

Facebook als digitaal Panopticon

Over surveillance binnen online social networks

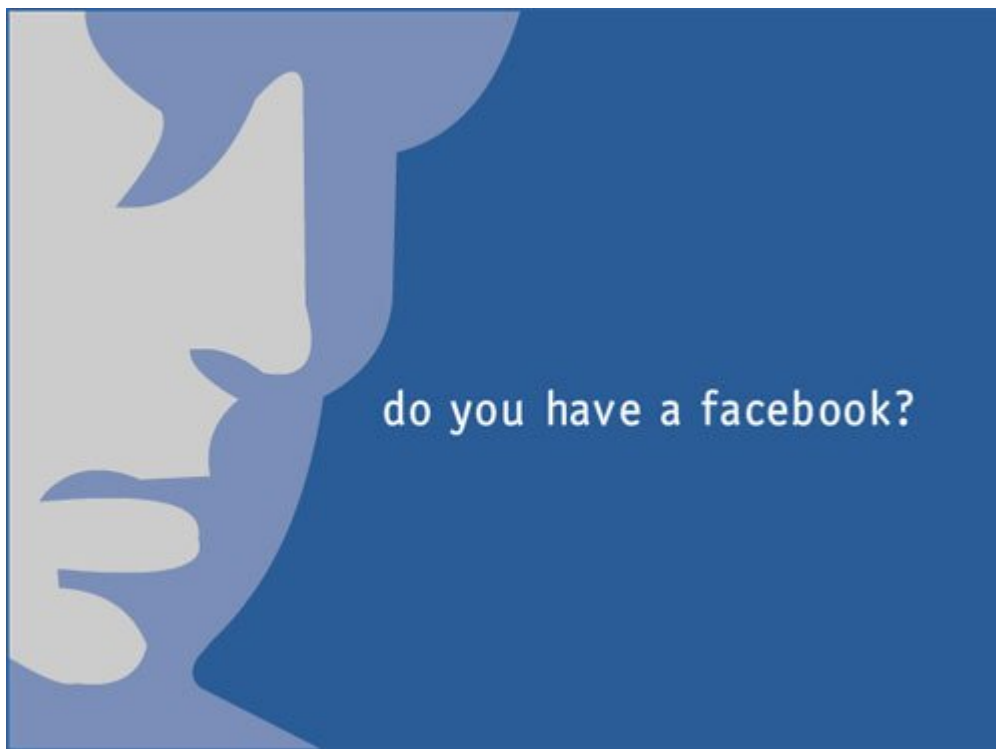


Image: libizblog.wordpress.com

Annewil Neervens

Studentnr.: 5816181

Analyse en Methode Nieuwe Media 2

Media en Cultuur, Universiteit van Amsterdam

Docent: Reinder Rustema

Werkgroep: M426

Datum: 6 juni 2008

Inhoudsopgave

Abstract en sleutelwoorden	blz. 3
1. Introductie	blz. 3
2. Theoretisch kader	blz. 5
2.1 Surveillance en het Panopticon	blz. 5
2.2 The New Surveillance	blz. 6
2.3 Participatory Surveillance	blz. 7
2.4 Een huidig Digitaal Panopticon	blz. 8
3. Analyse	blz. 9
3.1 Facebook	blz. 9
3.2 Peer-to-Peer Surveillance	blz. 11
4. Reflectie	blz. 13
5. Conclusie	blz. 14
Bronnenlijst	blz. 16

Abstract

In dit paper wordt onderzocht hoe en in welke mate surveillance is veranderd, sinds Foucault er in *Discipline and Punish* over schreef. Het idee van een eventueel huidig digitaal Panopticon wordt verondersteld en er wordt gekeken hoe dit zich verhoudt tot de social networking site Facebook.

Sleutelwoorden: Facebook, participatory surveillance, peer-to-peer surveillance, persoonlijke informatie, Panopticon.

1. Introductie

Wie een profiel aanmaakt op een social networking site zal een aantal persoonlijke gegevens moeten achterlaten. Vaak wordt gevraagd om de naam, leeftijd, sekse en woonplaats van de gebruiker in kwestie. Ook heeft hij de gelegenheid om meer informatie over zichzelf openbaar te maken, zoals bijvoorbeeld relatiestatus en opleiding.

