

Checking in & Creeping out?

Een discoursanalyse naar locatiegebaseerde diensten en privacy

Masterscriptie Nieuwe Media & Digitale Cultuur
Faculteit Geesteswetenschappen Universiteit Utrecht
Naam: Jenneffer Schepers
Studentnummer: 3298949
Begeleider: Dr. Imar de Vries
Tweede lezer: Dr. Michiel de Lange
Datum: 17 april

Samenvatting

Aan de hand van een kritische discoursanalyse volgens de principes van Norman Fairclough (o.a.1992), wordt in dit onderzoek onderzocht hoe er op technologieblog *Wired* invulling wordt gegeven aan institutionele en sociale locational privacy (Frith, 2012). Middels een analyse van twee blogartikelen op het vlak van institutionele en sociale locational privacy zal er naast een kritisch perspectief op de discursieve constructie van deze onderwerpen, een tastbaar idee worden gegeven van het abstracte concept locational privacy en worden gekeken naar de toepasbaarheid van deze benadering met als doel om privacy in de context van locatiegebaseerde diensten te begrijpen. Geconcludeerd wordt dat de gebeurtenissen in de twee blogartikelen bijdragen aan de onderhandeling van de normatieve grenzen van wat acceptabel is in het discours van locatiegebaseerde applicaties in relatie tot privacy. Beargumenteerd wordt dat het concept locational privacy het mogelijk maakt om de dynamiek van privacy te vangen in de context van locatiegebaseerde diensten vanuit de focus voor het handelingsvermogen van de gebruiker en aandacht voor de sociale situatie bij onderling gebruik en zakelijke instituties.

Inhoudsopgave

Inleiding	4
1 Locatiegebaseerde diensten en privacy	10
1.1 Locatiegebaseerde diensten	10
1.2 Locatiegebaseerde diensten en de discussie over privacy	12
1.3 Locational privacy	17
2 Kritische Discoursanalyse	24
2.1 De discoursanalyse	24
2.2 De kritische discoursanalyse en de principes volgens Norman Fairclough	25
2.3 De communicatieve gebeurtenis	27
2.4 Werkwijze	30
3 Analyse	32
3.1 Tekstuele dimensie	32
3.2 Discursieve dimensie: tekstproductie en -consumptie	40
3.3 Sociale praktijk	43
4 Conclusie	47
Bibliografie	50
Bijlagen	54

Inleiding

Als student Nieuwe Media en Digitale Cultuur ben ik gefascineerd door de manier waarop het medialandschap zich evolueert en hoe wij, als gebruikers en consumenten, omgaan en denken over media in ons dagelijks leven. In de afgelopen jaren heb ik vooral de ontwikkeling van de smartphone en in het bijzonder het gebruik, de adoptie en het denken over locatiegebaseerde diensten gevolgd. Deze locatiegebaseerde diensten staan in deze scriptie centraal.

Locatiegebaseerde diensten kunnen worden uitgelegd als diensten die aan de hand van de geografische locatie van een mobiel toestel, middels locatiegebaseerde technologieën, locatie-specifieke digitale informatie genereren (Sui, 2004). Met locatiegebaseerde diensten kunnen gebruikers van een mobiel toestel onder andere navigeren in de publieke ruimte, aanbevelingen geven over bezochte locaties zoals restaurants en ook real-time locaties en ervaringen delen met vrienden of andere medegebruikers. Deze diensten zijn in de begin jaren van de 21e eeuw vooral verkend door onderzoekers en mediakunstenaars en waren voor slechts een beperkt publiek toegankelijk (Wilken, 2012). Inmiddels zijn er talrijke commerciële locatiegebaseerde diensten op de markt gebracht en is de verwachting dat het gebruik hiervan toeneemt naarmate de adoptie van smartphones stijgt (Zickuhr, 2013). Een bekend commercieel voorbeeld hiervan is Foursquare. Foursquare is een locatiegebaseerde app waarmee gebruikers informatie kunnen opzoeken aan de hand van een fysieke locatie.¹ Zo kunnen ze bijvoorbeeld zien welke locaties vrienden uit het sociale netwerk recent hebben bezocht en aanraden. Ook is het mogelijk om als gebruiker zelf opmerkingen te delen over bezochte locaties.

Wat in deze ontwikkeling van locatiegebaseerde diensten vooral mijn aandacht heeft getrokken is dat deze diensten, in de vorm van applicaties (apps), in de afgelopen jaren steeds meer onderdeel zijn geworden van het alledaagse smartphonegebruik en tegelijkertijd steeds vaker door vooral nieuwsmedia en het academische discours in verband worden gebracht met het onderwerp privacy. Bij het gebruik van deze applicaties worden de locatiegegevens van gebruikers bijgehouden en gecommuniceerd aan bedrijven dan wel andere leden van een sociaal netwerk. Hoewel gebruikers hiervoor doorgaans bewust en soms onbewust toestemming geven, kan dit privacykwesties met zich meebrengen daar locaties, en in het bijzonder een verzameling van bezochte locaties, details kunnen onthullen over het persoonlijke leven van een individu (Damiani, 2014).

Nieuwsmedia brengen het gebruik van deze diensten regelmatig in verband met mogelijk 'verlies van privacy' en behandelen daarbij vooral kwesties als overheidsinstuties die locatie-informatie gebruiken voor surveillance of zakelijke instuties die informatie gebruiken voor marketingdoeleinden (de Souza e Silva & Frith, 2010).

¹ Zie voor meer informatie over Foursquare: www.foursquare.com/about.

Deze presentatie van locatiegebaseerde diensten en privacy in de media is opmerkelijk aangezien er ook aanwijzingen zijn, uit onderzoek van onder andere Debatin et al.(2009) en Raynes-Goldie (2010), dat gebruikers zich meestal niet zoveel zorgen maken over het gebruik van informatie door instituties. Individuele gebruikers zouden zich vooral ongerust maken over gebruik of eventueel misbruik van (locatie-)gegevens door andere gebruikers (Ibidem). Dergelijke sociale privacykwesties zouden door nieuwsmedia echter juist beperkt worden behandeld (de Souza e Silva & Frith, 2010).

Deze discrepantie in de behandeling van dit onderwerp heeft mij aangezet om de manier waarop er wordt gesproken over locatiegebaseerde diensten in relatie tot privacy, nader te onderzoeken. In deze scriptie wil ik dan ook gaan bekijken hoe dit discours wordt gemaakt. Het is hierbij de moeite waard om beide invalshoeken betreft privacykwesties op het vlak van instituties en gebruikers onderling – in het academische discours ook wel bekend als institutionele locational privacy en sociale locational privacy (Frith, 2012) – kritisch te bekijken. Hierin ben ik vooral benieuwd naar de manier waarop er, op een technologieblog, invulling wordt gegeven aan deze typen privacykwesties.

De reden voor de keuze voor dit type onderzoeksobject is dat technologieblogs en technologiesites een centrale rol spelen in het discours over technologieën zoals locatiegebaseerde diensten (Cacciatore et al. 2012). Dit type nieuwsmedia zit meer in de kern van het onderwerp locatiegebaseerde diensten dan bijvoorbeeld (online) dagbladen of populaire nieuwsmagazines die technologie als een nieuwscategorie naast andere categorieën behandelen. Technologieblogs en -sites berichten over onderwerpen als gadgets, social media, mobile, games, start-ups, ondernemerschap en (grote) bedrijven op het gebied van technologie.² Ze bespreken en bevorderen de adoptie van nieuwe technologieontwikkelingen in sociale culturele dagelijkse praktijken. Daarbij zijn dergelijke blogs als zijnde ‘technologieblog’ ook zelf onderdeel van dit discours en kunnen bovendien als zakelijke institutie worden beschouwd vanwege de achterliggende verdienmodellen. Mijn verwachting is dat dergelijke blogs zodoende ook op een bepaalde – wellicht meer institutionele manier – bijdragen aan de invulling van privacy wanneer het gaat om locatiegebaseerde diensten. In dit onderzoek zal ik daarom proberen licht te werpen op de manier waarop een technologieblog bijdraagt aan de eerder besproken discrepantie.

Hoewel meerdere techblogs een interessante bron zouden kunnen vormen voor deze scriptie, richt ik mij in dit onderzoek specifiek tot blogartikelen van de Amerikaanse technologiesite *Wired.com*. *Wired* is wellicht internationaal een van de meest bekende technologiepublicaties en komt voort uit het gelijknamige magazine dat sinds 1993 bestaat (Fisher, 2010). *Wired* kan worden beschouwd als een centrale actor in het domein en branche van de populaire technocultuur (Ibidem). Hoewel ik in acht neem dat *Wired* regelmatig is bekritiseerd voor het uitdragen van een technologiegedreven of technologie-optimistische ideologie, beschouw ik *Wired* – in lijn

² Hierbij kan gedacht worden aan blogs als Techcrunch, The Verge, Mashable, The Next web.

met socioloog Eran Fisher – niet als een publicatie over technologie maar juist als een publicatie over maatschappelijke kwesties waarbij de besproken onderwerpen worden gefilterd door technologie (2010, p. 37). Ik wil hierbij benadrukken dat hoewel dit blog een invloedrijke rol speelt in dit onderzoek, dit niet een onderzoek is over *Wired* maar juist het discours over locatiegebaseerde diensten en privacy centraal staat binnen de omgeving van dit technologieblog.

Om het discours over privacy in de praktijk van locatiegebaseerde diensten op een technologieblog in kaart te kunnen brengen en te analyseren hoe er hierbij invulling wordt gegeven aan institutionele en sociale privacykwesties, is het van belang om inzicht te hebben in theoretische perspectieven en concepten die dit debat kunnen duiden. Daarom zal ik in dit onderzoek naast discoursanalytische methoden, waarvan ik de interpretatie en werkwijze later in deze inleiding zal toelichten, ook non-discoursanalytische theorieën gebruiken (Jorgensen & Philips, 2002). Voor de selectie van geschikte theoretische perspectieven en concepten zal een kwalitatieve literatuurstudie worden verricht waarbij: “literature including theory is used mainly to understand what is going on in the field and to discover theoretical perspectives, including proper concepts to look at the social phenomenon of interest” (Boeije, 2010, p. 5).

Vanuit de literatuur zal ik dus naar privacy gaan kijken en in het bijzonder naar de manier waarop privacy in de context van locatiegebaseerde diensten kan worden begrepen. Vooropgesteld kan worden dat privacy een complex begrip is en niet eenduidig valt te definiëren. Om hier duidelijkheid in te scheppen zal ik daarom in dit onderzoek enkele centrale noties van privacy behandelen vanuit de filosofie, sociologie en rechtsgeleerdheid. Ook dient te worden opgemerkt dat hoewel privacy in de wetenschap een veelbesproken onderwerp is, er op het gebied van locatiegebaseerde diensten nog tekortkomingen te ontdekken zijn. Zo is middels een verkennend onderzoek duidelijk geworden dat er behoefte is aan meer specifieke benaderingen, die privacykwesties in de praktijk van locatiegebaseerde diensten, kunnen ondervangen (Damiani, 2014). Huidige benaderingen uit de juridische en sociale wetenschap zouden, volgens academici die locatiegebaseerde diensten onderzoeken, niet volstaan (o.a. de Souza e Silva & Gordon, 2011; en Minch, 2011). De kern van de kritiek op deze bestaande benaderingen van privacy is dat deze benaderingen gebaseerd zijn op een onderscheid tussen publieke en privé gegevens. De algemene juridische opvatting van privacy kan worden uitgelegd als de bescherming van datgene dat niet publiek is (Raynes-Goldie, 2010). In deze optiek is iets ofwel publiek of privé.

In dit onderzoek zal ik mij aansluiten bij academici als de Souza e Silva & Gordon (2011) en Minch (2011) en beargumenteren dat dit onderscheid – naar publiek en privé – het begrip van privacy bij locatiegebaseerde diensten in de weg kan staan omdat het gebruik van deze diensten juist betrekking heeft op het publiek maken van informatie over je fysieke locatie. Hoewel ook privacywetenschappers uit de filosofie of rechtsgeleerdheid dit onderscheid verwerpen en een relevante contextuele benadering van privacy voorstellen (o.a. Solove 2008; Nissenbaum 2004), kunnen deze worden

bekritiseerd vanwege het gebrek aan aandacht voor de fysieke dimensie van locatiegebaseerde diensten.

Een andere tekortkoming in de literatuur is te ontdekken op het vlak van privacy als informationele privacy, waarbij privacy vooral gerelateerd wordt aan het gebruik of misbruik van persoonsgegevens voor commerciële doeleinden of voor surveillance door instituties. Onderzoek naar privacy bij het gebruik van de sociale netwerksite Facebook leert dat dergelijke benaderingen van privacy voorbijgaan aan de perspectieven en ervaringen van gebruikers (Raynes-Goldie, 2010). Zo zouden gebruikers privacy niet alleen begrijpen naar aanleiding van kwesties die betrekking hebben op deze instituties, maar door het toenemend gebruik van sociale netwerksites eerder begrijpen als een afweging tussen het onderhouden en versterken van relaties en de communicatie en presentatie van persoonlijke informatie (Ibidem). Voor beter inzicht in perspectieven op privacy is volgens Raynes-Goldie een contextuele benadering van privacy van belang waarbij rekening wordt gehouden met sociale privacy (ibid.). Omdat een groot deel van locatiegebaseerde diensten overlap heeft met sociale netwerksites, veronderstel ik in lijn met Raynes-Goldie dat het voor een begrip van privacy van belang is om ook dergelijke vormen van sociale privacy mee te nemen.

Recent onderzoek naar het concept locational privacy van media- en communicatiewetenschapper Jordan Frith lijkt hierin wellicht een uitkomst te kunnen bieden (Frith 2012). In zijn onderzoek naar de privacydynamica van Foursquaregebruikers gaat Frith uit van een benadering waarbij privacy in de context van zowel instituties (institutionele locational privacy) en gebruikers onderling (sociale locational privacy) wordt begrepen. De benadering van Frith is contextueel te noemen omdat hij privacy als controle per sociale situatie beschouwt (Ibidem).

Middels deze benadering van Frith beoog ik meer inzicht te kunnen verkrijgen in de eerdergenoemde discrepantie. Hierin ben ik benieuwd hoe deze benadering helpt bij de aandacht voor sociale privacy in de behandeling van privacy op het gebied van locatiegebaseerde diensten in de praktijk. Door te onderzoeken hoe de perspectieven over locational privacy van toepassing zijn op het discours over locatiegebaseerde diensten en privacy op een technologieblog beoog ik zodoende de benadering van Frith te kunnen aanvullen met perspectieven uit de praktijk en daarmee een bijdrage te leveren aan het academische discours over locatiegebaseerde diensten en privacy. Dit is van belang omdat Frith in zijn onderzoek bijdraagt aan de discursieve constructie van locational privacy en voornamelijk sociale privacy bij foursquaregebruikers in kaart brengt en zodoende geen inzicht geeft in de verhouding tussen institutionele en sociale kwesties in de praktijken van locatiegebaseerde diensten.

Nu ik het gekozen onderzoeksobject en de geselecteerde theorie zijn geïntroduceerd zal ik de vraagstelling toelichten. De onderzoeksvraag die hier centraal staat luidt:

Hoe wordt er in het populair journalistieke discours op technologieblog Wired invulling gegeven aan institutionele locational privacy en sociale locational privacy?

