn van deze angst zijn we zelfs bereid onze vrijheid op te offeren(...). Onze regeringen sluiten zich aan bij dit project van angst door onze angst voortdurend te bevestigen en zelfs aan ons op te dringen."⁴³ Door in gedachten de technologische ontwikkeling te koppelen aan wat de terrorist op bizar grote schaal aan zou kunnen richten is in onze op preventie gerichte tijd voldoende om tot grote veiligheidsmaatregelen over te gaan. Een volgende aanslag hoeft al niet meer werkelijk te worden gepleegd. In het hoofd van iedere burger is deze al in volle gang. Men hoeft nu alleen maar te denken aan de enorme dreiging die uitgaat van *het idee* van een nucleaire aanslag en er wordt al op geanticipeerd. De wereld moet steeds veiliger gemaakt worden, meer weerbaar tegen terroristische aanslagen. En hiermee snijden we onszelf in de vingers. De cirkel is rond, de terrorist heeft zijn taak volbracht: elke burger is verstrikt geraakt in de angst en handelt naar de wil van de terrorist.⁴⁴

Paniek. Paniek! PANIEK!

De wereld heeft te maken met één grote massahysterie. Iedereen is verdacht. Iedereen is terrorist. Die vriendelijke buurman die u altijd begroet tijdens het wateren van zijn bloempjes in de voortuin? Het zou zomaar eens zo kunnen zijn, dat hij er in de late uurtjes heel wat andere plannen op nahoudt. Misschien beraamt hij wel samen met alle andere inwonenden van het zo rustige dorpje een

⁴² Hans van Driel en Anke Coumans, op. Cit. (noot 40)

⁴³ Idem

⁴⁴ Idem

echte terroristische aanslag. Doordat de overheid en de media angst zaaien en verspreiden over terreurdreiging, raken mensen hierdoor geïndoctrineerd. We zijn allemaal bang gemaakt door de overheid in het kader van de staatsveiligheid. De angst voor terrorisme is in een ieder voelbaar. De vraag is: krijg je te zien wat er echt speelt? Mag ik u dan vragen: maar wie is er nu eigenlijk de terrorist?

Ik ben van mening dat de overheid en de media zelf de angst voor terrorisme verspreiden en uitvergroten, waarmee zij in feite zelf de terrorist zijn. Door tegelijkertijd steeds grotere angst voor terrorisme te kweken en de surveillance technieken te verbeteren en uit te breiden, wordt er een steeds grotere voedingsbodem gekweekt voor een totale wereldorde. De kans op een auto-ongeluk is vele malen groter dan de kans op een terroristische aanslag. Kunnen we niet beter met zijn allen er op gaan letten dat we wat minder hard rijden? Ik denk niet dat het terrorismegevaar zo groot is als waar wij nu zo bang voor gemaakt worden. In feite is de terrorist nu al geslaagd in het grootste resultaat dat hij kan bereiken: elke burger is bang en hij heeft de grootste macht. Volgens mij heeft de overheid gezorgd voor zowel een onzichtbare toezichthouder als een onzichtbare vijand, waarbij iedereen voelt dat hij constant gemonitord wordt en er een constante dreiging bestaat.

Hoofdstuk 4

Afstudeerproject

Waar het gevaar van biometrie ligt moge duidelijk zijn. Gegevens kunnen in verkeerde handen vallen van criminelen, maar ook van bedrijven en van de overheid. Bovendien worden alle burgers bij voorbaat verdacht en boeten zij sterk in aan privacy en bewegingsvrijheid. Het opstellen van risicoprofielen voor niet alleen criminelen maar voor alle burgers die 'afwijkend gedrag' vertonen werkt in mijn ogen een 'self fulfilling prophecy' in de hand. Als mensen eenmaal een label opgeplakt krijgen, gaan ze zich daar ook naar gedragen. En door steeds meer gedrag te bestempelen tot afwijkend, is er straks helemaal niemand meer veilig. Als alles hoopvol in werking treedt zullen er fouten en incidenten plaatsvinden die niet goed te praten zijn. Hoe meer we centraliseren om terrorisme te voorkomen, hoe meer focus we creëren voor datzelfde terrorisme. En hoe verder we gaan in de techniek, hoe verder we het terrorisme kunnen voeden, wat we eigenlijk willen bestrijden. We maken het alleen maar onnodig complex voor onszelf waarbij de burger ook nog eens steeds meer aan privacy inboet, terwijl het uiteindelijk niets significant zal opleveren. Het is niet onwaarschijnlijk dat we straks een wereld van gated communities hebben gecreëerd waarbij de tussenwereld een onderwereld bovengronds is met criminaliteit en armoede.⁴⁵

De overheid helt in de balans tussen veiligheid en privacy sterk over naar de veiligheid. Probleem is dat deze behoefte aan veiligheid door een door de overheid en de media zelf gecreëerd en versterkt angstbeeld steeds extremer wordt en het eenvoudig is vanwege die behoefte de wet aan te passen waarbij de burger nog verder aan privacy inboet. En waar ligt dan de grens? De techniek gaat snel vooruit, maar een stapje terug is niet meer te nemen.