Ook in het privacybeleid van de netwerksite Facebook is te lezen: ‘wanneer je je aanmeldt bij Facebook, geef je ons bepaalde persoonlijke informatie, zoals je naam, je emailadres, je telefoonnummer, je adres, je geslacht, waar je naar school bent gegaan en alle andere persoonlijke informatie en voorkeuren die je opgeeft.’¹

De Deense onderzoeker Anders Albrechtslund schrijft in een onderzoek naar participatory surveillance binnen online social networking, het volgende over de informatie die gebruikers moeten afstaan:

“Most social networking sites ask their users to provide these sorts of details; in part this information appears in casual digital conversations within given social networking communication platforms. Consequently, the needed information to profile people is not something hidden that must be uncovered or retrieved using exotic technologies, human agents or advanced bugging equipment. People themselves are publishing this

¹ <<http://www.facebook.com/policy.php>> Laatste bekeken: 6 juni 2008.

information in question, free for all to see and collect. Of course, this makes online social networking appear as a ‘snoop’s dream.’”²

Maar ondanks deze ‘snoop’s dream’ lijken gebruikers massaal een profiel aan te maken bij social networking sites – Facebook zit inmiddels op 60 miljoen leden, MySpace op 300 miljoen leden en Hyves op 5 miljoen leden³ - terwijl uit onderzoek blijkt dat veel mensen online juist zo weinig mogelijk persoonlijke informatie willen bloot geven.⁴

Professor dr. Jos de Mul en dr. Y.H. van der Ploeg schrijven in een onderzoeksprogramma over internet en privacy over deze merkwaardige tegenstelling:

“Ten aanzien van privacyvraagstukken in verband met elektronische netwerken doet zich een merkwaardige paradox voor. Enerzijds wordt het ‘privacy vraagstuk’ van het prille begin van de ontwikkeling van elektronische netwerken beschouwd als een urgent ethisch vraagstuk, terwijl anderzijds de burger zich blijkens zijn gedrag en uitlatingen steeds minder gelegen laat liggen aan de groeiende inbreuk die er op diens privacy zou worden gedaan.”⁵

In dit paper wil ik de redenen onderzoeken voor deze ogenschijnlijke paradox die plaats heeft binnen online social networks, in de context van privacy en surveillance. Daarbij wil ik ook een parallel trekken met een eventueel huidig digitaal Panopticon, zoals we dat in online communities kunnen aantreffen. Bovendien wil ik de vragen onderzoeken of gebruikers van social networking sites wellicht een (participatory) surveillance fetish hebben of dat ze met zachte hand gedwongen deze persoonlijke informatie bekend te maken. Want: als er online geen informatie over je te vinden is, ‘besta’ je dan nog wel?

² Albrechtslund, Anders. Online Social Networking as Participatory Surveillance. *First Monday*, Volume 13, Number 3, 2008.

³ Hubers, Jordy. ‘Online netwerken beleven een groeispurt’ Gepubliceerd op: <http://www.elsevier.nl/nieuws/internet_en_gadgets/artikel/asp/artnr/199613/index.html> Laatst bekeken: 6 juni 2008.

⁴ Hoffman, D.L., T.P. Novak, M.A. Peralta. Building Consumer Trust Online. *Communications of the ACM*, Vol. 42, Number 4, April, 80-85, 1999.

⁵ Van der Ploeg, Y.H., J. De Mul. *Internet & Privacy; een inventarisatie van normatieve aspecten van toezicht op internetgebruik in de organisatie*. 2001. Gepubliceerd op: <[http://www.publicinnovation.nl/downloads/Ploeg%20vd%20en%20J%20de%20Mul%20\(2001\)%20Internet%20en%20privacy%20IOB.pdf](http://www.publicinnovation.nl/downloads/Ploeg%20vd%20en%20J%20de%20Mul%20(2001)%20Internet%20en%20privacy%20IOB.pdf)> Laatst bekeken: 6 juni 2008.

2. Theoretisch kader

2.1 Surveillance en het Panopticon

De Franse filosoof Michel Foucault borduurt in het boek *Discipline and Punish: The Birth of the Prison* voort op Jeremy Bentham's idee van het Panopticon. Een perfect cirkelvormige gevangenis, met in het midden een grote toren van waaruit de bewakers de gevangenen in de gaten kunnen houden. Foucault stelt dat dit een ultieme vorm van surveillance en zelfdisciplinerende bewerkstelligt, doordat de gevangenen niet weten wanneer ze in de gaten gehouden worden. Op die manier zijn ze zich te allen tijden bewust van hun eigen gedrag en houden ze zichzelf in toom.