Om deze onderzoeksvraag te beantwoorden in het licht van het gekozen onderzoeksobject betekent dit concreter dat ik het discours over locatiegebaseerde diensten en privacy met betrekking tot institutionele en sociale privacykwesities in kaart zal brengen; zal meenemen hoe technologieblog *Wired.com* bijdraagt aan dit debat; en zal gaan kijken naar de manier waarop de theoretische perspectieven over locational privacy van toepassing zijn op deze praktijk.

Om deze drie aspecten te kunnen belichten zal er, zoals eerder aangekondigd, gebruik worden gemaakt van een discoursanalytische methode. Discours kan worden uitgelegd als: “a particular way of talking about and understanding the world (or an aspect of the world)” (Jorgensen & Philips, 2002, p. 1). In dit onderzoek zal ik uitgaan van de kritische discoursanalyse volgens de principes van Norman Fairclough (1992). Taal of taalgebruik wordt in de benadering van Fairclough omschreven als een communicatieve gebeurtenis die bestaat uit drie dimensies, te weten: tekst, de discursieve praktijk en de sociale praktijk (Jorgensen & Philips, 2002, p. 68). Deze drie dimensies vormen de basis van zijn driedelige model die ik in dit onderzoek als analytisch instrument zal gebruiken.

Deze methode is relevant voor dit onderzoek om zichtbaar te kunnen maken op welke manier ideeën en meningen over locatiegebaseerde diensten en privacy in de media en samenleving circuleren, zich vormen en normaliseren. De kritische discoursanalyse volgens Fairclough maakt het mogelijk om het discours over locatiegebaseerde diensten en privacy in kaart te brengen, maar ook om te analyseren welke sociale (machts)relaties hieraan ten grondslag liggen en inzicht te geven in de positie van *Wired*. Ook maakt deze benadering het mogelijk om hierbij in de analyse non-discoursanalytische theorieën te integreren (Jorgensen & Philips, 2002). Op deze wijze zal er niet alleen een tastbaarder idee worden gegeven van de besproken theoretische concepten, maar is het ook mogelijk te analyseren hoe de benadering van locational privacy, die uitgaat van zowel institutionele als sociale privacy, van toepassing is op deze vorm van praktijk.

Omdat dit onderzoek een kwalitatieve insteek heeft en de gekozen methode volgens de principes van Fairclough alleen een analyse van een kleine hoeveelheid teksten mogelijk maakt, is de onderzoekscorpus beperkt tot twee blogartikelen van *Wired.com*. Hierbij is lijn met de vraagstelling gekozen voor een artikel op het vlak van institutionele locational privacy en sociale locational privacy. Voor de selectie van deze artikelen heb ik verder geprobeerd om zo veel mogelijk aansluiting te vinden met de aanleiding, vraagstelling en het theoretisch kader.

Onderzoek naar de onderhandeling van dit onderwerp is relevant aangezien het gebied van locatiegebaseerde diensten zich in hoog tempo ontwikkelt (Damiani, 2014). Apps volgens elkaar snel op en doen zich continu voor in nieuwe variaties waardoor dit ook steeds andere privacykwesities met zich meeneemt. Regelgeving loopt hier doorgaans op achter en communicatie hierover vanuit instituties is voor de meeste gebruikers niet transparant met het risico dat de privacy wellicht onvoldoende is

gewaarborgd. Vanuit het wetenschappelijk denkkader van de discoursanalyse is het van belang vanzelfsprekendheden en ongelijke machtsrelaties in dit debat bloot te leggen. Als student Nieuwe Media & Digitale Cultuur acht ik het van belang om deze vanzelfsprekendheden, die in discours genormaliseerd worden, te ontmaskeren zodat we kunnen ingrijpen door bijvoorbeeld zelf deel te nemen aan het discours.

De opbouw van dit onderzoek ziet er als volgt uit. In het eerste hoofdstuk zal ik een kader schetsen van het debat over locatiegebaseerde diensten in relatie tot privacy. Hiervoor zal ik eerst een toelichting geven van locatiegebaseerde diensten en de technische mogelijkheden ten aanzien van het beheer van locatie-informatie. Vervolgens zal ik in de tweede paragraaf voor een algemeen begrip van privacy eerst enkele centrale noties behandelen vanuit de filosofie, sociologie en rechtsgeleerdheid. Daarbij zal ik onderzoeken hoe locatiegebaseerde diensten verschillende noties van privacy uitdagen en stilstaan bij het belang van een contextuele benadering. Beargumenteerd wordt dat benaderingen die uitgaan van een onderscheid tussen publiek of privé niet geschikt zijn op om privacy in de context van locatiegebaseerde diensten te plaatsen. In de derde paragraaf zal ik in de notie van locational privacy onderzoeken waarbij het onderscheid tussen sociale en institutionele privacy zal worden behandeld.

In het tweede hoofdstuk zal ik de onderzoeksmethode van de kritische discoursanalyse en gekozen onderzoekscorpus verder beargumenteren en toelichten. Na een korte introductie van het bredere domein van de discoursanalyse, zal ik in de tweede paragraaf de methode kritische discoursanalyse volgens de interpretatie van Norman Fairclough bespreken (dat voornamelijk gebaseerd is op zijn werk uit 1992). Hierbij zal ik de centrale principes bespreken die deze methode van belang maken voor dit onderzoek waarna ik zijn model verder zal toelichten. In de derde paragraaf zal ik de keuze van onderzoeksobject en de corpus beargumenteren en inzicht geven in de implicaties van deze keuze voor dit onderzoek. Tot slot zal ik in de vierde paragraaf de werkwijze voor de analyse uiteenzetten.

In het derde hoofdstuk zal ik de analyse van de twee blogartikelen behandelen volgens het model van Fairclough (1992). Per dimensie (tekst, discursieve praktijk en sociale praktijk) zal ik de artikelen voor zover mogelijk verbinden met de benadering locational privacy en de overige besproken theoretische perspectieven. Zodoende zal ik analyseren hoe er op technologieblog *Wired.com* invulling wordt gegeven aan institutionele en sociale privacy in de praktijk van locatiegebaseerde diensten waarop ik in de conclusie zal reflecteren.

1 Locatiegebaseerde diensten en privacy

In dit hoofdstuk zal er worden gekeken naar het fenomeen privacy in relatie tot locatiegebaseerde diensten.³ Ik zal hierbij in dit hoofdstuk onderzoeken op welke manier theoretische perspectieven en conceptualisaties van privacy van toepassing zijn op de praktijk van locatiegebaseerde diensten. Hiervoor zal ik in de eerste paragraaf toelichten wat er in deze scriptie wordt verstaan onder locatiegebaseerde diensten en welke technische mogelijkheden er zijn om de locatie-informatie – en daarmee de privacy – te controleren. Om te kunnen begrijpen hoe privacy als sociaal fenomeen kan worden bekeken zal ik daarom in de tweede paragraaf theoretische perspectieven en concepten over privacy behandelen. Hierbij zal ik enkele algemene noties op privacy uit de filosofie en rechtsgeleerdheid beschouwen en vervolgens aan de hand van academici die locatiegebaseerde diensten bestuderen, onderzoeken hoe traditionele en bestaande noties van privacy worden uitgedaagd door locatiegebaseerde diensten. Tot slot zal ik in de derde paragraaf de notie van locational privacy bespreken om te onderzoeken op welke wijze een dergelijk perspectief licht kan werpen op institutionele en sociale privacykwesties en mogelijkheden biedt om privacy in de context van locatiegebaseerde diensten te plaatsen. Met dit hoofdstuk verwacht ik zodoende aan de hand van de besproken termen, concepten en perspectieven een kader te kunnen schetsen voor de analyse en interpretatie van het discours over locatiegebaseerde diensten in relatie tot privacy op *Wired.com*.

1.1 Locatiegebaseerde diensten

In de inleiding is al een indruk gegeven van wat locatiegebaseerde diensten zijn. Vanuit een technisch perspectief gezien kunnen locatiegebaseerde diensten worden uitgelegd als mobiele media die gebaseerd zijn op locaties en daarmee geografisch georiënteerde data mogelijk maken (Sui, 2004). Tegenwoordig zijn de meeste mobiele media zoals mobiele telefoons uitgerust met locatiegebaseerde technologieën. Gebruikers van mobiele media kunnen zo bijvoorbeeld hun positie op een kaart herkennen en zichzelf lokaliseren ten opzichte van andere locaties. Zo kunnen gebruikers bijvoorbeeld middels de mobiele applicatie *Yelp* ondermeer de dichtstbijzijnde bakker lokaliseren en hierover een aanbeveling geven.⁴

Om de positie van de gebruiker te bepalen zijn er verschillende technologieën beschikbaar zoals Bluetooth, Wi-Fi (Wireless Fidelity), RFID (Radio Frequency Identification) en GPS (Global Positioning System) (Lange, 2010, pp. 139-140). Deze laatste is de meest gebruikte positiebepalingstechnologie. GPS maakt gebruik van

³ Zoals in de inleiding al aangegeven wordt er in deze scriptie gekeken naar commerciële locatiegebaseerde diensten in de vorm van mobiele applicaties. Experimentele of specialistische vormen van locatiegebaseerde diensten waaronder locative media (art) zullen hier buiten beschouwing worden gelaten.

⁴ Zie voor meer informatie over Yelp: www.yelp.com/about.

satellietsignalen om de geografische locatie van een GPS-ontvanger te indiceren. De meest recente smartphones kunnen daarbij, middels een ingebouwd kompas, versnellingsmeter en nabijheidsensor, bepalen welke richting het apparaat opwijst en meten of het zich nabij een ander object bevindt (Ibidem).

Op basis van deze technologieën is er een grote verscheidenheid aan locatiegebaseerde diensten ontwikkeld waarbij gebruikers van mobiele media onder andere informatie over hun fysieke omgeving kunnen op zoeken, delen of toevoegen. Hierbij kan gedacht worden aan diensten die gebruikt kunnen worden om hardlooperoutes of golfbanen in kaart te brengen; om de dichtstbijzijnde pinautomaat te vinden; aan locatiegebaseerde games en locatiegebaseerde sociale netwerken (Gordom & de Souza e Silva, 2011).

Het aantal en de variatie in beschikbare commerciële locatiegebaseerde diensten – vaak in de vorm van applicaties – zijn in de afgelopen aanzienlijk toegenomen. De sector van locatiegebaseerde diensten is in de afgelopen jaren bovendien verondersteld als de snelst groeiende sector in de webtechnologiebranche te zijn en heeft het steeds meer de aandacht gekregen van het grotere publiek (Gordon & de Souza e Silva, 2011, p. 9). Vanwege de commerciële en communicatieve potentie zijn de verwachtingen van locatiegebaseerde diensten in deze branche dan ook hoog. Locatie-informatie is ook voorgesteld als heilige graal voor de marketingbranche vanuit het potentieel voor advertenties (Wilken, R. & Sinclair, J. 2009, p. 440). Desondanks de grotere adoptie van smartphones en de verwachtingen voor toenemend gebruik van locatiegebaseerde diensten zoals al aangegeven in de inleiding, zijn advertenties op dit vlak nog niet groots doorgebroken. De reden hiervoor wordt vaak gezocht in de privacygevoelige aard van deze diensten en advertenties (Dhar & Vharsney, 2011).

Vragen over locatie en locatiebewustzijn worden met deze ontwikkelingen steeds centraler in het gebruik van internet en mobiele media en daarmee ook discussies over de schending van privacy of de vrees daarvoor. Om locatiegebaseerde diensten te kunnen gebruiken, is het namelijk nodig om informatie over je locatie te ontsluiten. Ter illustratie, een gebruiker van de eerdergenoemde app *Yelp* zal om informatie te kunnen opzoeken over de dichtstbijzijnde bakker, hiervoor locatie-informatie kenbaar moeten maken aan de provider en beheerder van de applicatie. Naast de provider en applicatiebeheerder kan de locatie-informatie gedeeld worden in het netwerk van de gebruiker en met derden. Dergelijk gebruik van locatie-informatie kan implicaties hebben voor de privacy van de gebruiker. Wat dit dan precies inhoudt en hoe privacy in deze kan worden begrepen is niet eenduidig en zal in de volgende paragraaf verder worden onderzocht. Hieronder zal ik eerst toelichten hoe een gebruiker zelf enige controle kan uitoefenen op de toegankelijkheid en het gebruik van haar of zijn locatie-informatie bij locatiegebaseerde apps.

De gebruiker van locatiegebaseerde diensten kan door middel van het design van de applicaties gebruik maken van bepaalde instellingen om de locatie-informatie zo te controleren. Het is bijvoorbeeld mogelijk om beveiligingsopties in te stellen zoals het

verbergen van locaties voor bepaalde contactpersonen bij locatiegebaseerde sociale netwerkkapps (de Souza e Silva & Frith, 2010, p. 496). Daarbij is er doorgaans in mobiele applicaties een opt-in functie ingebouwd. Hierbij worden gebruikers bij het downloaden van de applicatie expliciet verzocht om de softwarebeheerder toegang tot de telefoon of ander mobiel medium te geven. Tevens is het mogelijk om de nauwkeurigheid van de locatiebepaling aan te passen (Ibidem). Hierbij kan de gebruiker aangeven hoe exact haar of zijn locatie wordt weergegeven of deze locatie handmatig aanpassen. Een gebruiker kan zodoende de locatie bij benadering weergeven of zelfs 'liegen' over haar of zijn locatie. Ook is het mogelijk om de locatievoorzieningen op een mobiel medium voor alle of een specifieke applicatie uit te zetten of de zogenaamde "out of reach" functie in te schakelen. De gebruikers kunnen zodoende de locatie-informatie van de telefoon blokkeren (Ibid.). Hoewel beveiligingsopties van belang en nuttig zijn voor de controle van locatie-informatie, is de gewenste controle en bescherming van privacy hierdoor niet altijd te ondervangen (Damiani, 2014).

In deze eerste paragraaf heb ik een indruk gegeven van locatiegebaseerde diensten aan de hand van een technisch perspectief. Hierover wil ik opmerken dat media als locatiegebaseerde diensten uiteraard complexer zijn dan nu is voorgesteld. Immers worden dergelijke media niet alleen gevormd door technische kwaliteiten maar wordt de betekenis vooral onderhandeld in sociale en culturele praktijken. Ik sluit mij hierin aan bij de visie van Zeffiro die locatiegebaseerde media en diensten niet zozeer beschouwd als een technologie of een ding maar als: "a field of cultural production that is perpetually evolving and continuously reproduced vis-a-vis struggles between technological interpretations and different visions of future use" (2012). In navolging van Zeffiro zullen locatiegebaseerde diensten in dit onderzoek worden beschouwd als een veld van culturele productie zodat de ontwikkeling van deze diensten in een bredere context kan worden begrepen inclusief de discursieve en sociale onderhandeling.

1.2 Locatiegebaseerde diensten en de discussie over privacy

In deze paragraaf beoog ik kader te schetsen van wat privacy is en hoe dit in relatie tot locatiegebaseerde diensten kan worden begrepen. Hiervoor zal ik, om duidelijkheid te scheppen over wat privacy inhoudt, eerst enkele perspectieven op privacy uit een meer algemeen debat bespreken met noties uit de filosofie en rechtsgeleerdheid en ook beleidsgeoriënteerde opvattingen.⁵ Vervolgens zal aan de hand van academici die locatiegebaseerde diensten bestuderen, worden onderzocht hoe locatiegebaseerde diensten in de context van privacy kunnen worden begrepen en hoe hierbij bepaalde benaderingen van privacy worden uitgedaagd.