⁴⁵ TILT, op. cit. (noot 4), p. 49

Met elke stap vooruit begaan we in mijn ogen een vergissing en maken we wat makkelijker oogt juist complexer. Informatie zal heimelijk worden gewonnen en ook dat vind ik een te grote inbreuk op de privacy. We hebben niks meer zelf in de hand. Vrijwilligheid is verdwenen, we staan onder dwang. En de privacy, die ligt op straat.

De wereld is een panautomaticum geworden en dat is een wereld waar ik niet graag in leef. Vrijheden die we verworven hebben moeten we nu stap voor stap weer inleveren, alleen maar omdat we met z'n allen door de media en de overheid verschrikkelijk bang zijn gemaakt voor een onzichtbare vijand. De angst zit in ons hoofd genesteld. Door urgente dreigingen van buitenaf wordt deze angst bevestigd en heeft de overheid ruim spel om de regels en wetten wederom verder aan te scherpen, zoals in tijden van de plaag het geval was. De privacy boet hierbij automatisch aan in, want veiligheid gaat boven alles.

Als huidige intelligente beeldmaker wil ik meehelpen aan de bewustmaking van de angstcultuur als tegenwicht tegen de boodschappen die nu worden uitgezonden om deze angstcultuur juist te behouden. Ik wil een tegenaanval inzetten tegen de terreur van de angst door mensen er bewust van te maken dat de angst voor terreur zwaar overtrokken is en dat de manier van controle door middel van surveillance van tegenwoordig in plaats van de terreur oplost ons als burgers juist inperkt in bewegingsvrijheid. De meeste kunstenaars die ik heb besproken geven vorm aan de angstgevoelens die de nieuwe ontwikkelingen oproepen op het gebied van biometrische technologieën door via het gebruik van soortgelijke technieken een bewustmakingsproces op gang te brengen van de implicaties ervan. Ik ben niet technisch onderlegd, dus deze optie valt voor mij af. Wel kan ik mijn kwaliteiten als illustrator inzetten in het op gang brengen van een bewustwordingsproces. Wat ik interessant vind aan de projecten van Shoeveillance en De-surveillance is het oplossingsgerichte karakter ervan. Deze projecten

maken ons niet puur bewust van de implicaties, maar bieden ook een manier om anders met de situatie om te kunnen gaan. Shoeveillance richt zich op een oplossing voor de overheid, zodat deze de burger een meer privacyvriendelijke surveillance-methode kan aanreiken. Zelf ben ik meer gecharmeerd van de oplossing die De-surveillance biedt. In dit project wordt namelijk uitgegaan van een bestaande situatie en is het niet de overheid, maar de burger zelf die het initiatief neemt actief zijn privacy terug te nemen. Op deze manier wil ik mijn eigen project ook aanpakken. Gezien de complexiteit van de situatie ga ik uit van een voortschrijdende monitoring en registratie van private gegevens, waarbij ik de burger zelf het initiatief laat nemen zijn overgebleven karige stukje privacy te kunnen waarborgen. Ik focus me hiervoor op fantasievolle scenario's van de gevolgen van een controlestaat op de privacy, die enorm zullen kunnen zijn, niet alleen in de publieke ruimte, maar ook in de private ruimte. Onderzoeksbureau TILT heeft zich al bezig gehouden met toekomstscenario's, waar ik samenvattend een gedeelte uit naar voren wil halen:

Er zijn nog maar weinig plekken in de openbare ruimte waar je totale privacy hebt. De regering heeft de openbare ruimte gemaakt tot een steriele verkeersruimte, waarin alle ongewenste contacten, personen en activiteiten angstvallig bestreden worden. In de publieke ruimte hangen veel camera's die de wandel van burgers vastleggen. Door de combinatie van gezichtsherkenning en de vastlegging van alle biometrische gegevens in een centrale database die door justitie kan worden ingezien, kan een burger geïdentificeerd worden. Het is ook al mogelijk bepaald gedrag door camera's te laten herkennen. Burgers zijn dus door de verplichtstelling van biometrische gegevens in het paspoort en de registratie door camera's bij voorbaat verdacht. In de publieke ruimte zal iemand zich koest houden of juist helemaal doorschieten, omdat hij zich niet in het systeem kan schikken. Het wordt een gedigitaliseerde publieke ruimte, waar fysieke en virtuele ruimte één worden.

“Als we door de fysieke ruimte bewegen, dragen we onze virtuele identiteit met ons mee. Onze virtuele identiteit zorgt voor een zeker gemak en een gevoel van controle: we vinden onze weg, betalen en krijgen toegang. Tegelijkertijd wordt de technologie ook door bedrijven en overheden ingezet om de gebruikers te volgen, controleren en sturen. De volgende handelingen worden in toenemende mate gedigitaliseerd: lokaliseren, betalen, identificeren, autoriseren en profileren.”⁴⁶ De burger wordt steeds transparanter in de publieke ruimte en is bijna niet meer dan virtueel. Op basis van groepsprofielen kan iemand onterecht een bepaald stempel opgedrukt krijgen en daar nooit meer vanaf komen.