Het Panopticon is voor Foucault een metafoor voor de moderne maatschappij, waarin de burger voortdurend door zijn omgeving bekeken wordt en zich daarom automatisch aanpast aan wat 'normaal' is. Alles wordt zichtbaar en het individu lijkt een slachtoffer te worden van een alles doordringende transparantie.

Het idee van een Panopticon, en de surveillance daarbinnen - waarbij gevangen vast zitten in de gaten gehouden worden - is breder te trekken als we kijken hoe gebruikers van online social networks gesurveilleerd worden. Deze vergelijking wordt goed duidelijk als Foucault het heeft over de manier waarop registratie werkt:

“This surveillance is based on the system of permanent registration: reports from the syndics to the intendants, from the intendants to the magistrate or mayor. At the beginning of the 'lock up', the role of each of the inhabitants present in the town is laid down, one by one; this document bears 'the name, age, sex of everyone, notwithstanding his condition': a copy is sent to the intendant of the quarter, another to the office of the town, another to enable the syndic to make his daily roll call.”⁶

Foucault beschrijft in deze paragraaf de manier waarop medewerkers van de gevangenis de gevangenen controleren en vastleggen of registreren aan de hand van persoonlijke gegevens en de manier waarop die informatie wordt doorgespeeld naar andere medewerkers, zodat ook zij op de hoogte zijn van de gevangenen.

⁶ Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Vintage, 1979. Translation Alan Sheridan. p.135-228.

Ook binnen online social networks is er sprake van het registreren en doorspelen van persoonlijke informatie. Dit zal ik later nader toe lichten aan de hand van een analyse van de netwerksite Facebook.

2.2 The New Surveillance

Wat is er sinds Foucault veranderd aan surveillance? Hoe ziet het tegenwoordige surveillance eruit in de context van de digitalisering?

M.I.T. professor Gary T. Marx schrijft in het artikel *What's New about the 'New Surveillance'? Classifying for Change and Continuity* over de betekenis van new surveillance. Hij geeft hierin aan dat tegenwoordige surveillance voor een groot gedeelte kijkt naar de kaders en patronen van relaties, zoals in onderstaand fragment is te lezen.

“A better definition of the new surveillance is the use of technical means to extract or create personal data. This may be taken from individuals or contexts. In this definition the use of ‘technical means’ to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. Many of the examples extend the senses by using material artifacts or software of some kind, but the technical means for rooting out can also be deception, as with informers and undercover police. The use of ‘context’ along with ‘individuals’ recognizes that much modern surveillance also looks at settings and patterns of relationships. Meaning may reside in cross classifying discrete sources of data (as with computer matching and profiling) that in and of themselves are not of revealing. Systems as well as persons are of interest.”⁷

Marx legt bij new surveillance vooral de nadruk op moderne (digitale) technologieën, zoals camera's, email en databases. Om aan te geven hoe new surveillance wordt gebruikt in het alledaagse leven geeft hij voorbeelden van ouders die hun kinderen in de crèche in de gaten houden via een webcast, en een verborgen camera in een pinautomaat. Het zijn de kleine, alledaagse vormen van surveillance die inmiddels volledig zijn geïntegreerd in ons leven.

⁷ Marx, G. T. What's New About the New Surveillance? Classifying for Change and Continuity. *Surveillance and Society* Vol. 1 (1), 2002.

2.3 Participatory Surveillance

Volgens Albrechtslund wordt (online) surveillance vaak als negatief ervaren en het liefst zoveel mogelijk vermeden. Het probleem hierbij is volgens hem echter, dat het lijkt of er geen adequate beschrijving gegeven kan worden van de eigenlijke ‘practice’ van online social networking.

In dat licht komt hij met de term ‘participatory surveillance’, dat bestaat uit twee aspecten. Het eerste aspect is het idee van ‘user empowerment and the building of subjectivity’. Het tweede aspect is ‘the understanding of online social networking as a sharing practice instead of an information trade’.⁸ Albrechtslund schrijft hierover verder:

“The practice of online social networking can be seen as empowering, as it is a way to voluntarily engage with other people and construct identities, and it can thus be described as participatory.”⁹

Ook Bart Simon ziet in zijn artikel *The Return of Panopticism: Supervision, Subjection and the New Surveillance*¹⁰ het belang van individueel, menselijk handelen. Hij stelt dat hoe meer er in surveillance studies de nadruk wordt gelegd op de technieken van supervisie, des te minder de ‘individual agency’ wordt geanalyseerd.