⁵ In deze scriptie wordt uitgegaan van een Westerse benadering privacy. Er is voor gekozen om andere culturele opvattingen van privacy niet te behandelen.

Privacy: een complex begrip

Privacy is een veelomvattend begrip dat zich lastig laat vangen door definities. Wat privacy precies is en waarom en wanneer dit beschermd dient te worden is daarom ook vaak onderwerp van vele discussies. Het begrip is zodoende onder andere door vele verschillende filosofen, sociologen en juristen bediscussieerd, bekritiseerd en ge(her)conceptualiseerd (Solove, 2008). Dit kan worden verklaard doordat privacy veelal intuïtief wordt geïnterpreteerd. Wat voor de één inbreuk op privacy is voor de ander misschien wellicht niet privacygevoelig. De betekenis van privacy is bovendien cultuur-, tijd- en situatieafhankelijk (Solove, 2008). Zo zijn er bijvoorbeeld grote verschillen in de opvattingen over privacy van Westerse landen met Aziatische landen. In Westerse landen zijn ideeën over privacy vaker gebaseerd op het individu terwijl in Aziatische landen, waar de cultuur een meer collectief karakter heeft, is privacy meer georiënteerd op een groep (Dourish & Bell, 2011: pp. 140-142). Daarnaast is de betekenis van privacy in de afgelopen tijd sterk veranderd en onder andere steeds meer opgeschoven van het beschermen van de huishoudelijke fysieke sfeer naar het beschermen van de persoonlijke informationele sfeer. Om een duidelijker beeld te verkrijgen van de betekenis van privacy en de relevantie zal ik hieronder een aantal invloedrijke perspectieven behandelen uit verschillende disciplines.

Een veelbesproken perspectief dat privacy behandelt als gevoel en inbreuk op privacy beschrijft als een gevoelsmatige kwestie is afkomstig van de filosoof James Rachels (1975). Volgens Rachels, die in 1975 in zijn veelgeciteerde paper de vraag stelde waarom privacy belangrijk is, heeft het belang van privacy te maken met de sociale relaties die mensen met anderen aangaan en de rol die controle op persoonlijke informatie daarbij speelt (Mooradian, 2009). Met controle op persoonlijke informatie wordt hier bedoeld dat een individu de mogelijkheid heeft om zelf te bepalen welke informatie, en in welke mate, zij of hij ontsluit om zo verschillende soorten relaties met anderen te kunnen onderhouden (Ibidem). In de interpretatie van Rachels wordt privacy daarmee gezien als een voorwaarde voor het kunnen onderhouden van een verscheidenheid aan persoonlijke relaties. Het gebrek aan controle over het delen van informatie zou daarbij tot een afname van het aantal relaties en verschillende type relaties kunnen leiden (Mooradian, 2009).

De theorie van Rachels is onder andere in het licht van ontwikkelingen op gebied van 'social computing' en sociale netwerksites bekritiseerd en opnieuw geëvalueerd (Ibidem). De toegenomen hoeveelheid persoonlijke informatie die onder andere via sociale netwerksites wordt geproduceerd – en dus ook locatiegebaseerde (sociale) netwerken – zou in de gedachte van Rachels leiden tot een afvlakking of verlies (in diversiteit) van sociale relaties. Mooradian benadrukt echter dat gebruikers van sociale netwerksites de overtuiging delen dat dergelijke sites juist de soort en het aantal relaties verrijken, in plaats van afvlakken (Ibidem). Mooradian wijst zodoende Rachels' theorie in deze context af en beargumenteert dat: "relationship building characteristics of personal information exchanges include more than the static content of the information."

They include contextual and modal variables such as caring, intent, source, and others” (Ibid., p. 174).

Waar Rachels' werk over privacy als een gevoelsmatige kwestie schrijft, als “our sense of privacy” (1957), wordt privacy in een andere ook veel aangehaalde interpretatie gewaardeerd als een recht. Dit betreft de interpretatie van het concept privacy zoals geformuleerd door de Amerikaanse rechters Warren en Brandeis als “The right to be let alone” (1890). Deze visie op privacy was een reactie op de toenmalige ontwikkelingen van de geschreven pers en hangt sterk samen met het idee van persoonlijke vrijheid waarbij de informatie van een persoon geacht wordt beschermd te worden (Solove, 2008). Hoewel deze ideeën nog steeds van toepassing lijken te zijn voor het begrip privacy, is deze omschrijving onder andere volgens privacy wetenschapper Daniel Solove te beperkt (2008). Het concept privacy beslaat volgens Solove een breder gebied en betreft onder andere onderwerpen als: “freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations” (2008, p. 1).

In zijn boek *Understanding Privacy* onderzoekt Solove verschillende noties van privacy in de negentiende en twintigste eeuw. Hij bekritiseert deze begrippen omdat ze bijvoorbeeld te vaag, breed of te nauw zijn (Ibidem). In deze visies wordt privacy bijvoorbeeld gezien als een concept met een uniforme waarde waarbij wordt uitgegaan van specifieke en noodzakelijke condities of bepaalde toegewezen kernkarakteristieken van privacy. Solove wijst deze eerdere definities, die uitgaan van een sterke gemeenschappelijke noemer, af. Hij stelt voor dat we privacy in een contextuele situatie begrijpen door bijvoorbeeld te focussen op het specifieke privacy probleem. Solove licht dit zelf als volgt toe:

When we protect privacy, we protect against disruptions to certain activities. A privacy invasion interferes with the integrity of certain activities and even destroys or inhibits some activities. Instead of attempting to locate the common denominator of these activities, we should conceptualize privacy by focusing on the specific types of disruption. (p. 9)

Privacy: een kwesties van publiek of privé?

Solove's voorstel van een contextueel begrip van privacy is aannemelijk aangezien het gebied dat onze privacy betreft steeds gecompliceerder is geworden door het toenemende gebruik van diverse informatietechnologieën. Ook Nissenbaum lijkt het hiermee eens te zijn (2004). Om de specifieke karakteristieken van privacy in digitale communicatie te adresseren pleit ook zij daarom voor een contextuele benadering.⁶ Zij beschouwt informatie als iets dat in zichzelf niet publiek of privé is. Nissenbaum betoogt

⁶ Nissenbaum stelt voor een contextuele benadering van privacy het concept “contextual integrity” voor (zie o.a. 2004 en 2010).

dat deze informatie lading krijgt in de context waarin deze wordt verspreid en wij privacy ook als zodanig dienen te begrijpen (2010, p. 216). Volgens Nissenbaum zijn traditionele noties van privacy, waarbij wordt uitgegaan van ideeën als het beperken van surveillance, het limiteren van toegang tot gevoelige informatie en inperken van inbreuk in private plekken, niet geschikt om de complexiteit van privacy in digitale werelden te benaderen (Ibidem, p. 153).

Deze contextuele benadering wordt verder doorgetrokken door Fieschi van de Britse denktank Demos (2007). In een rapport over de sociale waarde van privacy in de maatschappij stelt Fieschi de ideeën over de dichotomie tussen publiek en privaat ter discussie (2007). Volgens Fieschi zijn ideeën over de scheiding tussen publiek en privaat, die met privacy worden geassocieerd, verouderd. Zij benoemt dat genetwerkte stromen van informatie van digitale technologieën de grenzen van de publieke en private ruimten vervagen (Ibidem). Fieschi benoemt dat privacy steeds vaker wordt gezien in relatie tot de hedendaagse sociabiliteit waarin persoonlijke 'gevoelige' informatie dient als een sociaal ruilmiddel (Ibidem). Fieschi laat zien dat privacy daardoor ook in termen van een zogenaamde "exchange value" kan worden beschouwd waarin mensen aspecten van hun privacy ruilen voor specifieke diensten, communicatiegoederen of voor een sterkere sociale band tussen gebruikers onderling (Ibid.).

Een herconceptualisatie van privacy?

Net als Solove, Nissenbaum en Fieschi plaatsen academici die locatiegebaseerde diensten onderzoeken, vraagtekens bij de traditionele noties van privacy. In deze opvattingen worden zorgen voor het verlies van privacy of de schending hiervan volgens deze wetenschappers vaak onterecht geassocieerd met Orwelliaanse noties van surveillance. In discussies over privacy en surveillance wordt er ook vaak verwezen naar George Orwell's "Big Brother" uit het boek en gelijknamige hoorspel *1984* waarbij burgers in angst leven omdat alles wordt geobserveerd door surveillancetechnologie (2013). Deze top-down benadering van surveillance zou zijn verouderd en niet langer relevant zijn wanneer het gaat over de discussie privacy en digitale communicatietechnologie (de Souza e Silva & Gordon, 2011). Sommige onderzoekers vragen zich zelfs af of de term privacy nog wel nuttig is (Dourish & Bell, 2011). Anderen stellen dat er voor het begrijpen van locatiegebaseerde diensten er een specifieke (her)conceptualisatie nodig is van privacy omdat deze diensten de visies op privacy uitdagen (o.a. Blumberg & Eckersley, 2009; Minch, 2011; en Gordon & de Souza e Silva, 2011).

Hoewel de eerdergenoemde ideeën van onder andere Solove en Nissenbaum relevant zijn, voegen locatiegebaseerde diensten naast de digitale dimensie nog een ander element toe aan de discussie van privacy, namelijk: locatie. Gebruikers van locatiegebaseerde technologieën navigeren zowel in de fysieke als de digitale ruimte. Het gebruik van locatiegebaseerde diensten heeft derhalve implicaties voor beide ruimtes. De context waarin privacykwesties over locatiegebaseerde diensten kunnen worden geplaatst, betreft dus niet alleen de context van de digitale ruimte maar een

combinatie van de digitale en de fysieke ruimte. In het academische discours over locatiegebaseerde diensten wordt hiervoor ook wel het concept de ‘hybride ruimte’ gebruikt (de Souza e Silva, 2006).⁷ Dit concept is voorgesteld om onder andere de vervaging en vermenging van grenzen tussen de digitale en fysieke ruimte te kunnen vatten en kan worden uitgelegd als een mix van sociale connecties, digitale informatie en de fysieke ruimte (Ibidem). De Souza e Silva definieert dit begrip als volgt: “Hybrid spaces are mobile social spaces created by the constant movement of users who carry portable devices continuously connected to the Internet and to other users” (2006, p. 262).

Locatiegebaseerde applicaties worden in het academische discours beschouwd als een exemplarisch voorbeeld van het gebruik van mobiele media in hybride ruimtes bijvoorbeeld omdat deze applicaties het mogelijk maken om digitale informatie te koppelen aan fysieke plaatsen en deze informatie vervolgens weer te delen (Wilken, 2012). Ook is het mogelijk om (real-time) locaties van gebruikers te zien of deze gebruikers te tracken. Een relatief recent voorbeeld hiervan is de locatiegebaseerde applicatie *Connect*. De ontwikkelaars omschrijven deze applicatie als: “The real-time marketplace for professional networking” (Appsology 2014). Deze app combineert de gegevens van verschillende sociale netwerken zoals Facebook, Twitter en Linked-In. Aan de hand van deze digitale gegevens laat *Connect* de locaties van contacten zien die zij hebben bezocht en beschikbaar hebben gesteld. Gebruikers kunnen daarbij de locaties van de contacten volgen en fysiek opzoeken. Elke keer wanneer een contactpersoon ergens incheckt of een locatie achterlaat, ontvangt zij of hij een notificatie. Via deze applicatie is het bijvoorbeeld ook mogelijk om aan de hand van diverse criteria andere niet-bekende “zakelijke” gebruikers op te zoeken. Applicaties als *Connect* worden in media-uitingen regelmatig in verband gebracht met discussies over privacy omdat het volgen van de fysieke locatie van een gebruiker kan worden gezien als stalken.⁸

Het voorbeeld van *Connect* geeft aan dat de context van locatiegebaseerde diensten inderdaad kan verschillen van online sociale netwerken zonder locatie-informatie vanwege de fysieke dimensie. De Souza e Silva en Frith verwoorden dit verschil op treffende wijze in het volgende citaat: “Letting a random acquaintance know your favorite books or even your current status is far different from letting that acquaintance know where you are” (2010, p. 496). Het voorbeeld van *Connect* geeft dus een indruk van de vervaging van grenzen tussen digitale informatie en

⁷ De hybride ruimte is niet het eerste concept dat is voorgesteld om de vervaging en vermenging van grenzen tussen de digitale en fysieke ruimte te kunnen begrijpen. Zie voor meer informatie over eerdere conceptuele benaderingen bijvoorbeeld Milgram’s en Colquhoun’s “Mixed Reality” (1999) en Lev Manovich’s “Augmented Space” (2002).

⁸ Zie voor meer informatie over de applicatie *Connect* van Appsology de website connectapp.mobi. Een voorbeeld van een artikel die *Connect* in relatie tot stalking bespreekt is te lezen op de volgende website: www.yahoo.com/tech/new-app-makes-it-easy-to-stalk-friends-or-strangers-78039826303.html.

daadwerkelijke fysieke locaties, wat kan leiden tot een toename van vragen over privacy.

Deze paragraaf heeft laten zien dat privacy complex en diffuus is. Resumerend kan in navolging van Solove worden gesteld dat visies die privacy formuleren als 'gevoel' of 'recht' tekortschieten aangezien privacy een breder domein beslaat. Tevens heb ik beargumenteerd dat de combinatie van fysieke en digitale karakteristieken van locatiegebaseerde diensten visies van privacy, die uitgaan van een onderscheid naar publiek en privé, in de weg staan. Om recht te doen aan de complexiteit van de privacy bij locatiegebaseerde diensten lijkt een contextuele benadering hier meer op zijn plaats. In de analyse zal ik daarom deze complexiteit en meervoudigheid van privacy meenemen door dit niet te beschouwen vanuit een specifieke uniforme waarde of vanuit veronderstelde noodzakelijke condities maar door te letten op de context. Om een beter begrip te kunnen krijgen van de context van privacy bij locatiegebaseerde diensten zal in de volgende paragraaf het concept locational privacy verder worden onderzocht – welke dus veronderstelt acht te slaan op de hybride karakteristieken van locatiegebaseerde diensten.

1.3 Locational privacy

Locational privacy, ook wel location privacy genoemd, is een term die in het academische discours wordt gebruikt om privacykwesties bij locatiegebaseerde diensten beter te kunnen duiden. Locational privacy kan worden omschreven als een term die refereert naar de mogelijkheden om in de publieke ruimte controle uit te oefenen over de toegang en het gebruik van locatie-informatie (Blumberg & Eckersley, 2009). Volgens Duckham en Kulik kan controle van locatie-informatie bovendien als de kern van locational privacy worden beschouwd (2006). Deze auteurs definiëren locational privacy – weliswaar in de tijd van de meer experimentele fase van locatiegebaseerde diensten – als een speciaal type van informatiele privacy uitgaande van de voorwaarde dat individuen voor zichzelf kunnen controleren wanneer, hoe en in welke mate, er locatiegegevens naar anderen worden gecommuniceerd (Ibidem, p. 2).