De private ruimte blijft natuurlijk de eigen woning, die steeds meer zal worden afgeschermd van de onveilige omgeving. Er zullen gated communities ontstaan, waar een gevoel van veiligheid wordt gecreëerd. Deze private ruimtes worden echter steeds meer verweven met de publieke ruimte door het internet. “De woning wordt onderdeel van een netwerk, waarbij processen in de woning van buitenaf raadpleegbaar en stuurbaar zijn, en waarbij de buitenwereld meer dan ooit de huiskamer binnenkomt.”⁴⁷ Dwars door de bunker heen is de burger toch nog zichtbaar via het computernetwerk. De computer kan door politie of hackers worden binnengedrongen en telecommunicatie kan worden afgetapt. Zelfs binnenshuis zal het alziende oog voelbaar zijn. Er zullen ook bewakingscamera's binnenshuis geplaatst worden voor de veiligheid.

Dit zijn beelden uit de toekomst die weleens waarheid zouden kunnen worden. In mijn project wil ik -naast het tonen van een aantal mogelijke gevaren- scenario's schetsen van mogelijke manieren waarop de burger zijn steeds beperkter wordende privacy kan proberen te beschermen binnen de veranderende publieke en de private ruimte, zonder dat hij grote protestacties onderneemt.

⁴⁶ Ibid., p. 30.

⁴⁷ Christiaan van 't Hof, Digitalisering van de openbare ruimte. Vrij surfen binnen een groeiende poortjeszuur. Position paper, Rathenau Instituut, 2008, p. 1.

Een soort Darwiniaanse adaptatie aan de veranderde omgeving.

Hiermee wil ik elke burger een spiegel voorhouden en laten nadenken over wat de gevolgen zouden kunnen zijn voor hemzelf. Als je door de overheid compleet wordt uitgekleet en in je nakie staat, bij voorbaat verdacht, hoe kun je je privacy dan nog zoveel mogelijk waarborgen? Hoe kun je je ware identiteit dan nog tonen? En dan doel ik niet op de opgedrongen identificatieplicht...

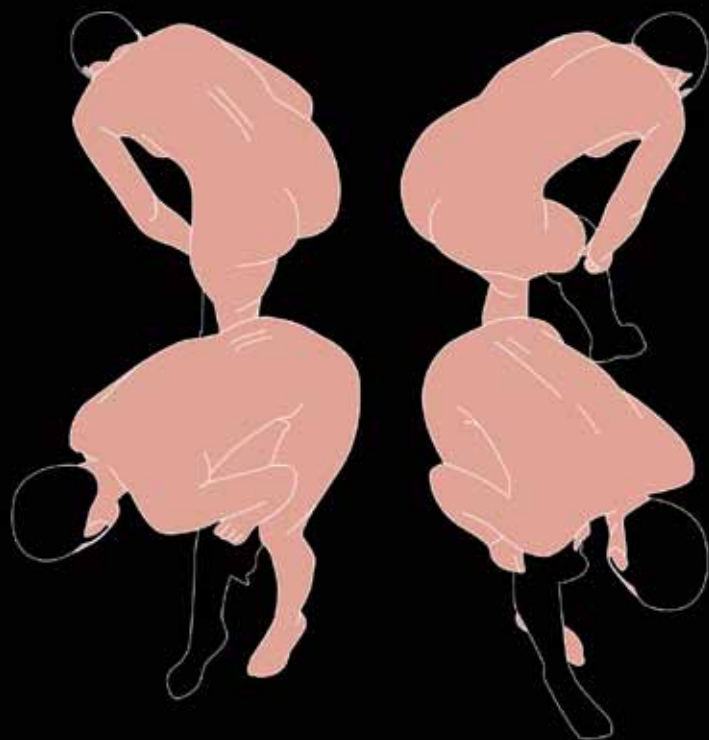
Ik heb de drie belangrijkste scenario's van mijn afstudeerproject uitgekozen om in mijn scriptie wat nader te belichten. Deze scenario's vormden mijn startpunt van waaruit ik ben gaan illustreren.⁴⁸

— Identificatie en identiteit (beharing/ontharing) —

Stel dat de overheid beslist dat kleding verboden wordt en iedereen naakt over straat moet, zodat er niks verborgen kan blijven. Om zich niet geheel naakt te voelen en het niet te koud te krijgen kan de burger hierop reageren door en masse over te gaan op transplantatie van complete lichaamsbeharing. De overheid tolereert dit vervolgens, mits de haargroei de centimeter niet overstijgt. Om toch zijn identiteit uit te kunnen dragen kan de burger in zijn vacht lokaal motieven aanbrenge door delen weg te scheren. In de zomer is het wat minder urgent om de kou te weren. Vachten kunnen weggeschoren worden, waardoor er fraaie lichaamstattoeages zichtbaar worden. Deze tattooeages kunnen dienen ter misleiding van de met gezichtsherkenning uitgeruste camera's .