Albrechtslund lijkt met deze conclusie echter te negeren dat het meegaan in online social networks ook andersom kan werken. Dat het niet altijd ‘empowering’ is. En dat het zelfs niet altijd zo vrijwillig is als hij stelt. Hij vergeet namelijk dat sommige gebruikers wellicht een bepaalde *sociale druk* voelen om mee te doen en niet achter te blijven. Later in dit paper komen hier een aantal voorbeelden van terug in een analyse van Marx.

Ook zijn er bij deze conclusie van Albrechtslund verschillende vragen te stellen. Heeft de gebruiker bijvoorbeeld (last van) een participatory fetish? Vind hij het prettig om in de gaten te worden gehouden? Of wordt hij juist met zachte hand gedwongen om informatie over

⁸ Albrechtslund, Anders. Online Social Networking as Participatory Surveillance. *First Monday*, Volume 13, Number 3, 2008.

⁹ Albrechtslund, Anders. Online Social Networking as Participatory Surveillance. *First Monday*, Volume 13, Number 3, 2008.

¹⁰ Simon, Bart. The Return of Panopticism: Supervision, Subjection and the New Surveillance. *Surveillance & Society*, 3(1), 1-20, 2005.

zichzelf online te zetten. Want: ‘bestaat’ hij nog wel als er geen informatie online over hem te vinden is?

Mark Poster schreef immers al ‘we are now being convinced that ‘information’ is a first commodity.’¹¹ Wordt (persoonlijke) informatie steeds meer vermaakt tot een product? En moeten wij als producenten van die informatie zorgen dat dit product te allen tijden voorhanden is? Is dat immers niet wat een goede producent hoort te doen? Het verworden van persoonlijke gegevens tot ‘verhandelbaar’ product zou wellicht één van de redenen kunnen zijn dat gebruikers toch besluiten deze informatie te publiceren. Als persoonlijke informatie een product wordt, kun je er misschien meer afstand van doen. Waardoor persoonlijke informatie, helemaal niet meer zo persoonlijk is.

2.4 Een huidig Digitaal Panopticon

Het is interessant te bedenken hoe de klassieke surveillance theorie en het Panopticon-model zich verhouden tot de laatste digitale ontwikkelingen. Als het idee van het Panopticon is toe te passen op online communities, dan zouden we dus kunnen spreken van een huidig digitaal Panopticon.

Marx schetst in zijn artikel *A tack in the Shoe: Neutralizing and Resisting the New Surveillance*¹² in grote lijnen het verschil tussen de gesurveilleerde die zijn privacy zoveel mogelijk probeert te beschermen, en de surveillant die deze grenzen juist zoveel mogelijk probeert op te rekken en te doorbreken. Wederom stuiten we hierbij op het paradoxale punt. Waarom geven gebruikers die zich zoveel mogelijk proberen te verzetten tegen surveillance toch zoveel van zichzelf bloot?

Volgens Marx heeft dit onder andere te maken met het idee dat er voordelen te behalen zijn in het geven van dit soort informatie én de angst om er niet in mee te gaan en daardoor bepaalde dingen mis te lopen of te verliezen:

“One noteworthy aspect is the extent to which individuals go along with requests for personal information. This is likely related to beliefs about the advantages of, and need

¹¹ Poster, Mark. *Foucault and Databases*. The Mode of information. Chicago: UCP, 1990, p. 69-98.

¹² Marx, G.T. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, Vol. 59 (2), 2003.

for, providing such information, and trust in authority - factors which often override the ambivalence resulting from traditional privacy and autonomy concerns. Moreover, a lack of resistance to intrusive surveillance may mask as acceptance because of a fear of being sanctioned or losing one's job, position or privilege, or as a necessary condition for something desired such as employment, credit, apartment or car rental, air travel or government benefits. There may also be fatalism and resignation, believing it is impossible to resist.”

Maar er zijn volgens hem ook andere redenen te bedenken:

“Many cultural beliefs support the legitimacy of surveillance. Consider statements I heard such as, ‘I have nothing to hide’, ‘it’s for my own good’, ‘I support the goals’, ‘I’m getting paid’, ‘it’s just the way they do things here’, ‘they have to do it to ...[stay competitive, obtain insurance, stop crime, avoid risks]’, ‘the measure is valid’, and ‘they promise to protect confidentiality’. Lack of awareness of the extent and nature of surveillance, or of the potential for abuse and misuse of personal information, may also support acquiescence.”