Beide interpretaties van locational privacy definiëren privacy als een controlekwestie en gaan er in de basis van uit dat het gebruik of misbruik van locatie-informatie betrekking heeft op instanties (Blumberg & Eckersley, 2009; Duckham & Kulik, 2006). De soort controle die de gebruiker verondersteld wordt te hebben, wordt in de toelichting van deze benaderingen, uitgelegd aan de hand van technische mogelijkheden hiervoor zoals privacyinstellingen. Wat in deze interpretaties van locational privacy onderbelicht blijft is de kwesties die het gebruik van locatie-informatie bij gebruikers onderling betreffen. Zoals in de inleiding aangegeven begrijpen gebruikers privacy niet alleen naar aanleiding van kwesties die betrekking hebben op deze instituties, maar meent Raynes-Goldie dat zij dit eerder zien als een afweging tussen het onderhouden en versterken van relaties en de communicatie en presentatie

van persoonlijke informatie (2010). Hoewel deze uitleg overeen lijkt te komen met de bekritiseerde ideeën van Rachels (1975) zoals besproken in de vorige paragraaf, doet Raynes-Goldie hier echter op een interpretatie die in lijn is met het idee privacy-pragmatisme waarbij gebruikers privacy wel belangrijk vinden maar ook bereid zijn om sommige informatie te delen om daar zelf voordeel van te ondervinden (2010). Dit lijkt dus echter meer aansluiting te vinden met ideeën over privacy als sociaal ruilmiddel, hetgeen Fieschi aanduidt in termen van “exchange value” zoals besproken in paragraaf 1.2 (Fieschi, 2007). Naar aanleiding van Raynes-Goldie, zal ik in deze paragraaf de notie locational privacy in de interpretatie van media- en communicatiewetenschapper Frith beschouwen (2012), die veronderstelt niet alleen uit te gaan van privacy in context maar privacy ook benadert op het vlak van sociale privacy en institutionele locational privacy. In het vervolg van deze paragraaf zal ik onderzoeken wat dit begrip inhoudt en hoe dit begrip een contextueel perspectief biedt op privacy in relatie tot locatiegebaseerde diensten en rekening houdt met zowel institutionele als sociale privacykwesties.

1.3.1. Locational privacy

Volgens Frith kan locational privacy worden omschreven aan de hand van danah boyd's definitie van privacy (2011), namelijk: “the control over social situations” (2012).⁹ Deze enigszins brede definitie van privacy gaat uit van het idee dat mensen de mogelijkheid hebben om de informatie die zij communiceren en delen met anderen ook kunnen controleren en zodoende hun privacy kunnen (be)houden (ibid.). Met controle over informatie bedoelt Frith specifiek het handelingsvermogen of ‘agency’ (Frith, 2012, p. 105). Hierbij gaat het om de mogelijkheid om handelingsvermogen uit te oefenen over de wijze waarop gebruikers de informatie delen en in welke context deze informatie wordt verspreid (Ibidem). Anders dan voornoemde definities van locational privacy stelt Frith dat het begrip controle hierbij niet zozeer gaat over hoe de gebruiker privacy-instellingen van locatiegebaseerde mobiele applicaties kan aanpassen en informatie kan beheren, maar over of de gebruiker controle heeft over de sociale context van de praktijken waarin locatiegebaseerde diensten worden gebruikt (Ibid.).

Centraal in Frith's interpretatie staat dat privacy kan worden behouden wanneer individuen zelf de beslissing kunnen maken over welke informatie zij delen met anderen in plaats van dat derden (zoals instituties of andere mede-gebruikers) deze beslissing voor hen maken. Hierbij is het van belang dat individuen de mogelijkheid hebben om de consequenties van het delen van locatie-informatie te kunnen begrijpen. Het risico is anders dat de ‘agency’ van de gebruiker beperkt wordt en de privacy van de gebruiker in het geding kan komen (Ibid.). Met andere woorden kan een disruptie van privacy – zoals omschreven vanuit Solove in de vorige paragraaf (2008)– in termen van Frith dus worden toegeschreven aan een verlies of gebrek aan ‘agency’.

⁹ De naam van de wetenschapper danah boyd is hier bewust zonder kapitalen geschreven. Zie voor meer informatie ook de website van boyd op: <http://www.danah.org/name.html>.

Vanuit de aandacht voor de sociale situatie waarin locatiegebaseerde diensten worden gebruikt, gaat Frith in zijn benadering voorbij aan de scheiding tussen publiek en privé in het debat over privacy. Volgens Frith is locatie op zichzelf namelijk niet inherent publiek of privé, maar afhankelijk van de sociale context. Frith legt dit uit door te refereren aan Simmel's (1950) theorie over anonimiteit in publieke mensenmassa's. Simmel beweert dat een individu tot op zekere hoogte anonimiteit kan bewaren in een menigte mensen, waardoor mensen in staat zijn om hun privacy ook in de publieke ruimte te behouden. Aan de andere kant is locatie niet altijd privé. Zo kunnen bezoekers van een café zien welke andere bezoekers er ook zijn (Frith, 2012). De aandacht voor de sociale situatie maakt zodoende tevens mogelijk dat er rekening kan worden gehouden met zowel de fysieke en digitale aspecten van locatiegebaseerde diensten, echter blijft in de benadering van Frith impliciet hoe de vermenging van deze aspecten hierin precies een rol spelen. Daarnaast maakt dit uitgangspunt van privacy op de sociale situatie ook mogelijk om zowel institutionele als sociale privacykwesties te beschouwen. Deze beide typen van locational privacy zullen hieronder achtereenvolgens worden besproken.

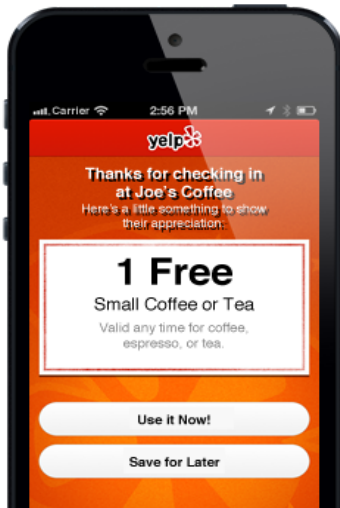
1.3.2 Institutionele locational privacy

Privacykwesties die betrekking hebben op het gebruik van locatie-informatie door instanties als bedrijven of overheden wijst Frith toe aan institutionele locational privacy (2012). Hoewel er kan worden bediscussieerd of privacykwesties die overheden en bedrijven betreffen wel tot dezelfde klasse behoren, worden deze kwesties vanuit het oogpunt van de gebruiker door Frith onder dezelfde categorie geplaatst (2012). Frith gaat in zijn benadering alleen uit van institutionele privacykwesties die bedrijven betreffen. De verklaring hiervoor is dat zijn onderzoek naar Foursquaregebruikers weinig raakvlakken heeft met het gebruik van locatie-informatie door overheidsinstanties. Dit heeft als implicatie dat als we Frith's benadering van locational privacy in dit onderzoek beschouwen in relatie tot de praktijk, dit geen licht zal werpen op kwesties met betrekking tot overheidsinstanties. Hoe kunnen we institutionele locational privacy dan wel begrijpen volgens Frith (2012)?

Frith belicht institutionele locational privacy voornamelijk aan de hand van kwesties die betrekking hebben op locatiegebaseerde advertenties die naar gebruikers worden gecommuniceerd (2012). Locatie-informatie van gebruikers (van mobiele media) kan voor bedrijven relevant zijn om meer specifieke informatie over klanten in te winnen en te gebruiken voor marketingdoeleinden. Hierbij kan dan, inderdaad zoals Frith veronderstelt, vooral gedacht worden aan locatiegebaseerde advertenties. Om deze privacykwesties met betrekking tot locatiegebaseerde advertenties beter te begrijpen belicht Frith een classificatie naar pull- en pushadvertenties. Deze zullen hieronder worden toegelicht.

Pulladvertenties

De voorwaarde voor een pulladvertentie is dat gebruikers ingelogd dienen te zijn bij een locatiegebaseerde dienst om een advertentie te kunnen ontvangen (Frith, 2012, p.110). Gebruikers ontvangen dan bijvoorbeeld een advertentie naar aanleiding van locatiespecifieke informatie die zij hebben opgezocht. Een voorbeeld hiervan is dat individuen die gebruik maken van de dienst *Yelp* in aanmerking kunnen komen voor een speciale aanbieding omdat zij bijvoorbeeld hebben ingecheckt op deze locatie (zie afbeelding 1).



Afbeelding 1: Pulladvertentie Yelp

Bij pulladvertenties kunnen gebruikers van een bepaalde locatiegebaseerde dienst – wanneer zij deze dienst raadplegen en ingelogd zijn – ook advertenties ontvangen van locaties die zich op dat moment in de buurt bevinden. Pulladvertenties worden volgens Frith over het algemeen als minder agressief ervaren dan pushadvertenties (Ibidem).

Pushadvertenties

Bij pushadvertenties wordt er naar gebruikers automatisch een advertentie verstuurd wanneer zij zich in de buurt van een bepaalde locatie bevinden (Frith, 2012, p. 110). Afbeelding 2 illustreert een voorbeeld van Hennes & Mauritz die gebruikers van de app H&M een advertentie stuurt wanneer zij zich in de nabije omgeving van de winkel bevinden.



Afbeelding 2: Pushadvertentie H&M

Hoewel de pulladvertenties volgens Frith dominant lijken te zijn (2012, p. 111), zijn er nog steeds zorgen over hoe deze locatie-informatie wordt gebruikt. In zijn onderzoek identificeert hij drie kwesties van locational institutionele privacy aan de hand van gebruikerspraktijken van de app *Foursquare* (Ibidem, pp. 111-114).

De eerste kwestie die Frith beschrijft betreft het gebruik van locatie-informatie door appbeheerders en lokale ondernemingen, ook wel merchants genoemd (Ibidem). Wanneer de API (Application Programming Interface) van een bepaalde locatiegebaseerde applicatie publiek is gemaakt, kunnen andere bedrijven en ontwikkelaars ook beschikken over de functionaliteit en data van de betreffende locatiegebaseerde dienst.

Een tweede kwestie die hij noemt heeft te maken met het gebruik van een zogenaamde “third party application” (Ibid., p. 112). Ontwikkelaars kunnen publieke API’s gebruiken en aan de hand van de data die deze API’s beschikbaar stellen, nieuwe applicaties ontwikkelen. Een implicatie hierbij is dat gebruikers van deze “third party apps” niet langer beschermd zijn door de privacyvoorwaarden van de oorspronkelijke applicatie omdat deze derde partijen eigen voorwaarden handhaven. Bovendien hebben gebruikers niet altijd kennisgenomen van deze privacyvoorwaarden (Debatin et al., 2009).

Een derde kwestie presenteert Frith in het licht van de grotere maatschappelijke trends op het gebied van dataverzameling en het gebruik hiervan (2012, p. 114). Dit betreft bijvoorbeeld de bundeling van transactiedata, social data, webdata, clickdata en locatiedata.

Institutionele locational privacy wordt door Frith dus grotendeels voorgesteld vanuit het gebruik van locatie-informatie door commerciële instanties. Hierbij worden kwesties in relatie tot bijvoorbeeld surveillance niet besproken, maar ligt de focus vooral op locatiegebaseerde advertenties. Dit betekent dat ik in de analyse, met betrekking tot institutionele locational privacy, ga letten op de manier waarop dit gebruik van locatie-informatie in relatie tot advertenties terugkomt in relatie tot de controle op sociale situaties van gebruikers.

1.3.3. Sociale privacy

Volgens Raynes-Goldie is privacy vanaf de eind jaren ‘70 vooral begrepen als informatieel en institutioneel (2012, p. 80). Hierbij wordt vooral een verbinding gemaakt met de manier waarop instituties zoals overheden, banken en andere bedrijven gebruik maken of misbruik maken van persoonlijke informatie (Ibidem). Zoals in de inleiding besproken zijn ook in de populaire journalistiek privacykwesties rondom locatiegebaseerde diensten vooral gerelateerd aan instituties als overheden of bedrijven en staat dit in contrast met de manier waarop gebruikers van sociale media waaronder locatiegebaseerde (sociale netwerk) diensten dit beleven. Frith meent dat voor een breder begrip van locational privacy het daarom ook zaak is te beschouwen hoe

gebruikers onderling locatie-informatie delen (of verkiezen niet te delen). Dit type privacy kan worden aangeduid als sociale locational privacy (Frith, 2012).

De aandacht voor sociale privacy, binnen locational privacy, is van belang omdat uit onderzoek onder gebruikers van sociale media van onder andere Debatin (2009) en Raynes-Goldie (2010) is gebleken dat gebruikers zich vooral zorgen maken dit type privacykwesaties. Ook het onderzoek van Frith laat dit zien (2012). Dit staat in contrast met een bekend narratief, namelijk dat gebruikers van bijvoorbeeld sociale media niet zouden geven om hun privacy aangezien zij ervoor kiezen dergelijke informatie publiekelijk delen (Ibidem, p. 118). Frith benadrukt dat gebruikers wel degelijk geven om (sociale) privacy. Hij laat dit zien door het onderwerp sociale locational privacy te behandelen aan de hand van de tactieken die gebruikers ontwikkelen voor het controleren van de sociale situaties in het gebruik van locatie-informatie en daarmee voor het beschermen van hun privacy. Als voorbeeld noemt Frith dat gebruikers van locatiegebaseerde (sociale netwerk) apps het (vrienden)netwerk op een bepaalde manier controleren door selectie of toevoegen van vrienden. Hierin benadrukt Frith dat dat de beslissing voor de gebruiker om locatie-informatie te delen met het eigen netwerk, maar ook met andere netwerken, afhankelijk is van de omstandigheden (Ibid.).

Een tweede tactiek uit het onderzoek van Frith die Foursquaregebruikers inzetten is het (micro)managen van bepaalde locaties zoals het inchecken bij het verlaten van locaties.¹⁰ Ook maken gebruikers bijvoorbeeld in de buurt van hun huis een locatie aan om de locatie van hun adres minder exact te maken (Ibid.).

Uit de bespreking van bovengenoemde tactieken is gebleken dat de beslissing om locatie-informatie te delen wordt gerelateerd aan de omstandigheden. Hierbij gaat het volgens Frith om een constante onderhandeling tussen individuen over de wenselijkheid en gepastheid om informatie te delen, wat samenhangt met de bredere sociale of culturele context (Ibid.). De nadruk wordt hierbij gelegd op de mate van controle door de individuele gebruiker over zijn eigen locatie-informatie ten aanzien van andere individuele gebruikers. Opvallend is dat Frith in de behandeling van dit onderwerp niet in termen van schending of de inbreuk over privacy bij gebruikers spreekt.