⁴⁸ Omdat deze scriptie eerder zal zijn afgerond dan mijn afstudeerproject, zijn eventuele wijzigingen voorbehouden.



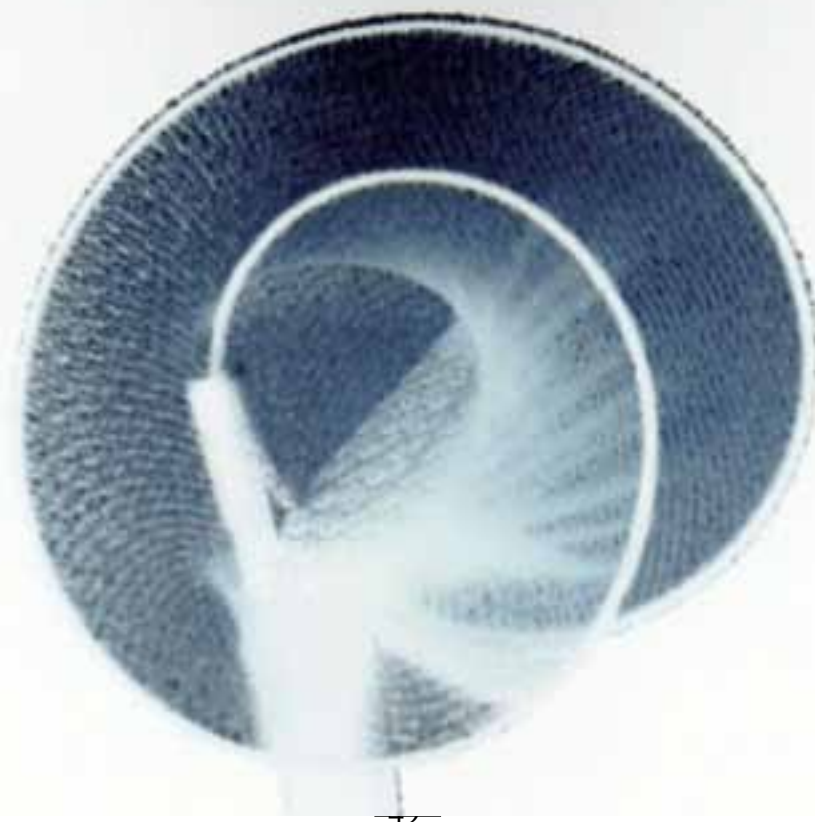


—Privacy in de private ruimte (ICU)—

Stel: de overheid kondigt aan in alle vier de hoeken van elke kamer van elke woning onzichtbare camerabeveiliging aan te brengen, maar doet dit slechts steekproefsgewijs, waardoor iedereen het gevoel heeft dat hij constant van alle kanten bekeken kan worden, ook de mensen waar tijdens het bezoek geen camera's bij zijn geplaatst. Aankleden wordt dan een krampachtige beweging, als een omgekeerde striptease. De macht over het private lichaam kan teruggenomen worden door een compleet zwart bodykostuum aan te trekken en daarmee de camera te wijzen op het bewustzijn van diens aanwezigheid: ICU (I see you).

—Privacy in de publieke ruimte (transparantie)—

Stel je de huidige situatie voor als een overheid die zijn burgers zowel heeft uitgekleed als bij voorbaat verdacht gemaakt. Het benauwende kostuum dat zij opgedrongen hebben gekregen is metaforisch een compleet huidskleurig pantykostuum, waardoor het gehele lichaam zichtbaar is, maar het gezicht gemorft als een dief. Om toch nog zelf wat privacy te kunnen waarborgen kan het kostuum zo ontworpen worden dat de burger zelf bepaalde gevoelige stukjes naar wens minder of meer transparant kan maken, al naar gelang de meer afstandelijke of juist intieme band met de persoon die hij voor zich heeft.



*Door: Dr. Huub Dijkstra (Universiteit van Amsterdam/
Wetenschappelijke Raad voor het Regeringsbeleid)*

“Als je niks te verbergen hebt, heb je ook niks te vrezen”

Privacy is een vraagstuk dat in principe iedereen aangaat. Geen mens ontkomt tegenwoordig aan enige vorm van controle van zijn of haar bewegingen. Een willekeurige burger staat in enkele honderden databases opgenomen. Bijna nergens mag de politie zoveel telefoongesprekken afluisteren als in Nederland. Internetbedrijven zijn verplicht de gegevens van ons zoek-gedrag enkele jaren te bewaren. Cameratoezicht neemt een enorme vlucht. De hoofdcommissaris van politie van Amsterdam wil van de hoofdstad een digitale vesting maken. De voormalig minister van Binnenlandse Zaken, Guusje ter Horst, verklaarde plompverloren van de lijn ‘veiligheid boven privacy’ te zijn.