Deze redenen voor het verstrekken van bepaalde persoonlijke informatie online zijn te beschouwen als de zelfdisciplinerende van de gevangenen binnen het huidige digitale Panopticon. Wie er niet in meegaat, maakt van zichzelf een uitzondering – waar ‘I have nothing to hide’, ‘I have something to hide’ wordt. Bovendien wordt er, zoals Marx ook aangeeft, groot vertrouwen gelegd in de autoriteiten die onze informatie bewaken. Veel mensen staan niet stil bij het feit dat er misbruik gemaakt kan worden van hun informatie.

3. Analyse

3.1 Facebook

In het kader van surveillance is Facebook een boeiende casestudy. Niet alleen omdat er wordt getwijfeld aan de vrijheid die een gebruiker heeft binnen het netwerk en de manier waarop met privacygevoelige informatie wordt omgegaan.¹³ Maar ook omdat Facebook met Facebook

¹³ Hodgkinson, Tom. ‘*With friends like these...*’ Gepubliceerd op: <<http://www.guardian.co.uk/technology/2008/jan/14/facebook>> Laatst bekeken: 6 juni 2008.

Beacon¹⁴ een functie introduceerde, waarmee precies te zien is welke handelingen andere gebruikers doorvoeren op hun pagina. Zo kan een gebruiker precies zien wie van zijn vrienden een bepaald product toe heeft gevoegd aan een verlanglijstje, welke quiz hij net heeft gemaakt, welke diensten hij installeert op zijn account en met wie hij online vrienden is geworden.

Er werd door gebruikers en media volop geprotesteerd op deze privacyinbreuk en in december 2007 plaatste oprichter Mark Zuckerberg op the Facebook Blog¹⁵ een verontschuldigend bericht voor de 'bad job' die ze hebben gedaan bij de release van de tool.

Niettemin maakt Facebook Beacon nog steeds prominent onderdeel uit van de netwerksite en staat automatisch aan als een nieuwe gebruiker zich registreert. Het is mogelijk de functie uit te schakelen; daarvoor moet de gebruiker handmatig in zijn privacy settings aangeven dat hij niet wil dat websites informatie naar zijn profiel sturen. Informatie wordt nu niet meer gepubliceerd, maar Facebook ontvangt het nog wel. Het is onmogelijk na te gaan of zij deze informatie niet op slaan en gebruiken - zoals ze claimen.

Zoals eerder vermeldt is Foucault's notie van 'lock up' in zekere zin terug te vinden binnen online social networks, waarbij persoonlijke informatie van een gebruiker vast wordt gelegd in een profiel. Het doorspelen van deze informatie kan in het licht van deze profielensites op twee manieren worden gezien. Alles dat een gebruiker online publiceert is bekend bij andere gebruikers die zijn profiel kunnen bekijken. Ook de beheerders van de website kunnen alle informatie zien. Op deze manier circuleert en verspreidt informatie zich dus binnen een online community.

Daarnaast komt het regelmatig voor dat netwerksites informatie doorspelen naar derden, bijvoorbeeld adverteerders of marketingbedrijven. Zo is in het privacybeleid van Facebook dat advertenties die op Facebook verschijnen soms direct door externe adverteerders aan gebruikers worden geleverd.¹⁶ Facebook vermeldt er wel bij dat externe adverteerders geen toegang hebben tot contactinformatie die is opgeslagen, tenzij de gebruiker ervoor kiest om deze met hen te delen.

¹⁴ <<http://www.facebook.com/business/?beacon>> Laatst bekeken: 5 juni 2008.

¹⁵ Zuckerberg, Mark. 'Thoughts on Beacon' Gepubliceerd op: <<http://blog.facebook.com/blog.php?post=7584397130>> Laatst bekeken: 5 juni 2008.

¹⁶ <<http://www.facebook.com/policy.php>> Laatste bekeken: 6 juni 2008.

Het doorspelen van dit soort informatie voor commerciële doeleinden neemt soms heftige vormen aan. Zo maken veel social networking sites niet alleen gebruik van ‘contextual ads’ die getriggerd worden door sleutelwoorden op de pagina, maar inmiddels ook van ‘contextual visual targeting technology’ dat foto’s of plaatjes bij sleutelwoorden zoekt.¹⁷

Bovendien is er bij Facebook een tweede, letterlijk aspect van ‘lock up’ te bespeuren, daar waar de gebruiker zijn account niet kan verwijderen, alleen deactiveren.¹⁸

Albrechtslund trekt in zijn artikel een parallel tussen ‘true friendship that lasts forever’ en online social networking, waarbij hij aangeeft dat de ‘digitale paden van een online vriendschap *echt* voor altijd zijn, aangezien ze voor eeuwig worden opgeslagen op servers.¹⁹ In het geval van Facebook kan informatie wel van een profiel worden verwijderd, maar de account zelf niet. Waardoor er in theorie altijd informatie over de gebruiker is terug te vinden op de servers van Facebook.