In deze paragraaf heb ik privacy als locational privacy behandeld omdat dit onderzoek privacy in relatie tot locatiegebaseerde diensten betreft. Geconcludeerd kan worden dat Frith met de benadering van locational privacy een bepaalde interpretatie geeft aan de manier waarop we privacy kunnen beschouwen in de praktijken van locatiegebaseerde diensten. Zijn benadering is contextueel in de zin dat privacy kan worden begrepen in termen van controle op de sociale situaties waarbij de “agency” van de gebruiker centraal staat. In dit licht kan een gebrek aan “agency” in vergelijking tot Solove – zoals beschreven in paragraaf 1.2 – leiden tot een disruptie van een bepaalde activiteit (Solove, 2008). Hierbij dient te worden opgemerkt dat deze benadering minder

¹⁰ Sinds 1 mei 2014 heeft Foursquare het inchecken op locaties ondergebracht onder de mobiele applicatie: Swarm. Zie voor meer info o.a.: www.theverge.com/2014/5/1/5666062/foursquare-swarm-new-app.

de aandacht vestigt op het begrijpen van een bepaalde disruptie als inbreuk of schending, maar privacy behandelt als een bepaalde mate van handelingsvermogen vanuit de gebruiker. Zodoende belicht deze interpretatie van locational privacy een breed spectrum van privacy en behandelt het belang van privacy voor gebruikers in relatie tot de keuzes en mogelijkheden van gebruikers. Hierbinnen is het mogelijk om zowel naar institutionele als sociale privacy te kijken en privacy te bekijken vanuit een visie die voorbij gaat aan de afbakening tussen wat publiek is en privé waardoor rekening kan worden gehouden met het complexe karakter van locational privacy. Dit maakt het concept tegelijkertijd abstract en dit betekent dat iedere kwestie anders kan zijn. Volgens Solove kan het nadeel hiervan zijn dat dit onvoldoende mogelijkheden biedt voor het maken van beleid en het nemen van juridische beslissingen (2008, p. 48). Echter is er ook onderzoek dat uitwijst dat een contextuele benadering – die weliswaar wel meer is uitgewerkt (o.a. in de vorm van een model) – wel toepassingsmogelijkheden heeft voor beleidsvorming (Barth et. 2006).¹¹ Tot slot kan er opgemerkt worden dat de benadering van Frith in dit onderzoek hier meer als een filosofisch perspectief wordt ingezet om privacy te kunnen bekijken, en niet vanwege beleidsgeoriënteerde doeleinden. Bezien vanuit het geschetste kader betekent dit dat ik in de analyse zal gaan letten op privacy als “controle op sociale situaties” in de praktijk van locatiegebaseerde diensten; een privacykwestie zal benaderen vanuit de mate van handelingsvermogen voor gebruikers; en zowel de besproken termen en kwesties ten aanzien van institutionele locational privacy en sociale locational privacy zal aanwenden om de besproken kwesties op het technologieblog te duiden.

¹¹ Het onderzoek van Barth et al. – waaraan ook Nissenbaum heeft meegewerkt – gaat uit van noties van het conceptuele raamwerk “contextual integrity” om noties van privacy te vangen in wetgeving op gebied van “Health Insurance Portability and Accountability Act (HIPAA), the Children’s Online Privacy Protection Act (COPPA), and the Gramm–Leach–Bliley Act (GLBA)” (Barth et al., 2006).

2 De kritische discoursanalyse

Zoals in de inleiding is aangegeven zal dit onderzoek worden uitgevoerd vanuit het wetenschappelijk denkkader van de kritische discoursanalyse. Middels de principes van de kritische discoursanalyse beoog ik zichtbaar te kunnen maken op welke manier ideeën en meningen over locatiegebaseerde diensten en privacy in de media en samenleving circuleren, zich vormen en normaliseren. Concreet beoog ik met de kritische discoursanalyse het volgende te verduidelijken, namelijk: op welke wijze er op technologieblog Wired invulling wordt gegeven aan locational privacy (met in het bijzonder de verhouding tussen institutionele en sociale privacykwesities); hoe dit blog zelf bijdraagt aan dit discours en tot slot inzicht te verkrijgen in de manier waarop de besproken theoretische perspectieven over locational privacy van toepassing zijn op de praktijk. De kritische discoursanalyse (KDA) is onderdeel van de stroming discoursanalyse die is ontstaan aan het einde van de jaren '60 en in het begin van de jaren '70 vanuit de disciplines: linguïstiek, literatuurstudie, antropologie, semiotiek, sociologie, psychologie en communicatiewetenschap (Dijk, 1997, pp. 25-27). Zowel van de KDA, als andere vormen van discoursanalytisch onderzoek, is er geen eenduidige definitie en aanpak. In dit hoofdstuk zal ik toelichten wat de kritische discoursanalyse inhoudt en beargumenteren hoe dit als methode van dit onderzoek kan worden ingezet. Hiervoor zal ik eerst enkele algemene opvattingen van de discoursanalyse en KDA toelichten. Daarna beschrijf ik de methode KDA aan de hand van de principes van Norman Fairclough (1992), die in dit onderzoek zullen dienen als richtlijnen voor de analyse van het technologieblog. Ten slotte, zal ik in lijn met deze principes de gekozen onderzoekscorpus bespreken en de werkwijze voor de analyse hiervan toelichten.

2.1 De discoursanalyse

We build up our sense of the social world through the language we use, the talk we hear, the words we combine, while any sustained strips of social actions and interaction would not be possible without the language we use in specific cultural and historical contexts, as a means for engaging in them (Deacon et al. 1999, p. 148).

In de basis gaat de discoursanalyse over taal in de ruime zin van het woord (Berg, 2004). Wat onder deze 'ruime zin van het woord' kan worden verstaan, wordt mijns inziens op treffende wijze duidelijk gemaakt in bovenstaand citaat van Deacon et al. (1999). Naast dat taal gaat over beelden, gesproken en geschreven teksten, maakt het citaat van Deacon et al. duidelijk dat taal meer is dan alleen een middel voor communicatie (ibidem). De auteurs lichten uit dat er met taal en vooral door taal in sociale acties en interacties, een begrip van de sociale wereld wordt gevormd en

geleefd. Het citaat sluit aan op de centrale opvatting binnen de discoursanalyse, dat taal niet alleen als middel dient om fenomenen te beschrijven, maar taal deze fenomenen ook helpt te construeren. Met andere woorden, de manier waarop onze realiteit wordt gekend is gebaseerd op de manier waarop we de sociale wereld categoriseren. Kortom, binnen de stroming van de discoursanalyse, zijn het discursieve en het sociale onlosmakelijk met elkaar verbonden (Deacon et al. 1999, p. 147).

Er zijn verschillende begrippen en benaderingen van de discoursanalyse zoals van invloedrijke wetenschappers als Laclau en Mouffe, Michel Foucault, Norman Fairclough en Teun van Dijk (Deacon et al., 1999, pp. 144-155). In een meer algemene zin kan de discoursanalyse echter als volgt worden uitgelegd: “onderzoek naar de manier waarop meningen en werkelijkheden discursief – dat wil zeggen in taal – geconstrueerd worden” (Berg, 2004, p. 30). Enkele gemeenschappelijke aannames van de discoursanalyse zijn volgens Van den Berg de volgende (Ibidem, pp. 30-33): taal wordt gezien als sociaal gedrag; taalgebruik is niet neutraal en kan meta-boodschappen in zich dragen; taalhandelingen kunnen leiden tot sociale acties en kunnen consequenties hebben; en taal is afhankelijk van de sociale en culturele context.

Het doel van de discoursanalyse is volgens Van den Berg tweeledig (Ibid.). Ten eerste is de discoursanalyse gericht op het vergaren van kennis over de manier waarop sociale werkelijkheden via discursieve praktijken worden geconstrueerd (Ibid., p. 33). En ten tweede beoogt de discoursanalyse te ontmaskeren hoe deze constructies als het ware tot vanzelfsprekendheden zijn geworden. Hiermee stipt Van den Berg tevens de kritische kwaliteit van de discoursanalyse aan (Ibid.). De discoursanalyse biedt namelijk de mogelijkheid om deze ogenschijnlijke vanzelfsprekendheden kritisch aan de kaak te stellen door te kijken hoe de teksten – die als constructies worden beschouwd – zijn opgebouwd. Door het debat over locatiegebaseerde diensten en privacy op een technologieblog te analyseren middels een discoursanalyse is het zodoende mogelijk om zichtbaar te maken op welke wijze en in welke termen er over dit onderwerp wordt gesproken en daarbij kritisch te kijken naar de ‘vanzelfsprekende’ manier waarop dit onderwerp wordt behandeld. De discoursanalyse helpt zodoende om onderliggende betekenissen en relaties in de behandeling van privacy in de context locatiegebaseerde diensten, zoals de verhouding tussen institutionele en sociale privacykwesties, bloot te leggen.

2.2 De Kritische Discoursanalyse en de principes volgens Norman Fairclough

In deze thesis zal er onderzoek worden verricht aan de hand van een meer specifieke vorm van discoursanalyse, namelijk de kritische discoursanalyse (KDA). De benadering van de KDA is in dit onderzoek van belang aangezien dit mij in staat stelt om de relaties en interacties tussen discours en sociale en culturele veranderingen te duiden (Fairclough, 1995). Hierdoor is het bijvoorbeeld mogelijk om te kijken naar de manier waarop er over locatiegebaseerde diensten wordt gesproken en dit te relateren aan

theoretische perspectieven over privacy zoals behandeld in hoofdstuk 1 (o.a. context, controle en institutionele en sociale locational privacy).

De KDA is voor dit onderzoek daarbij relevant omdat het zeer geschikt is voor onderzoek van het nieuwsdiscours, die in dit geval de gedaante heeft van een technologisch nieuwsblog. Binnen de KDA kunnen nieuwsmedia worden gezien als een ideologisch proces met een belangrijke sociale rol (Ibidem). Hierbij proberen de KDA-analisten de onderliggende rol in en invloed van de discursieve praktijk op de sociale wereld bloot te leggen (Jorgensen & Philips, 2002, p. 63). De KDA beoogt hierbij de sociale relaties en sociale machten te identificeren (Ibidem, 2002, p. 64). In dit onderzoek zou dit bijvoorbeeld kunnen leiden tot inzichten in de rol en bijdrage van technologieblog *Wired* in het te onderzoeken debat.

Zoals eerder aangegeven zijn er verschillende interpretaties van discoursanalyse mogelijk. Een van de meest invloedrijke en ontwikkelde binnen de KDA is van Norman Fairclough (Ibidem, p. 60). Fairclough's benadering van KDA zal als uitgangspunt dienen voor de analyse van dit onderzoek en is om een aantal redenen gekozen (1992).

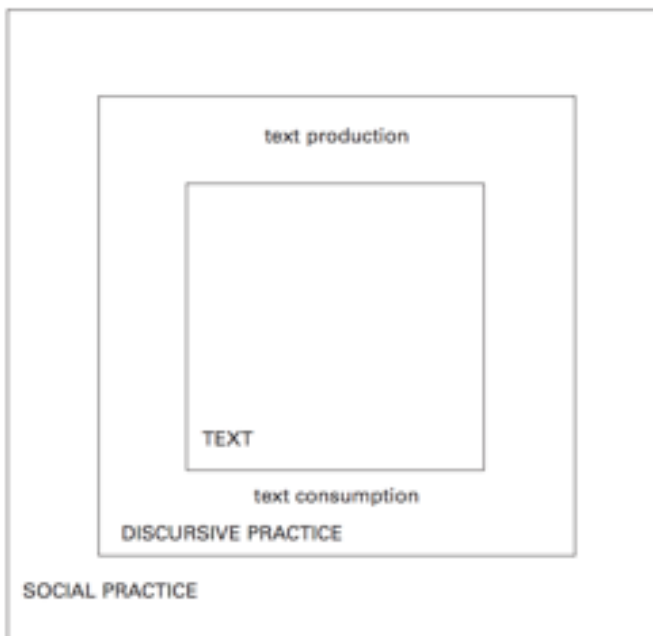
Ten eerste omdat zijn interpretatie uitgaat van een transdisciplinair perspectief (Jorgensen & Philips, 2002). Hiermee wordt een benadering bedoeld die meer in dialoog is met andere disciplines en theorieën waarbij hedendaagse processen van sociale verandering centraal staan. Volgens Fairclough volstaat het niet om alleen naar de gesproken tekst te kijken, maar zijn non-discoursanalytische theorieën van belang om meer inzicht te verkrijgen in de relatie tussen tekst en sociaal-culturele processen en structuren. Fairclough verschilt in dit opzicht van andere benaderingen van de KDA zoals Laclau en Mouffe (Jorgensen & Philips, 2002, p. 63). Laclau en Mouffe zijn voor dit onderzoek minder relevant omdat zij uitgaan van een meer poststructuralistische opvatting en de opvatting delen dat er op cultureel niveau niets bestaat buiten het discours (Ibidem). Uitgaande van Fairclough is het dus van mogelijk om behandeld theorieën over locational privacy te incorporeren in de analyse en derhalve inzicht te verschaffen in de manier waarop deze perspectieven van toepassing op de praktijk.

Ten tweede is de benadering van Fairclough gekozen omdat deze benadering meer aandacht besteedt aan het talige aspect en praktische handvatten biedt voor de analyse in de vorm van een model (zie afbeelding 3). Dit staat in contrast met de benadering van Laclau en Mouffe waarbij methodische instrumenten zeer beperkt aanwezig zijn (Jorgensen & Philips, 2002, p. 146). Hierbij dient te worden opgemerkt dat het nadeel van de methode van Fairclough wel is dat, doordat er een dergelijke mate van aandacht voor het talige aspect wordt verlangd, er in dit onderzoek slechts een beperkte hoeveelheid teksten kunnen worden geanalyseerd (Ibidem). De consequenties van deze limitatie zijn voor dit onderzoek beperkt omdat het voor de beantwoording van de onderzoeksvraag niet nodig is om kwantificeerbare uitspraken te doen. Echter is het van belang om inzicht te verschaffen in de manieren waarop er een bepaalde werkelijkheid in taal wordt geconstrueerd waarbij een bepaalde diepte van linguïstische processen juist waardevol kan zijn.

Driedimensionale model volgens Fairclough

In de analyse zal er als leidraad gebruik worden gemaakt van het model van Fairclough(1992), waarvan de werkwijze in paragraaf 2.4 zal worden besproken. Middels het model kan het discours volgens drie dimensies worden geanalyseerd en inzichtelijk worden gemaakt. Deze drie dimensies zijn:

- de tekst;
- de discursieve praktijk (inclusief de non-discursieve elementen); en
- de sociale praktijk.



Afbeelding 3: Fairclough's driedimensionale model voor Kritische Discoursanalyse (Jorgensen & Philips, 2002, p. 68)

In Fairclough's model heeft "text" betrekking op de semiotische dimensies van sociale gebeurtenissen (Jorgensen & Philips, 2002, pp. 68-69). Het gaat hierbij om een brede opvatting van tekst. De discursieve praktijk gaat over de processen die gerelateerd zijn aan de productie en consumptie van de tekst. De discursieve praktijk vormt en wordt daarbij gevormd door de sociale praktijk (Ibidem., 2002, pp. 68-69). In de dimensie sociale praktijk wordt geanalyseerd hoe de discursieve praktijk de discourses reproduceert en/of herstructureert (Ibid.).