Toch maken veel mensen zich geen zorgen. Hoewel er door experts, toezichthouders en belangenorganisaties bij voortduring wordt gewaarschuwd voor de aantasting van de privacy, blijft grote maatschappelijke onrust vooralsnog uit. “Als je niks te verbergen hebt, heb je ook niks te vrezen” lijkt voor velen het motto te zijn.

Privacy is in de 21e eeuw in rap tempo een toonaangevend issue geworden. In het kader van het aangescherpte veiligheidsbeleid na de aanslagen van 9/11 en de War on Terror, en de toegenomen focus op preventie in de criminaliteitsbestrijding, hebben overheden wereldwijd hun bevoegdheden stevig opgerekt. De maatschappelijke acceptatie en het daarbij behorende discours is steeds welwillender tegenover ingrijpende maatregelen komen te staan. Een identificatieplicht zoals we die nu kennen bijvoorbeeld

onaanvaardbaar.

Technische toepassingen maken het ook steeds beter mogelijk gedrag van burgers vast te leggen, hun bewegingen te volgen, hun identiteit vast te stellen en te anticiperen op hun gedrag. De registratie van dataverkeer bijvoorbeeld en de opmars van de camera in het straatbeeld, staan garant voor een indringend cordon aan maatregelen. Het accent komt daarbij steeds sterker te liggen op technologie die gebruik maakt van de informatie die het lichaam biedt. Het menselijk lichaam gaat steeds meer als een informatiedrager fungeren en wordt door de overheid en de technologie beschouwt als een 'leugendetector'.

De subtiele werking van technologie maakt dat burgers steeds minder besef hebben van de middelen die op hun van toepassing zijn. Wie geconfronteerd zou worden met een lijstje van wat de verschillende overheidsdiensten (en bedrijven) allemaal van burgers weten, zou versteld staan. Maar doordat de verzameling van deze gegevens op afstand plaats vindt en we er zelden mee worden geconfronteerd, voelt een groot deel van de burgers zich (blijkbaar) nog steeds niet aangetast in de persoonlijke integriteit en levenssfeer en blijft massaal verzet uit.

Van verontrusting naar verzet

Dat er desalniettemin reden tot bezorgdheid is, maakt de scriptie *Privacy* is verdacht van Hanneke Wetzer zonneklaar. In een helder, overtuigend, goed geschreven maar ook verontrustend verhaal maakt ze duidelijk dat het privacyvraagstuk inmiddels tot zeer dicht op de huid van het menselijk lichaam is doorgedrongen. Dat toont ze niet alleen aan via woorden, maar juist ook via beelden. Aan de hand van een analyse van het werk van verschillende kunstenaars over privacy laat ze de mogelijkheden en de gevaren zien.

Kunst is in dit geval uitermate geschikt om de relatie tussen technologie, privacy en het lichaam te verbeelden. Meer dan dat, kunst roept op tot reflectie, kritiek en zelfs verzet.

Bijna alle ontwikkelingen die door Hanneke Wetzer worden beschreven, zijn vormen van surveillance die door de staat 'van bovenaf' worden toegepast om burgers te controleren. Deze vorm van surveillance is indringend verbeeld door het panopticum van Jeremy Bentham en door Michel Foucault spreekwoordelijk gemaakt voor het proces van disciplineren: de uiteindelijke incorporatie van de controle door het subject in de eigen geest. We worden onze eigen bewaker.

Wat de Franse filosoof Pierre Rosanvallon in zijn recente boek *Counter-Democracy* (2008) echter laat zien is dat de term surveillance verrassend genoeg oorspronkelijk juist voor precies het omgekeerde stond, namelijk: de controle van de staat door de burger, met als ultieme vorm het parlement. Vanuit dat inzicht is het dus niet gek om te gaan zoeken naar manieren waarop burgers door middel van de technologie de controle op hun eigen bestaan kunnen heroveren.

En dat is precies wat Hanneke Wetzer doet. Zij bespreekt vele kunstprojecten, waaronder ACCESS, Open Biometrics initiative, Physiognomic Scrutinize, Biomapping en de Automeet. Die brengen volgens haar "op een ludieke en toegankelijke manier de implicaties

die -naast de voordelen- ook aan de biometrische systemen en technologieën kleven onder de aandacht.”

Uiteindelijk omarmt ze de projecten Planbperformance, De-surveillance en Shoeveillance, omdat die “zich niet direct op een bewustmakingsproces van de implicaties richten, maar mogelijke oplossingen bieden.”

Die oplossingen zijn hard nodig. Ze is namelijk van mening dat “de overheid en de media zelf de angst voor terrorisme verspreiden en uitvergrooten, waarmee zij in feite zelf de terrorist zijn. Door tegelijkertijd steeds grotere angst voor terrorisme te kweken en de surveillance technieken te verbeteren en uit te breiden, wordt er een steeds grotere voedingsbodem gekweekt voor een totale wereldorde.”