Verschillende onderdelen van de eerder beschreven (klassieke) teksten zijn toepasbaar op de huidige digitale ontwikkelingen en online social networks. Surveillance blijft ook - of misschien wel *vooral* digitaal – aanwezig.

3. 2 Peer-to-Peer Surveillance

Peer-to-peer interactie wordt vaak neergezet als een alternatief voor de traditionele one-to-many broadcast modellen.²⁰ Ook wat betreft surveillance lijkt het accent te verschuiven van one-to-many naar many-to-many. Waarbij één autoritaire surveillant (zoals bijvoorbeeld de overheid) plaatsmaakt voor meerdere gefragmenteerde surveillanten, die los van elkaar staan. Deze surveillanten zijn te beschouwen als de gebruikers die online anderen in de gaten houden; het zogenaamde peer-to-peer surveillance. Journalist James Harkin legt dit fenomeen in the Guardian²¹ als volgt uit:

¹⁷ <<http://www.techcrunch.com/2008/06/01/likecoms-creepy-facebook-ads/>> Laatst bekeken: 5 juni 2008.

¹⁸ <<http://www.facebook.com/policy.php>> Laatste bekeken: 6 juni 2008.

¹⁹ Albrechtslund, Anders. Online Social Networking as Participatory Surveillance. *First Monday*, Volume 13, Number 3, 2008.

²⁰ Bruns, Axel. *From Blogs to Open News: Notes towards a Taxonomy of P2P Publication*. In Proceedings of the Australia and New Zealand Communication Association Conference (ANZCA03): Designing Communication for Diversity, Brisbane, Australia, 2003.

²¹ Harkin, James. ‘Peer-to-peer surveillance’ Gepubliceerd op: <<http://www.guardian.co.uk/commentisfree/story/0,,1868319,00.html>> Laatst bekeken: 5 juni 2008.

“The emerging idea that the constant operation of a whole range of digital devices will increasingly be used as evidence against us by parties other than the state.”

Harkin ziet peer-to-peer surveillance hier als een negatieve ontwikkeling waarbij ‘bewijs tegen ons gebruikt zal worden’. Bovendien moeten we nu meer surveillanten dan alleen de overheid moeten vrezen. Toch hoeft peer-to-peer surveillance niet per definitie als negatief te worden opgevat.

Gekoppeld aan een profielensite als Facebook zou peer-to-peer surveillance gezien kunnen worden als het tweede aspect uit de notie van participatory surveillance, namelijk: ‘the understanding of online social networking as a sharing practice instead of an information trade’. De nadruk ligt hierbij op de keuze van de gebruiker. Hij *kies*t ervoor om een profiel aan te maken en informatie met anderen te delen: het is een sharing practice.

Peer-to-peer surveillance lijkt toe te nemen. Eén van de redenen daarvoor is dat gebruikers door de ontwikkeling van een ‘open web’ en Web 2.0 sites zelf actief bij kunnen dragen aan content op het internet.

Participatory surveillance kan bij Facebook gezien worden als een *handeling*. Een motivatie achter het ‘waarom’ van de gebruikers. Het kan daarmee ook een reden aangeven voor de gebruiker om een account aan te maken. ‘Empowerment’ is daarbij een belangrijk aspect; de gebruiker krijgt meer invloed over zijn eigen persoonlijke gegevens en wat hij daarmee doet. Hij kan er voor dus zelf voor kiezen dit online te publiceren, of om dat niet te doen.

Peer-to-peer surveillance zou in dit kader gezien kunnen worden als de *manifestatie* of uiting van de nieuwe surveillance-vorm die online social networking sites – en Web 2.0 sites in het algemeen – bewerkstelligt. De gebruiker krijgt de mogelijkheid (en daarmee misschien zelfs wel de macht) om surveillance uit te oefenen.

4. Reflectie

In het theoretisch kader en de analyse heb ik getracht uit te werken waar de (klassieke) teksten over de surveillance theorie op toegespitst zijn en hoe deze zich verhouden naar nieuwe media – en in het bijzonder Facebook.