2.3 De communicatieve gebeurtenis

In deze paragraaf licht ik de communicatieve gebeurtenis toe die ik middels KDA, zal gaan analyseren in het licht van de besproken theoretische perspectieven in hoofdstuk 1. Het begrip communicatieve gebeurtenis kan volgens Fairclough worden uitgelegd als

“an instance of language use such as a newspaper article, a film, a video an interview or a political speech” en betreft in dit onderzoek een corpus van twee blogartikelen van technologieblog *Wired* (1995, p. 66). Hoewel discoursanalyses van nieuwsmedia doorgaans gericht zijn op meer traditionele media zoals dagbladen richt ik mij, zoals beargumenteerd in de inleiding, op de mediavorm technologieblog. Specifieker zal er worden gekeken naar twee blogartikelen van de Amerikaanse technologiesite *Wired*. Ik erken dat andere blogs ook zouden volstaan voor dit onderzoek en dat deze keuze uiteindelijk vooral een persoonlijk keuze is. Zoals eerder aangegeven sluit dit blog goed aan bij het karakter van het onderzoeksonderwerp en kan *Wired* worden beschouwd als een centrale actor in het domein en de branche van de populaire technocultuur.

Wired is opgericht door journalisten Louis Rosetto en Jane Metcalfe in 1993 en gestart als magazine. *Wired* heeft in haar beginjaren diverse awards gewonnen vanwege haar innoverend vermogen en culturele invloed (Fisher, 2010, p. 35). Het doel van het magazine van destijds wordt door Fisher als volgt omschreven (Ibidem): “The magazine’s goals was to register and articulate this new [digital] revolution and make sense of the new society to which it gave birth”. *Wired* was gevestigd in Silicon Valley en zat zodoende bovenop de ontwikkelingen waarover zij berichten: “to tell the stories of companies, the ideas, and especially the people making the Digital Revolution”(Ibid.) Naast het magazine volgden er al snel online publicaties zoals verschillende websites en blogs. Hoewel *Wired.com* tegenwoordig meer mainstream is en ook een breder publiek aanspreekt, kan verondersteld worden dat *Wired* vooral een bepaald type technologie-georiënteerd lezerspubliek aanspreekt. Dit type wordt ook wel eens aangeduid met de term digerati (Fisher, 2008). Ik ben mij ervan bewust dat de keuze voor *Wired.com* als onderzoeksobject daardoor consequenties heeft voor de resultaten van dit onderzoek aangezien dit een bepaalde interpretatie geeft van het discours over locatiegebaseerde diensten en privacy.

Voor dit onderzoek heb ik ervoor gekozen om twee blogartikelen te analyseren van *Wired.com*. Voor de selectie van twee artikelen heb ik mij laten leiden door de geconstateerde discrepantie in de behandeling van het onderwerp privacy in relatie tot locatiegebaseerde diensten op het vlak van institutionele en sociale kwesties; de beschreven probleemstelling; en de de behandelde theoretische perspectieven waar ik met dit onderzoek licht op wil werpen waaronder: privacy in context in plaats vanuit een privé-publiek onderscheid; (informatie) privacy als institutionele privacy; en locational privacy als institutionele en sociale locational privacy (zie hoofdstuk 1). Vanuit deze overwegingen acht ik het van belang dat de onderzoekscorpus bestaat uit een blogartikel die de praktijk van locatiegebaseerde diensten behandelt op het vlak van institutionele privacykwesties en een blogartikel die locatiegebaseerde diensten in verband brengt met sociale privacykwesties bij gebruikers onderling. Om in de selectie van de blogartikel op het vlak van beide privacykwesties aansluiting te vinden met het behandelde theoretisch kader heb ik onder andere gelet op onderwerpen, termen of zaken als: zakelijke instituties in de locatietechnologie sector; location-based

advertising; location-sharing; locatiegebaseerde sociale netwerkanwendungen; privacy en termen met een connotatie van privacy (o.a. controle of gebrek aan controle, schending, inbreuk, surveillance). Daarnaast heb ik gelet op of de artikelen daadwerkelijk commerciële locatiegebaseerde diensten bespreken in de vorm van smartphone-applicaties. Andere vormen van locatiegebaseerde diensten zoals navigatiesystemen zijn niet relevant voor dit onderzoek. Daarbij zijn artikelen die locatiegebaseerde diensten in een breder spectrum van online privacy bespreken (denk aan filosofische of juridische bespreking van privacy), buiten beschouwing gelaten.

Aan de hand van de besproken leidraad en voorwaarden heb ik in januari 2014, blogartikelen van het voorgaande jaar van de periode december 2012 tot en met december 2013, beoordeeld. Hiervoor heb ik eerst via Google Search een geavanceerde zoekopdracht gedaan op *Wired.com* aan de hand van de woorden "Location" en "Privacy". Ik heb bewust gebruik gemaakt van brede zoektermen omdat zoektermen als "location-based", "location-aware" en "location-sharing" zodoende meerdere relevante artikelen buitensluiten. Vervolgens heb ik de artikelen aan de hand van de gefilterde selectie vergeleken en beoordeeld op de besproken criteria, en uiteindelijk uit die selectie op basis van een persoonlijke inschatting twee artikelen gekozen. Ik ben mij ervan bewust dat er mogelijk ook andere artikelen geschikt waren en dit wellicht een iets andere voorstelling van dit debat zou kunnen hebben gegeven. Hieronder zullen de twee gekozen artikelen worden geïntroduceerd.

Artikel 1: *Foursquare Evokes Minority Report With Talk of Automatic Ads.*

Het blogartikel met bovenstaande titel, is geschreven door Ryan Tate. Het artikel is gepubliceerd op 16 december 2013, zie hiervoor bijlage 1. Ryan Tate, woonachtig in San Francisco, wordt door *Wired* omschreven als een senior schrijver voor *Wired* en is de auteur van *The 20% Doctrine: How Tinkering, Goofing Off, and Breaking the Rules Drive Success in Business* (2012). In dit boek, dat als managementboek zou kunnen worden getypeerd, onderzoekt de auteur op welke manieren kleine en grote bedrijven innovatief kunnen werken door kleine en specifieke veranderingen in de benadering en indeling van werktijd toe te passen.¹² Het artikel, dat circa 900 woorden beslaat, maakt binnen de website onderdeel uit van het thema Business. De tags die aan het blogartikel zijn verbonden zijn 'social' en 'advertising'. Bij dit artikel wordt ook een afbeelding getoond. Het betreft een beeld van Steven Spielbergs film *Minority Report* uit 2002 van 20th Century Fox (zie hiervoor afbeelding 4 en bijlage 1).

Het blogartikel *Foursquare Evokes Minority Report with talk of automatic ads* behandelt het spanningsveld van het potentieel van locatiegebaseerde advertenties voor bedrijven en het risico consumenten af te schrikken door de inzet van deze advertenties die mogelijke privacykwesties met zich meebrengen. Er wordt vanuit een kapitalistisch oogpunt een kritische blik getoond op de manier van communiceren door zakelijke

¹² Zie voor meer informatie over het boek:
www.harpercollins.ca/books/20-Doctrine-Ryan-Tate/?isbn=9780062003232

instituties over locatiegebaseerde advertenties in relatie tot privacy. De gebeurtenis speelt zich af rondom een van de bekendere apps in deze markt, namelijk *Foursquare*.¹³ Dit gebeurt vanuit het discours van de professional op het gebied van adverteren en marketing.

Artikel 2: *How Location-Based Apps Can Stave Off the ‘Creepy Factor’*

Het tweede artikel van de onderzoekscorpus is getiteld *How Location-Based Apps Can Stave Off the ‘Creepy Factor’*, zie hiervoor bijlage 2. Dit artikel is op Wired.com gepubliceerd op 4 maart 2012 en geschreven door Christina Bonnington. De auteur wordt op de website omschreven als een “staff writer” van Wired.com en blogt over Apple, robotica en “alles daar tussenin” (Wired.com). Bonnington heeft tevens geschreven voor het magazine Wired en de nieuwssite Gizmodo.com. Het artikel bestaat uit circa 800 woorden en is geplaatst op de blog Gadgetlab, welke onderdeel uitmaakt van de website van Wired. De tags die aan het artikel zijn verbonden zijn: ‘Security’ en ‘Apps’. Naast tekst bevat het artikel een afbeelding in de vorm van een foto die is gemaakt door Wired’s fotograaf Jon Snyder (zie hiervoor afbeelding 5 en bijlage 2). Het blogartikel van Bonnington behandelt de privacygevoeligheid en veiligheidsrisico’s van locatiegebaseerde applicaties. Dit gebeurt in het licht van de app *Girls Around Me* die is verwijderd uit de iTunes App Store wegens een vermeende privacyschending. De app maakte het gebruikers mogelijk de omgeving te scannen op meisjes die in de buurt zijn en dit deed aan de hand van de locatie-informatie verkregen vanuit de Api’s van Foursquare en Facebook. Vanuit de discussie rondom deze app belicht de auteur verschillende aspecten van privacy, veiligheidsrisico’s en beveiliging in het gebruik van locatiegebaseerde diensten waarbij perspectieven van deskundigen worden aangehaald. De gebeurtenis wordt besproken in een discours gericht op app-gebruikers en app-developers.

2.4 Werkwijze

Voor de analyse heb ik ervoor gekozen om de artikelen per dimensie uit het model van Fairclough (1992), te behandelen. Hierdoor wordt de verhouding tussen de verschillende discourses zichtbaar. Op het niveau van de tekstuele dimensie zal ik onderzoeken hoe de discourses tekstueel worden geactiveerd en hoe daarbij een bepaalde interpretatie wordt gepresenteerd. Daarbij zal er worden gekeken naar hoe de communicatieve gebeurtenis wordt genoemd en met welke onderwerpen een verbinding wordt gemaakt. In de tekstuele dimensie zullen er tot de tekst ook de volgende aspecten worden gerekend: afbeeldingen, de URL, de gebruikte links en hyperlinks. Bij het tweede artikel zijn er door lezers van Wired.com een achttal opmerkingen geplaatst.

¹³ In de analyse van dit artikel wordt er zowel over het bedrijf Foursquare alsmede de app *Foursquare* (in cursief) gesproken.

Deze reacties zullen niet worden meegenomen in de analyse aangezien er bij het andere artikel geen opmerkingen zijn gepubliceerd.

Op het niveau van de discursieve dimensie zal er worden gekeken naar de discoursen waarop het debat vaart. Daarbij zal worden gekeken naar de wijze waarop het artikel is geproduceerd ten opzichte van de eerdere discoursen. Voor de processen van tekstconsumptie zal ik, vanuit de positie van de KDA-analist, een interpretatie van de lezer analyseren en afleiden.

Voor de analyse op het niveau van de sociale praktijk, zal ik in lijn met Fairclough's principes (1992), mij richten op de ideologische, politieke en sociale effecten van het discours. Ik bekijk hiervoor hoe de relatie tussen de discursieve praktijk en daaraan gekoppelde praktijken eruit ziet, en aan welke institutionele en economische condities de discursieve praktijk is onderworpen. Daarnaast zal ik mij buigen over de sociale-culturele relaties en structuren. Hierbij wordt er gekeken naar de machtsverhoudingen: worden bepaalde relaties verborgen of worden er machtsposities versterkt.

Per dimensie zal er in de behandeling van de artikelen voor zover mogelijk gerelateerd worden aan termen uit het behandelde theoretisch kader. Zodoende zal per dimensie inzichtelijker worden hoe de theoretische perspectieven van toepassing zijn op deze praktijk van locatiegebaseerde diensten. Om antwoord te kunnen op de vraag op welke wijze er invulling wordt gegeven aan institutionele en sociale privacykwesities, zal er vooral gelet worden op de perspectieven met betrekking tot locational privacy zoals besproken door Frith (2012).

3 Analyse

In dit hoofdstuk staat de analyse van het discours over locatiegebaseerde diensten en privacy op technologieblog *Wired* centraal. Zoals toegelicht in het vorige hoofdstuk zullen hiertoe twee artikelen worden besproken aan de hand van de drie dimensies uit het model van Fairclough (1992). Het kan zijn dat er overlap is tussen de verschillende dimensies omdat de grenzen hiervan niet losstaand zijn maar juist permeabel en in elkaar overvloeien. Van de volledige artikelen is een kopie, zoals online gepubliceerd, opgenomen in de bijlagen. Per dimensie zullen de twee blogartikelen worden geanalyseerd in de context van de theoretische concepten zoals besproken in hoofdstuk 1. Hiervoor zal in de lopende tekst, waar relevant, op worden teruggegrepen. In het bijzonder zal er gelet worden op theoretische perspectieven en concepten van Frith om zo institutionele en sociale locational privacy te duiden (2012). Middels de discursieve dimensie in relatie tot de sociale praktijk zal ik analyseren hoe het technologieblog bijdraagt aan dit debat en onderzoeken hoe de theoretische perspectieven van toepassing zijn op (een zekere vorm van) de praktijk (2012). Aan het einde van dit hoofdstuk zal ik hier tot slot op reflecteren.

3.1 Tekstuele dimensie

Artikel 1: *Foursquare Evokes Minority Report with talk of automatic ads*

Zoals al kort toegelicht in paragraaf 2.3 betreft het blogartikel *Foursquare Evokes Minority Report with talk of automatic ads* het discours van de professional op het gebied van adverteren of marketing waarbinnen ontwikkelingen op gebied van locatiegebaseerde advertenties door Foursquare worden behandeld. Dit type discours wordt onder andere geactiveerd door de URL van de webpagina. In deze URL zijn de woorden “futuristic advertising at Foursquare” opgenomen. De titel van de URL speelt in op het verlangen van de lezer om innovatief te zijn op het gebied van adverteren. De combinatie van de titel van het artikel en de URL doen de lezer vermoeden dat de locatiegebaseerde dienst Foursquare een spannende, nieuwe en innovatieve vorm van adverteren gaat aanbieden. Deze combinatie leent zich bovendien sterk voor ‘sharing’ via sociale media. Zodoende wordt er middels de URL en de titel al een bepaalde identiteit geconstrueerd van de professional. In de tekst is een afbeelding opgenomen van een scène uit de sciencefictionfilm *Minority Report* van regisseur Steven Spielberg uit 2002, zie afbeelding 4. Deze afbeelding versterkt de futuristische en innovatieve connotatie waarin het onderwerp adverteren kan worden begrepen. De afbeelding betreft een filmscène waarbij acteur Tom Cruise in een warenhuis geconfronteerd wordt met advertenties.



Afb. 4: Foursquare says it wants to recreate the sort of automatic advertising you see in Steven Spielberg's *Minority Report*. But is that really a good idea?

In deze scène van de film, die zich in het jaar 2054 afspeelt, wordt de protagonist John Anderton, aan de hand van gezichtsherkenningstechnologie in de winkel, persoonlijke advertenties getoond. Hoewel dit voor een deel is af te leiden uit de afbeelding, wordt er in het artikel verondersteld dat de lezer kennis heeft genomen van deze film. Bij de afbeelding is in het ondertekening een kritische en bijna waarschuwende vraag geformuleerd (zie bijlage 1): "But is that really a good idea?" (Tate, 2013a). De lezer wordt hierbij opgeroepen alert te zijn en kritisch na te denken.