Dat zijn grote woorden. Maar ze signaleert heel scherp dat “het opstellen van risicoprofielen voor niet alleen criminelen maar voor alle burgers die ‘afwijkend gedrag’ vertonen een ‘self fulfilling prophecy’ in de hand werkt.”

Daar wil ze weerstand tegen bieden: “Als huidige intelligente beeldmaker wil ik meehelpen aan de bewustmaking van de angstcultuur als tegenwicht tegen de boodschappen die nu worden uitgezonden om deze angstcultuur juist te behouden. Ik wil een tegenaanval inzetten tegen de terreur van de angst door mensen er bewust van te maken dat de angst voor terreur zwaar overtrokken is en dat de manier van controle door middel van surveillance van tegenwoordig in plaats van de terreur oplost ons als burgers juist inperkt in bewegingsvrijheid.”

De opstand van het lichaam

De oplossingsgerichte kunstprojecten spreken Hanneke Wetzer het meeste aan. Als illustrator richt ze zich daar zelf ook op. Wat opvalt is dat ze de technologie niet met technologie te lijf wil gaan. In plaats daarvan wil ze het menselijk lichaam een centrale rol in het verzet geven.

Daarmee geeft ze een mooie paradox aan van de hedendaagse vraagstukken rond privacy en veiligheid. Technologie maakt steeds meer controle mogelijk in onze samenleving. Steeds meer en steeds betere informatie helpt om het gedrag van mensen te monitoren. Het aangrijpingspunt is het lichaam. Dat laat zich echter niet zonder protest als een soort ‘wachtwoord’ definiëren. Het lichaam kan doen waar het lichaam ook goed in is: bedriegen, voor de gek houden, veinzen, zich vermommen. De technologie wil het lichaam beheersen. Maar het lichaam kan zich als laatste verzetshaard in een ultieme poging trachten zich daaraan te onttrekken door middel van kunstzinnige list en bedrog.

Bijlage

Op de site van GLOW wordt 'Being public' als volgt omschreven: "Belichaming van de publieke omgeving is de stedelijke openbare ruimte als een open ruimte zonder enige toegangsbeperking en als een ruimte waarin open discussie en vrije meningsuiting mogelijk is. Door de voortdurende veranderingen in aanzien en betekenis van de openbare ruimte, zijn de blikken gericht op de kwetsbare individuele banden met geografische locaties en gemeenschappen, op de segmentatie van de openbare ruimte door gecommercialiseerd gebruik en op de ontbrekende schakel tussen de stedelijke planning en de belangen van de burgers. Om een publiek te genereren voor deze kwesties is GLOW 2009 een bron voor collectieve ervaringen en een platform voor gezamenlijke discussie over de huidige en toekomstige kwaliteiten, inclusief hun verantwoordelijkheden en uitdagingen."⁴⁹ Er participeerden twee kunstenaars die zeker het vermelden waard zijn in het kader van deze scriptie, namelijk de al eerder genoemde Rafael Lozano-Hemmer die zijn dynamische lichtproject 'Pulse Park' van het Madison Square Garden in New York verhuisde naar het Stadhuisplein van Eindhoven, en het project ACCESS van Marie Sester in de hal van het station.

De tentoonstelling 'For Security Reasons' in MAMA omschrijft haar thema als volgt: "In het kader van onze nationale veiligheid hebben we de afgelopen jaren (...) kennis kunnen maken met (...) de 'samen tegen terrorisme' campagnes letten we op elkaar (...). Veiligheidsmaatregelen worden door veel mensen als positief en effectief ervaren. Maar, hoe goed ze ook bedoeld zijn, ze beperken onze bewegingsvrijheid. De tentoonstelling For Security Reasons zoekt de balans tussen veiligheid en speelsheid en geeft een kritische kijk op de laatste veiligheidsontwikkelingen."⁵⁰

⁴⁹ GLOW. "Informatie", bezocht op 9 oktober 2009 (internet, http://www.glow eindhoven.nl/glow2009/informatie/pi_informatie.htm)

⁵⁰ Showroom MAMA. "For Security Reasons", bezocht op 9 oktober 2009 (internet, <http://www.showroommama.nl/projects/forssecurityreasons09.cfm>)

Participerende kunstenaars zijn Stylianos Schicho, Jeroen Jongeleen, SpY, Harmen de Hoop, Antoine Schmitt, Desiree Palmen, Fabian Bechtle, Stefan Reuter en Sander Veenhof.

Het Glazen Lichaam legt in haar tentoonstelling de nadruk op de informatiemaatschappij. Jan Staman schrijft in zijn voorwoord: "Technologie dringt steeds dieper door in ons lichaam en ons brein, en toont emotioneel wie we zijn en hoe we zullen worden: ziek, sterk, gevaarlijk, bijzonder, schuldig of ongewenst. Ons lichaam wordt van glas: doorzichtig en vertekend, hard en breekbaar. Dat lichaam is niet meer van onszelf. De informatie die we verkrijgen door geavanceerde technologieën, wordt gedigitaliseerd en op vele plekken vastgelegd. We worden niet alleen transparanter voor onszelf, maar ook voor anderen."⁵¹ Het Glazen Lichaam brengt de zegeningen en de dilemma's van deze technologie via haar programmering tot de aandacht. De programmering omvatte kunst, lezingen en performances van Rafael Redczus met zijn *DNA-Art*, Iris Honderdos met haar installatie *Vluchtelingen*, een *DNA Test CSI* door Rathenau, een *ambient technology demo* van Philips AMI, een *demonstratie Avatar*, *Google* door Rathenau, *Websitionisme* door Frank Kupper, muziek door Dr. Schmitt, een Poetry slam door Krijn Peter Hesselink en Dans door Leine & Roebana.