Als we ervan uitgaan dat het klassieke idee van een Panopticon ook terug te vinden is in onze huidige samenleving, kunnen we al snel uitkomen bij een digitaal Panopticon. Een plek waar surveillance is versleuteld in binaire code. Maar wie zijn in dit Panopticon de bewakers en de gevangenen? En hoe wordt er precies invloed uitgeoefend? Hoe ziet dit Panopticon eruit?

In het huidige digitale Panopticon zijn de gevangenen te beschouwen als de gebruikers van Facebook, degenen die hun persoonlijke informatie vastleggen in een profiel.

De bewakers zijn de beheerders van de site, die toegang hebben tot alle informatie. Zelfs de informatie die is opgeslagen in privé-profielen. Daarnaast zou je kunnen beargumenteren dat ook de mede-gebruikers - de mensen die je profiel kunnen bekijken - een surveillance functie hebben, doormiddel van peer-to-peer surveillance.

Zelfdisciplineren van de gebruikers wordt bereikt door het toepassen van Foucault's idee van 'the visible' en 'the unverifiable.'²² Waarbij 'the visible' staat voor de vrienden die hij steeds online ziet (komen) en 'the unverifiable' voor het idee dat hij niet weet welke vrienden of andere personen zijn profiel bekijken. Op die manier vindt er een vorm van conditionering plaats.

Aan de hand van de termen participatory surveillance (als handeling) en peer-to-peer surveillance (als manifestatie) kan er gekeken worden of de klassieke betekenis van surveillance een extra 'laag' heeft gekregen, waarbij er niet meer één autoritaire surveillant is, maar er nu meerderen zijn; in de vorm van de sitebeheerder én andere gebruikers die je profiel kunnen bekijken (of dat nu je online vrienden zijn, of zogenaamde 'lurkers'²³, die alleen webpagina's of profielen bekijken en er verder niets aan bijdragen).

²² Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York. Vintage, 1979. Translation Alan Sheridan. p.135-228.

²³ Nielsen, Jakob. 'Participation Inequality: Encouraging more Users to Contribute'. Gepubliceerd op: <http://www.useit.com/alertbox/participation_inequality.html> Laatst bekeken: 6 juni 2008.

5. Conclusie

In dit paper heb ik de ogenschijnlijke paradox onderzocht die plaats heeft binnen online social networks, in de context van privacy en surveillance. Waarbij gebruikers liever geen persoonlijke informatie over zichzelf op het internet plaatsen, maar dit wel doen. Ik heb geprobeerd uit te vinden wat de reden is voor deze tegenstelling en *waarom* zij er toch voor kiezen om een online profiel aan te maken.

Aan de hand van het theoretisch onderzoek blijkt dat hier verschillende, uiteenlopende redenen voor zijn. Zo schrijft Albrechtslund dat surveillance vaak in een negatief daglicht wordt gesteld, terwijl we ook naar participatory surveillance kunnen kijken als een handeling die een gebruiker op vrijwillige basis aangaat. Waarbij het belangrijk is te bedenken dat hij dus een keuze heeft.

Marx laat zien dat veel gebruikers aan de ene kant denken voordelen te kunnen behalen aan het plaatsen van persoonlijke gegevens op het net, en aan de andere kant bang zijn te worden benadeeld als ze dit niet doen.

Bovenstaande redeneringen zouden dus een antwoord kunnen zijn op de vraag waarom mensen ogenschijnlijk tegenstrijdig handelen. Maar er zijn ook andere redenen te bedenken. Om dit uit te zoeken is nader onderzoek nodig.

In mijn introductie stelde ik dat ik de vragen wil onderzoeken of gebruikers van social networking sites wellicht een (participatory) surveillance fetish hebben, of dat ze met zachte hand gedwongen deze persoonlijke informatie bekend te maken. Want: als er online geen informatie over je te vinden is, 'besta' je dan nog wel?

Aan de hand van mijn literatuurstudie ben ik tot de conclusie gekomen dat het mogelijk is dat gebruikers van online social networks te maken hebben met een (participatory) surveillance fetish, waarbij ze het prettig vinden om in de gaten gehouden te worden. Dit 'in de gaten gehouden worden' hoeft niet zo negatief te zijn als het klinkt. Wellicht is het egostrelend om te weten dat veel mensen je profiel bezoeken omdat ze geïnteresseerd zijn in wie je bent (om welke reden dan ook).