Voordat er in het artikel wordt ingegaan op deze vraag worden de locatiegebaseerde advertenties van het bedrijf Foursquare gepresenteerd als aantrekkelijke nabije toekomst voor de reclamewereld. Dit is onder andere af te leiden aan de hand van de volgende linguïstische aspecten. Ten eerste is er allereerst een citaat van Dennis Crowley (CEO van Foursquare) als blikvanger geplaatst in het artikel (zie bijlage 1). De woorden "paid promotions", die in termen van Frith kunnen worden geïnterpreteerd als pushadvertenties (2012, p. 110), activeren hier de zakelijke context van de reclamewereld. Ten tweede worden de 'betaalde advertenties' voorgesteld door Crowley in het artikel te introduceren op een wijze die in lijn is met de afgebeelde scène uit de film *Minority Report*. Zo wordt er beschreven dat Crowley een winkel binnenloopt en dat hij via zijn eigen locatiebewuste app *Foursquare*, op zijn mobiele telefoon, automatisch een locatiegebaseerde persoonlijke advertentie van American Express ontvangt (zie bijlage 1).

Hoewel er in het artikel wordt erkend dat de publieke versie van de app *Foursquare* niet op deze manier met betaalde advertenties werkt en hiervoor nog geen plannen zijn, wordt de suggestie gewekt dat er een soort 'inside information' is van waaruit is gebleken dat deze vorm van adverteren er wel gaat komen (zie bijlage 1). Om de lezer hiervan te overtuigen wordt er een koppeling gemaakt met de positie van het bedrijf en de financiële noodzaak van 'betaalde advertenties' voor Foursquare. De 'betaalde advertenties', die in het artikel verder als "automatic ads" worden aangeduid, worden zodoende vanuit een kapitalistisch perspectief gelegitimeerd als een logische volgende stap voor Foursquare. Dit wordt bovendien benadrukt in de volgende formulering: "It's only what you expect. After all, this is a maturing company hungry for

revenue” (Tate, 2013a). In verhouding tot de perspectieven van Frith over pushadvertenties (2012) – welke verondersteld worden minder dominant te zijn dan pulladvertenties – lijkt de blogauteur zodoende dit type pushadvertenties te normaliseren.

De context waarin deze “automatische ads” in het artikel kunnen worden begrepen in relatie tot privacy wordt zichtbaar naar aanleiding van de volgende vraag: “The question is whether Foursquare can deliver these automatic ads without turning people off” (Ibidem). Door de woorden “turning people off” wordt een bepaalde interpretatie ingezet van het onderwerp privacy in relatie tot locatiegebaseerde advertenties. Zo wordt de formulering “turning people off” in de context geplaatst van het risico om klanten te verliezen waarbij het woord privacy impliciet blijft. Het mogelijke verlies van klanten wordt in het artikel bovendien geïdentificeerd als het overkoepelende probleem van de (locatiegebaseerde) adverteerderindustrie. Dit ‘probleem’ wordt als volgt gearticuleerd: “[...]while trying to win people’s money, you may just get them angry – but this problem becomes particularly acute when you’re tracking people on mobile phones” (Ibid.). Het woord “acute” geeft hierbij een bepaalde urgentie en intensiteit aan het probleem.

Vanuit Frith bezien kan locational privacy alleen worden behouden wanneer individuen zelf de beslissing kunnen maken over welke informatie zij delen en de wijze waarop deze wordt verspreid (2012, p. 105). De risico’s moeten hierbij voor de individuen te overzien zijn (Ibidem). Door privacy hier in de tekst niet te noemen en dit als een ander ‘probleem’ te situeren, wordt locational privacy voorgesteld als een ander type institutionele kwestie, namelijk het verliezen van klanten. De achterliggende (mogelijke) privacyproblematiek voor gebruikers raakt zodoende naar de achtergrond.

De urgentie en intensiteit van het tweezijdige probleem – financiële situatie en het risico om klanten te verliezen – worden gedurende het artikel verder ontwikkeld en ingevuld. Allereerst is de verwachting gewekt dat deze vorm van adverteren er “echt gaat komen”, en wordt de komst van de “automatic ads” bovendien gepresenteerd als een logisch gegeven. Hiervoor wordt in de tekst het argument aangebracht dat Crowley vanaf de start van Foursquare al “droomde” van dit type ‘automatische advertenties’ en hij deze optie niet zonder doel aan het testen was: “He wasn’t testing that Amex ad just for fun” (Tate, 2014a). Ten tweede worden deze ‘automatische advertenties’ gepresenteerd als een financieel noodzakelijke stap voor het bedrijf waarbij nadruk wordt gelegd op de “grote” investeringen die er zijn gedaan en de “karige” inkomsten die Foursquare heeft verworven. Ten slotte wordt er benoemd dat Foursquare haar klanten kan afschrikken door “tracking” of door te veel advertenties te communiceren. Afschrikken wordt in het artikel geformuleerd als “creep users out”. Hoewel “creep users out” in deze context kan worden begrepen in relatie tot privacy en de connotatie heeft van oncomfortabele angstgevoelens bij gebruikers, is de aandacht in de tekst gericht op het verliezen van klanten. Door het ‘afschrikken van gebruikers’ in de tekst te verbinden aan het ‘verlies van het aantal geregistreerde gebruikers’, benadrukt de auteur hier de perspectieven van de marketingprofessionals of instituties en minimaliseert hij de rol

van de gebruiker. Het handelingsvermogen van de gebruiker bij institutionele locational privacy, zoals geconceptualiseerd door Frith (2012), lijkt hierdoor te worden gereduceerd tot de aan- of afmelding van de Foursquare-gebruiker.

Naast Crowley wordt in het artikel van Wired brand partner Brian Williamson van Foursquare aangehaald (zie bijlage 1). De aanleiding hiervoor is een recente presentatie op een evenement voor retail en marketing in december 2013 – het artikel in Wired linkt hierbij door naar een video van de presentatie (Bottger, 2013). Bij dit evenement sprak Williamson ondermeer over ‘locatiespecifieke retail advertenties’ (Ibidem). Het artikel op Wired behandelt een selectief deel van deze presentatie; namelijk het deel waarin Williamson spreekt over de locatiegebaseerde pushadvertenties en hierbij een vergelijking maakt met de film *Minority Report*.

Bepaalde linguïstische kenmerken in de tekst duiden er op dat de auteur de uitingen van Williamson afkeurt vanwege de vergelijking met *Minority Report*. Dit blijkt bijvoorbeeld uit de sfeer waarin de presentatie van Williamson kan worden begrepen. Deze heeft een cynische toon. De lezer wordt gestimuleerd om de presentatie te wantrouwen en daarbij Williamson niet serieus te nemen. Dit gebeurt onder andere door de woordkeuzes bij de introductie van Williamson. Zo wordt er besproken dat Williamson in de presentatie zou hebben opgescheept (“touted”) over de nieuwe automatische notificatietechnologie en over de schat aan data van Foursquare (“huge data trove”) (Tate, 2013a).

Volgens het artikel presenteert Williamson de nieuwe mogelijkheden voor Foursquare, om gebruikers te kunnen tracken en notificeren, als iets om als consument voor te vrezen. Uit de tekst is af te leiden dat de auteur deze wijze van communiceren (door Williamson) over locatiegebaseerde advertenties onverstandig acht omdat dit van negatieve invloed kan zijn op het succes van locatiegebaseerde advertenties. Dit gebeurt onder andere door de weergave van bepaalde citaten van Williamson in het artikel en deze citaten vervolgens te voorzien van een respons die de geloofwaardigheid van Williamson ontkracht (zie bijlage 1). Daarbij verwijst de auteur naar Crowley die, in een eerder interview met Wired (Tate, 2013b), heeft aangegeven dat een vergelijkbare situatie als in *Minority Report* niet zou gebeuren. Zodoende wordt er ingespeeld op de (machts)positie van Crowley waarmee de auteur poogt om de veronderstelde ongeldigheid van Williamsons uitspraken te bevestigen. Foursquare zou de gebruiker juist “iets waardevols willen geven in ruil voor het tracken van je bewegingen” (Tate, 2013a) – een uitspraak die in de eerder besproken termen van Fieschi geïnterpreteerd kunnen worden als ‘sociaal ruilmiddel’ (2007). Het artikel besluit met de boodschap dat als je in deze branche succes nastreeft, je geen vergelijkingen moet maken die betrekking hebben op een “dystopian vision of the future” (Ibidem). Op deze wijze wordt de aandacht gevestigd op dit communicatieprobleem en verplaatst de (impliciet aanwezige) privacyproblematiek van locatiegebaseerde pushadvertenties meer naar de achtergrond.

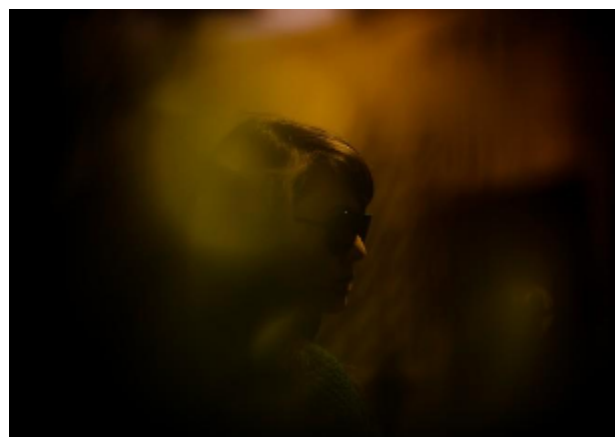
In de analyse van tekstuele dimensie is duidelijk geworden dat institutionele locational privacy zoals geformuleerd door Frith (2012), in het discours van

de professional op gebied van marketing of adverteren, in een kapitalistische context wordt ingevuld door het gebruik van termen als “turning off” en “creeping out” in relatie tot “automatic ads”. Zoals aangegeven wordt het woord privacy niet expliciet genoemd maar ligt de aandacht, door de gehanteerde woordkeuzes, op het risico om klanten te verliezen als zijnde ‘privacykwestie’ voor adverteerders. Door de sfeer waarin ‘klanten verliezen’ wordt gelinkt aan de presentatie over ‘locatiespecifieke retail advertenties’ met termen als “Minority Report” en ‘dystopische toekomst’ verschuift de aandacht van deze ‘privacykwestie’ naar het probleem met betrekking tot de communicatie over deze ‘ads’. Privacy wordt zodoende vermomd als ‘communicatieprobleem’. Hierbij verplaatst de rol van de gebruiker naar de achtergrond. Dit staat in contrast tot Frith’s interpretatie waar de controle over sociale situaties centraal staat vanuit het perspectief van de gebruiker (2012). In de verhandeling op *Wired* staat dus het perspectief van de instituties en de overkoepelende branche centraal en worden deze instituties deze in het onderwerp institutionele locational privacy prominent gepositioneerd.

Artikel 2: *How Location-Based Apps Can Stave Off the ‘Creepy Factor’*

Zoals eerder aangegeven zijn de gebeurtenissen van het tweede artikel gecentreerd rondom de app *Girls Around Me* waarbij onderwerpen privacy, veiligheidsrisico’s en beveiliging worden verbonden met locatiegebaseerde apps. Dit gebeurt vanuit een discours van appgebruikers en appdevelopers. Voor de activatie van dit type discours zijn in de URL alsmede in de titel beperkte aanwijzingen te vinden. Wel zijn deze bijvoorbeeld aanwezig in de combinatie van de afbeelding en ondertekening. De titel van het artikel *How Location-Based Apps Can Stave Off the ‘Creepy Factor’* impliceert dat de tekst een probleem en oplossing voor “Location-Based Apps” behandelt (zie bijlage 2). Uit de titel is niet direct af te leiden aan wie de oplossing is gericht. De nadruk ligt op de apps die verondersteld worden een “creepy factor” als eigenschap en als mogelijk probleem te hebben. Locatiegebaseerde apps worden zodoende in verbinding gebracht met het onderwerp ‘creepiness’, welke in de context van het artikel een associatie oproept van gevoelens van angst.

Deze angstgevoelens worden versterkt door de afbeelding die onder de titel is geplaatst (zie afbeelding 5). De afbeelding toont een vrouw met een zonnebril die en profiel is afgebeeld. De afbeelding is donker, vertoont weinig diepte en is wazig. De setting van de foto doet daarom een beetje grimmig en mysterieus aan en activeert een bepaalde beangstigende sfeer. De lezer krijgt hierbij het idee alsof de vrouw, die op de foto is afgebeeld, wordt bekeken door een andere persoon zonder dat zij dit door



Afb. 5: Is a mysterious stranger scoping you out based on your social media check-ins?

heeft. Deze 'stalkerachtige' sfeer wordt geïntensiveerd door het onderschrift en specifiek door de woorden "mysterious stranger" en "scoping you out" (Bonnington, 2012). Door het onderwerp 'creepiness' op deze wijze te visualiseren en te verbinden met het gebruik van locatiegebaseerde apps wordt door de auteur een bepaalde lading gegeven aan wat in termen van Frith kan worden uitgelegd als social locational privacy (2012), immers impliceert dit een situatie rondom gebruikers onderling. Hoewel het woord privacy hierbij (nog) niet expliciet wordt genoemd schetst het artikel op deze wijze de context van de sociale situatie waarin (de disruptie van) privacy dient te worden begrepen.

De app *Girls Around Me* wordt in de tekst in deze sfeer van 'creepiness' geïntroduceerd. Er wordt in de tekst gewezen op de problematische aspecten van de app, namelijk: het ontbreken van een "opt-in dating service" en vooral het verschaffen van publieke informatie van Foursquare en Facebook aan "voyeuristic, opportunistic gentlemen" met als doel om "local women" uit te checken (Bonnington, 2012). De aanduiding 'publieke informatie' kan gezien vanuit het beschreven theoretisch kader in hoofdstuk 1, in relatie tot privacy verschillend worden geïnterpreteerd. In de context van het artikel betekent 'publieke informatie' hier niet zozeer de 'traditionele' interpretatie van privacy waarbij een strikt onderscheid tussen privé en publiek wordt gemaakt (zoals besproken in paragraaf 1.2). Echter kan 'publiek' hier eerder worden begrepen in lijn met de opvattingen van Nissenbaum waarbij informatie lading krijgt in de context waarin deze wordt verspreid en (locatie)informatie dus niet per definitie publiek is (2010, p. 216).

Door de sfeer van de tekst lijken "local women" hier te worden neergezet als slachtoffers en wordt er gesuggereerd dat de "voyeuristic, opportunistic gentlemen" hier de daders zijn. De manier waarop deze subjecten in relatie tot de app worden beschreven impliceert een betekenis waarbij er in relatie tot locational privacy sprake is van een ongelijke man/vrouw-verdeling en deze apps vooral een probleem voor vrouwen kan zijn. Hier kan aan worden toegevoegd dat –hoewel dit niet wordt genoemd – er ook sprake is van een informatie-asymmetrieprobleem waarbij de een beschikt over meer informatie dan de ander. In termen van Frith duidt dit op een verlies van agency over de sociale situatie (2012).