Relevante kunstenaars op de website www.we-make-money-not-art.com zijn Fernando Orellana en Brendan Burns met *Sleep Walking*, Tuur van Balen met *My City = My Body*, Dislocate met *Ere Be Dragons*, Rafael Lozano Hemmer met *Wavefunction* en *Pulse Room*, Christian Nold met *Biomapping*, Marc Böhlen met *Shoeveillance* en *The Open Biometric Project*, Worm met *Automeet*, Luther Thie en Eyal Fried met *Acclair*, Ami Franceschini, David Lu en Michael Swaine met *Fingerprint Maze 2004*.

⁵¹ Jan Staman, directeur, Rathenau Instituut. Voorwoord. In: Est, Rinje van, Huub Dijkstra, bleem en Christian van 't

Relevante kunstwerken in het digitale archief van V2 zijn *Tangent Fear*, *Tele_Trust*, *Maat Netwerken*, *Biochemical Portrait* en *Paranoid Panopticum* van Karen Lancel en Hermen Maat, *Physiognomic Scrutinizer* van Marnix de Nijs, *Tangent Conspiracy* van de Media Design Groep van het Piet Zwart Instituut, Beat Brogle en Philippe Zimmermann met *Onewordmovie*, Marc Tuters met *CCC: Cartographic Command Centre*, Emanuel Danesch en David Rych met *Utopia Travel*, Eastwood met *Civilization IV*, David Rokeby met *n-cha(n)t*, OnesAndZeros, Axel Heide, Philip Pocock en Gregor Stehle met *UnMovie*, Zhang Ga met *Peoples' Portrait*, Roman Kirschner met *Ohrwurmbeschleuniger*, Christa Sommerer en Laurent Mignonneau met *Mobile Feelings*, Sponge met *Membrane*, Time's Up met *The Bar Bot*, Workspace Unlimited met *DEVMAP*, Joachim Montessuis en Eléonore Hellio met *M.U.S.H.*, Daniel Belasco Rogers met *Planbperformance*, Collectief 0100101110101101.org met *Perpetual Self Dis-Infecting Machine*, Tobias Grewenig met *Bitmirror* en *Emotion's Defibrillator*, en Miguel Andrés-Clavera en Inyong Cho met het *scanMemories Project*.

Literatuur

Vedder, Anton, Leo van der Wees, Bert-Jaap Koops en Paul de Hert, Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw. Den Haag: Rathenau Instituut, 2007; Studie.

Jaap Spaans. Biometrische identificatie: digitaal brandmerk? Amsterdam: Oogstpublicaties, 2002.

Rinie van Est, Huub Dijkstra en Christian van 't Hof, Het Glazen Lichaam: Gegrepen door informatie. Den Haag: Rathenau Instituut, 2008.

TILF - Centrum voor Recht, Technologie en Samenleving. Techniek. Veiligheid en privacy in 2030: twee toekomstscenario's. Universiteit van Tilburg, 2005.

Hans van Driel en Anke Coumans, 'Het onvoorstelbare. De werkelijkheid van beeld.'

Christiaan van 't Hof. Digitalisering van de openbare ruimte. Vrij surfen binnen een groeiende poortjescultuur. Position paper, Rathenau Instituut, 2008, p. 1.

R.L. van Renesse. Biometrische identificatie: alle mensen zijn ongelijk! Nederlands Tijdschrift voor Fotonica, 1998

COSMO Time & Security Systems. Wat is biometrie? Biometrie: whitepaper.

SD, RvdG, WEG! Wouter Bos wil problemen niet oplossen maar afschaffen. Briljant idee. Vrij Nederland 39, 2009, p. 8-9.

Kagie, R. Biometrie en privacy. Vingerportretrecht. Vrij Nederland 39, 2009, p. 24-29.