Het vermaken van informatie tot een 'first commodity', zoals Poster schrijft, is iets waar we in onze huidige maatschappij waarschijnlijk steeds meer rekening mee moeten houden. Het lijkt erop dat er inderdaad steeds onverschilliger met persoonlijke informatie

wordt omgegaan. Of wellicht was dit altijd het geval, maar wordt het door de komst van digitalisering beter zichtbaar.

Ook heb ik geprobeerd een beeld van een huidig digitaal Panopticon te schetsen, zoals we die in online communities als Facebook kunnen aantreffen. Dit beeld heb ik geprobeerd te concretiseren door de vragen uit de klassieke tekst van Foucault – wie zijn de gevangen en de bewakers? – te beantwoorden voor het digitale Panopticon. Facebook is met het oog op surveillance een goed studieobject, omdat Foucault's klassieke notie van het Panopticon duidelijk is toe te passen op de digitale netwerksite.

Tot slot ben ik in de veronderstelling dat surveillance een extra 'laag' heeft gekregen door peer-to-peer surveillance, waarbij we nu ook de allesdoordringende blik van de 'gewone man' in ons achterhoofd moeten houden. Verder onderzoek zou kunnen uitwijzen in hoeverre peer-to-peer surveillance een rol speelt binnen online social networks en wat voor invloed het heeft op de gebruiker.

Bronnenlijst

Literatuur

Albrechtslund, Anders. Online Social Networking as Participatory Surveillance.
First Monday, Volume 13, Number 3, 2008.

Bruns, Axel. *From Blogs to Open News: Notes towards a Taxonomy of P2P Publications*. In
Proceedings of the Australia and New Zealand Communication Association
Conference (ANZCA03): Designing Communication for Diversity, Brisbane,
Australia, 2003.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Vintage, 1979.
Translation Alan Sheridan. p.135-228.

Hoffman, D.L., T.P. Novak, M.A. Peralta. Building Consumer Trust Online.
Communications of the ACM, Vol. 42, Number 4, p. 80-85, 1999.

Marx, G. T. What's New About the New Surveillance? Classifying for Change and
Continuity. *Surveillance and Society* Vol. 1 (1), 2002.

--- A Tack in the Shoe: Neutralizing and Resisting the New Surveillance.
Journal of Social Issues Vol. 59 (2), 2003.

Poster, Mark. *Foucault and Databases*. The Mode of information. Chicago: UCP,
p. 69-98, 1990.

Simon, Bart. The Return of Panopticism: Supervision, Subjection and the New Surveillance.
Surveillance & Society, 3(1), 1-20, 2005.

Overige media

Harkin, James. '*Peer-to-peer surveillance*' Gepubliceerd op:

<<http://www.guardian.co.uk/commentisfree/story/0,,1868319,00.html>>

Laatst bekeken: 6 juni 2008.

Hodgkinson, Tom. '*With friends like these...*' Gepubliceerd op:

<<http://www.guardian.co.uk/technology/2008/jan/14/facebook>>

Laatst bekeken: 6 juni 2008.

Hubers, Jordy. '*Online netwerken beleven een groeisput*' Gepubliceerd op:

<http://www.elsevier.nl/nieuws/internet_en_gadgets/artikel/asp/artnr/199613/index.html> Laatst bekeken: 6 juni 2008.

Nielsen, Jakob. '*Participation Inequality: Encouraging more Users to Contribute*'

Gepubliceerd op: <http://www.useit.com/alertbox/participation_inequality.html>

Laatst bekeken: 6 juni 2008.

Schonfeld, Erick. '*Like.com's Creepy, But Effective, Facebook Ads*' Gepubliceerd op:

<<http://www.techcrunch.com/2008/06/01/likecoms-creepy-facebook-ads>>

Laatst bekeken: 6 juni 2008.

Van der Ploeg, Y.H., J. De Mul. *Internet & Privacy; een inventarisatie van normatieve aspecten van toezicht op internetgebruik in de organisatie*. 2001.

<[http://www.publicinnovation.nl/downloads/Ploeg%20vd%20en%20J%20de%20Mul%20\(2001\)%20Internet%20en%20privacy%20IOB.pdf](http://www.publicinnovation.nl/downloads/Ploeg%20vd%20en%20J%20de%20Mul%20(2001)%20Internet%20en%20privacy%20IOB.pdf)>

Laatst bekeken: 6 juni 2008.

Zuckerberg, Mark. '*Thoughts on Beacon*' Gepubliceerd op:

<<http://blog.facebook.com/blog.php?post=7584397130>>

Laatst bekeken: 5 juni 2008.

Websites

www.facebook.com