Kas, A en Heck, W, Vingerafdrukken voor de database. Afstaan biome-

~~trische gegevens voor identiteitsbewijs per vandaag verplicht. NRC Handelsblad, 2009, p. 1,3.~~

~~Jeroen Boomgaard. "Terreur en Kunst", Metropolis M No 2 2005 april/mei, bezocht op 27 november 2009 (internet, http://www.metropolism.org/magazine/2005_no2/terreur-en-kunst/).~~

~~Michel Foucault, "Panopticism", in *Visual Culture: the reader*, ed. Jessica Evans en Stuart Hall, p. 61 t/m 79.~~

~~Gerrit de Wit en Harry Westerink. "Het alziend oog", bezocht op 24 oktober 2009 (internet, <http://www.geblader.te.nl/00735p44.htm>).~~

~~Piet van der Lende. "Een systeem van zichtbaarheid - inspectie, controle en bewaking", bezocht op 23 oktober 2009 (internet, http://www.solidariteit.nl/Documenten/2008/achter_de_voordeur.html).~~

~~Rene ten Bos. "Kijken naar goudvissen", bezocht op 23 oktober 2009 (internet, http://beroepsopleider.web-log.nl/mijn_weblog/files/kijken_naar_goudvissen_rene_ten_bos_derde_vanwoodmanlezing.doc).~~

~~Showroom MAMA. "For Security Reasons", bezocht op 9 oktober 2009 (internet, <http://www.showroommama.nl/projects/forsecurityreasons09.cfm>).~~

~~GLOW. "Informatie", bezocht op 9 oktober 2009 (internet, http://www.gloweindhoven.nl/glow2009/informatie/nl_informatie.html).~~

~~Marie Sester. "ACCESS", bezocht op 10 oktober 2009 (internet, <http://www.sester.net/projects/access/access.html>).~~

~~Marie Sester. "Description and Concept", bezocht op 10 oktober 2009 (internet, <http://www.accessproject.net/concept.html>).~~

~~Marnix de Nijs. "Physiognomic Scrutinizer. 2008/2009", bezocht op 11 oktober 2009 (internet, http://www.marnixdenijs.nl/physiognomic_scrutinizer.htm).~~

~~We make money not art. "Interview of Marc Böhlen", bezocht op 25 oktober 2009 (internet, <http://www.we-make-money-not-art.com/archives/2006/05/interview-of-ma.php>).~~

~~Marc Böhlen. "The Open Biometrics Initiative", bezocht op 21 oktober 2009 (internet, <http://www.realtechsupport.org/pdf/OpenBiometrics.pdf>).~~

~~Daniel Belasco Rogers (mei 2004). "The daily practice of map making", bezocht 25 oktober 2009 (internet, <http://www.planbperformance.net/dan/texts/RadiusEdit.pdf>).~~

~~Christian Nold (2004, januari). "Bio Mapping", bezocht op 25 oktober 2009 (internet, <http://www.biomapping.net>).~~

~~Anna Benthkowska Kafel (2006, augustus). "Christian Nold interviewed by Anna Benthkowska Kafel", bezocht op 25 oktober 2009 (internet, <http://www.biomapping.net/interview.htm>).~~

~~V2. "Archive", bezocht op 1 november 2009 (internet, http://www.v2.nl/archive/articles/songmuller_growenig_kirschner_shulgin_0100).~~

~~0100101110101101.org. "Contagious Paranoia", bezocht op 1 november 2009 (internet, http://www.0100101110101101.org/home/bien-nale_py/index.html).~~

~~Antenne Rotterdam. "Onthulling van een biometrische bar", bezocht op 25 november 2009 (internet, http://www.antennerotterdam.nl/read/antenne_item/id/99660?tmpl=antenne_print.html).~~

~~—SNDRV. “De surveillance”, bezocht op 25 november 2009 (internet, <http://www.sndrv.nl/de-surveillance/>)—~~

~~—Alexander Lehmann, “Du bist terrorist”, bezocht op 26 november 2009 (internet, <http://www.youtube.com/watch?v=SGD2q2vewzQ>)—~~

~~—Computable/Computeridee (2006, april), “Nederlands paspoort krijgt vanaf augustus chip”, bezocht op 19 oktober 2009 (internet, http://www.computable.nl/artikel/ict_topies/overheid/1274578/1277202/nederlands-paspoort-krijgt-vanaf-augustus-chip.html)—~~

~~—SAROAD, “Wat is biometric?”, bezocht op 9 oktober 2009 (internet, <http://www.sa-road.com/nl/biometric.php>)—~~

~~—Security Database B.V., “Identity at your fingertips”, bezocht op 9 oktober 2009 (internet, <http://www.fingerident.com/fingerident.pdf>)—~~

~~—ID-nee, “Geen vingerafdruk van onschuldige burgers in politie en justitie registers gewenst”, bezocht op 10 oktober 2009 (internet, http://www.id-nee.nl/01-1%20Actueel%20hoofdttekst_bestanden/FOLDERvingerafdruk%2011-10-08.pdf)—~~

~~—Dirk Vlasblom (2008, februari), “Ga gerust mijn gangen na”, bezocht op 10 oktober 2009 (internet, http://www.nrc.nl/nieuwsthema/privacy/article1856854.ece/Ga_gerust_mijn_gangen_na)—~~

“Technologie bedreigt steeds meer onze privacy en dringt diep onze leefwereld binnen. Hanneke Wetzer laat zien dat daar een laatste obstakel wacht: het menselijk lichaam zelf.”

Huub Dijkstra

Huub Dijkstra is filosoof en verbonden aan de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).