Rondom de app *Girls Around Me* wordt er steeds meer invulling gegeven aan het onderwerp privacy in relatie tot locatiegebaseerde diensten door het woord 'creepy' op een bepaalde wijze te laden. De term 'creepy' wordt onder andere geladen door de mededeling dat de app is geboycot door Foursquare – die in de tekst daarmee tevens wordt neergezet als de autoriteit op het gebied van locatiediensten en locatiedata – met de voornaamste redenen dat het "too creepy" is en dat het in strijd is met het beleid van Foursquare. Dit geeft de lezer als het ware een 'bewijsstuk' dat deze app niet te vertrouwen is. Vervolgens wordt het geschetste probleem breder getrokken en het gebruik van locatiedata, verkregen door locatiegebaseerde diensten in een meer generieke zin, gesitueerd in dezelfde problematische context als het gebruik van de app

Girls Around Me. Zo wordt de geschetste situatie van *Girls Around Me* gebruikt om aan te duiden dat meer locatiediensten deze “creepy” eigenschappen mogelijk in zich kunnen dragen. Deze “creepy factor” van apps wordt vervolgens verbonden aan potentiële veiligheidsrisico’s die het delen van locatiedata met zich mee kunnen brengen waarbij de woorden “potential security risks” hyperlinken naar het artikel *Why you and your girlfriends should stop checking* in op de website van Venturebeat.com (O’Dell, 2012).¹⁴ In het licht van de besproken theorieën die privacy beschouwen vanuit de specifieke concrete context waarin de informatie wordt gedeeld of gebruikt (o.a. Nissenbaum 2010 en Solove 2008), lijkt dit te suggereren dat privacy hier wordt beschouwd als een kwestie die inherent is – als “creepy factor” – aan het gebruik of delen van locatiedata middels apps. Dit wordt echter in de rest van het artikel genuanceerd door uitspraken van deskundigen die vooral worden ingezet om de lading van de term ‘creepy’ en de relatie met locatiedata verder te construeren.

Middels citaten van deze deskundigen probeert de auteur haar verhandeling meer kracht bij te zetten. Hierbij wordt allereerst gewezen op een uitspraak van een autoriteit op gebied van digitale rechten waarmee wordt gepoogd de lezer te overtuigen dat de app *Girls Around Me* inderdaad “creepy” is, namelijk het volgende citaat: “This may not be illegal, but app developers should note the public outcry — the consensus here is that this is, in fact, socially unacceptable and super creepy (Rebecca Jeschke – EFF)” (Bonnington, 2012). Dit citaat geeft de lezer de indruk dat er een publieke discussie gaande is over deze app en het onderwerp serieus moet worden genomen. De woorden “consensus” en “fact” schetsen een bepaalde werkelijkheid waarin deze mening, dat de app ‘creepy’ is, unaniem wordt gedeeld en er bepaalde afspraken over zijn gemaakt. Uit dit citaat wordt tevens duidelijk voor wie de oplossing van het probleem dat het artikel schetst, is bedoeld: namelijk, de app developers. Zij nemen immers het probleem niet serieus.

Een tweede deskundige die wordt aangehaald betreft een autoriteit op gebied van ‘mobile security’. Deze autoriteit wordt ingezet als bron voor het antwoord op de vraag die de auteur aan de lezer stelt, namelijk de vraag: “What precisely makes us feel creeped out about an app?” (Bonnington, 2012). Hiermee wordt het angstgevoel van de lezer gekoppeld aan het gebruik van apps in een meer algemene zin. Middels het volgende citaat van de deskundige: “I think it’s anything that allows somebody who you don’t know, or don’t interact with, or don’t want to interact with, to retrieve more information about you than you’re comfortable with,” (Mahaffy in Bonnington 2012), articuleert de auteur dit angstgevoel vervolgens als de angst voor het gebrek aan controle van je locatiedata door “somebody who you don’t know”. Met de afbeelding in het achterhoofd van de lezer wordt het gebruik van “somebody” hier al snel gekoppeld aan de “mysterious stranger” uit het onderschrift bij de afbeelding (zie afbeelding 5). In relatie tot Friths interpretatie van social locational privacy, kunnen de aspecten die in het citaat worden

¹⁴ VentureBeat bespreekt nieuws op het gebied van technologie en innovatie en probeert uit te leggen waarom dit van belang is in ons dagelijks leven. De verdere inhoud van het artikel *Why you and your girlfriends should stop checking* in zal ik hier verder buiten beschouwing laten (O’Dell, 2012).

genoemd, zodoende worden geïnterpreteerd als sociale situaties waarin in het handelingsvermogen van de gebruiker wordt aangetast(2012).

De laatste deskundige die wordt geciteerd is een promovendus (Nick Doty) op het gebied van privacy en webstandaarden van de Universiteit van Californië (zie bijlage 2). Aan de hand van de thema's die de promovendus noemt verbindt de auteur eigenschappen aan "creepy apps" die verband houden met privacy. Een eerste thema die de deskundige noemt is het gebruik van data door derden over de gebruiker waarvan zij of hij zich niet bewust is. Volgens de deskundige kan dit, wanneer de gebruiker er achterkomt, leiden tot een gevoel van inbreuk op de privacy. Een tweede thema die deze deskundige noemt is hergebruik van locatiedata in een andere context die voor de gebruiker consequenties kan hebben die zij of hij niet had voorzien.

Vanuit het theoretisch kader over sociale locational privacy valt op dat privacykwesties in het artikel worden besproken vanuit het gebruik of mogelijke misbruik van data door de ander. Dit contrasteert de behandelde perspectieven van Frith waarbij juist de controle of tactieken van de gebruiker ten aanzien van privacy centraal staan (2012). Bezien vanuit dit perspectief lijkt het artikel zodoende het handelingsvermogen van gebruikers van locatiegebaseerde apps, af te zwakken en wordt de macht buiten de gebruikers om neergelegd.

Rondom de app *Girls Around Me* wordt vervolgens zichtbaar dat het artikel deze gebeurtenis niet alleen vanuit sociale locational privacy behandelt, maar er ook een koppeling aanwezig is met institutionele locational privacy. Zo wordt er vanuit de besproken privacythema's bij "creepy" apps een brug geslagen naar andere zogenoemde vormen van "creepy" gebruik van locatiegebaseerde apps waaronder "targeted advertising" en het (secundair) gebruik van data door "third-party party boys" (zie bijlage 2). Hierbij wordt het ondoorzichtige gebruik van locatiedata door derde partijen als problematisch neergezet. Vanuit deze context construeert de auteur de voorwaarden die nodig zijn voor: "keep[ing] an app from coming across untrustworthy or creepy" (Bonnington, 2012). De woorden "transparency" en "user control" dienen hierbij als sleutelwoorden en worden in de tekst gesitueerd als condities voor het behoud privacy. Hoewel dit in de buurt lijkt te komen van wat Frith onder locational privacy verstaat, wordt het onderwerp privacy hier voornamelijk gepresenteerd aan de hand van technische oplossingen in plaats van controle(tactieken) van de gebruiker over de sociale situatie (2012). Bovendien ligt de aandacht in de tekst hier bij de app developer in plaats van bij de gebruikers. Dit blijkt uit de genoemde specifieke technische oplossingen ten behoeve van deze "transparency" en "user control" die app developers kunnen verschaffen waaronder notificaties bij datamonitoring door instanties en een mogelijkheid tot een opt-out van locatiedatagebruik (Bonnington, 2012).

Resumerend kan er worden gesteld dat er in de analyse van de tekstuele dimensie van dit artikel is gebleken hoe er middels de term 'creepy', en de lading die er aan dit begrip wordt gegeven, een bepaalde invulling wordt gegeven aan wat Frith sociale locational privacy noemt (2012). Onderwerpen als privacygevoeligheid en

veiligheidsrisico's van locatiegebaseerde apps zijn hierbij gepresenteerd in een context van een ongelijke man/vrouw-verdeling. Het onderwerp privacy is daarbij behandeld vanuit de aandacht voor het gebruik of misbruik van locatie-informatie door de ander. In het licht van Frith's locational privacy betekent dit, dat in de bespreking van sociale locational privacy, het handelingsvermogen van gebruikers meer naar de achtergrond raakt (2012). De controle is in de tekst beperkt tot beveiligingsopties waarvoor app developers verantwoordelijk worden gesteld.

De linguïstische kenmerken van de tekst op *Wired.com* hebben zodoende bijgedragen aan de constructie van bepaalde sociale relaties en identiteiten waarin sociale locational privacy overlap heeft met institutionele locational privacy. Dit betekent dat het gebruik van locatiegebaseerde diensten en de onderhandeling tussen individuen over de wenselijkheid en gepastheid om locatie-informatie te delen, niet geheel los kan worden gezien van het gebruik van andere institutionele partijen.

3.2 Discursieve dimensie: tekstproductie en -consumptie

In deze discursieve dimensie zal ik beide artikelen analyseren op het niveau van tekstproductie en tekstconsumptie. Dit betekent dat er zal worden gelet op de wijze waarop het artikel is geproduceerd; welke onderwerpen er juist wel of niet in het debat ter discussie zijn gesteld, de discourses waarop het debat vaart en de wijze waarop de tekst kan worden geïnterpreteerd. Hierbij zal er worden onderzocht hoe er een bepaalde interpretatie van institutionele en sociale locational privacy op dit niveau tot stand komt en hoe *Wired.com* hier aan bijdraagt.

Artikel 1:

Het in het blogartikel *Foursquare Evokes Minority Report with Talk of Automatic Ads* wordt institutionele locationl privacy (Tate, 2013a), zoals beschouwd in paragraaf 1.3, gepresenteerd vanuit het discours van de marketingprofessional of adverteerder. Ofwel het discours van de (online) reclamewereld staat centraal. Vanuit een kapitalistische context worden privacykwesties als issue voor de communicatie van bedrijven over locatiegebaseerde diensten genormaliseerd. De privacykwestie kan hier worden geïnterpreteerd als bedreiging voor commercieel succes voor de "ad-business" door het risico "klanten verliezen" en termen als "turning-off" en "creeping-out" (Tate, 2013a). Door deze bedreiging te koppelen aan een kwestie van communicatie over adverteren, lijkt het probleem behapbaar voor deze industrie en wordt er voorbij gegaan aan de consequenties voor de gebruiker.

In relatie tot deze interpretatie van privacy worden de "automatic ads", ten opzichte van de eerdere discourses en de veronderstelde dominante pull-advertenties (Frith, 2012), gelegitimeerd. De eerdere discourses waarop de tekst op *Wired* is gebaseerd betreffen een interview met CEO Dennis Crowley (Tate, 2013b) en een presentatie van de senior brand partner Brian Williamson (Bottger, 2013). Beide teksten staan in het teken van de nieuwe notificatietechnologie van Foursquare die een nieuwe

vorm van adverteren mogelijk zou maken. Het artikel op *Wired* herstructureert deze discoursen door andere bewoordingen te gebruiken dan in de eerdere teksten over Foursquare. Zo worden er bijvoorbeeld rondom de nieuwe notificatietechnologie door Foursquare zelf de volgende termen gebruikt: "passive notifications", "paid promotions" en "automatic tips" (Tate, 2013a) en wordt dit in het artikel op *Wired* geherarticuleerd naar "automatic ads" (Ibidem). Bovendien presenteert de auteur de 'automatic ads' alsof het vanzelfsprekend is dat deze op korte termijn een rol gaan spelen in tegenstelling tot de eerdere discoursen. In deze teksten is de toon rondom deze advertenties veel voorzichtiger en wordt dit geformuleerd als een eventuele mogelijkheid voor de toekomst geformuleerd. Op deze manier worden de normatieve grenzen van wat als acceptabel geldt voor locatiegebaseerde advertenties, in relatie tot privacy, verlegd.

Hoewel deze redenering vanuit technologieblog *Wired* aannemelijk is, gezien zij een relatief technologie-georiënteerd publiek bedienen, dient te worden opgemerkt dat de gebruiker van locatiegebaseerde apps in deze verhandeling zeer beperkt aanwezig is. De gebruiker kan door de lezer worden begrepen als consumerende (potentiële) klant die inkomsten gaat opleveren. Dit blijkt bijvoorbeeld uit het volgende citaat: "while trying to make money, you make just get them angry" (Tate, 2013,a). Het gebruik van locatiedata van consumenten dient te worden begrepen als commoditeit.

Geconcludeerd kan worden dat de gebeurtenis in dit artikel institutionele locational privacy belicht op een wijze die enigszins in contrast staat met de interpretatie van Frith (2012). Er kan worden afgevraagd of en in hoeverre deze invulling van privacy implicaties heeft voor de controle van de gebruiker op de sociale situatie in het gebruik van locatiegebaseerde apps. De overwegingen of tactieken die gebruikers maken bij het gebruik van locatie-apps, zoals ook bij Foursquare, zijn in de deze bespreking niet aanwezig. Hoewel in de inleiding is aangegeven dat gebruikers zich niet zoveel zorgen zouden maken over institutionele locational privacy, worden de implicaties van locatiegebaseerde advertenties ook lastiger zichtbaar wanneer deze worden neergezet als communicatieprobleem (waarvoor bedrijven een oplossing kunnen vinden). Op deze manier draagt *Wired*, door privacy als 'communicatieprobleem' te vermommen op een bepaalde manier bij aan het debat over institutionele locational privacy.

Artikel 2: Discursieve dimensie

Vergeleken met het andere artikel, lijkt dit artikel te zijn geproduceerd vanuit een meer persoonlijke sfeer en een perspectief met een meer sociaal engagement. Waar artikel 1 met een meer kapitalistische insteek poogt om privacy als issue voor de communicatie van bedrijven in de sector van locatiegebaseerde automatische te normaliseren in relatie tot 'automatic ads' (Frith, 2012), tracht het artikel *How Location-Based Apps Can Stave Off the 'Creepy Factor'* juist aan te kaarten wat sociaal niet acceptabel is in het gebruik van locatiegebaseerde diensten (Bonnington, 2012). Dit gebruik van locatiegebaseerde diensten wordt in het artikel gesitueerd rondom de discussie over de app *Girls Around Me*. Hierbij ligt, zoals in de tekstuele dimensie is gebleken, het accent op de onderwerpen privacy, veiligheidsrisico's en beveiliging. De verbinding met deze

onderwerpen en de verbreding van de discussie over de app *Girls Around Me* naar locatiegebaseerde diensten in generieke zin, wordt onder andere bewerkstelligd door de articulatie van meerdere discoursen en verschillende stijlen waarbij er variërend wordt gesproken over "you", "us", "the user" en "consumers" (Ibidem). Zo is het artikel ten eerste geproduceerd vanuit het perspectief van de vrouwelijke lezer. Een voorbeeld hiervan is de afbeelding en het onderschrift waarbij "you" refereert naar een vrouw als een soort prooi (zie bijlage 1). Ten tweede wordt er een breder publiek lezers aangesproken vanuit een waarschuwend perspectief. Deze lezer zou het artikel kunnen interpreteren als een wake-upcall om deze vrouw, die hij of zij mogelijk in de omgeving heeft, te waarschuwen voor de veiligheidsrisico's van deze apps. Als derde spreekt het artikel ook het discours van app-ontwikkelaars aan. Deze worden opgeroepen om apps te ontwikkelen vanuit de waarden transparantie, betrouwbaarheid en gebruikerscontrole. Tot slot worden bedrijven aangesproken vanuit een kapitalistisch perspectief over het belang van veiligheid voor consumenten voor een succesvol verdienmodel.

Zoals hieruit blijkt, spreekt het artikel meerdere discoursen aan waardoor het een ambigu karakter krijgt. Omdat de 'oplossing' voor de potentiële veiligheidsrisico's van "creepy apps" bij de beheerders wordt neergelegd, krijgt de lezer het gevoel dat je als gebruiker niet veel invloed hebt om je hiervoor te beschermen. Net als in het andere artikel, wordt de rol van de overheid niet genoemd. Dit is te verklaren door het Amerikaanse perspectief waarbij de verantwoordelijkheid minder snel bij de overheid wordt neergelegd.

Voor de productie van de tekst heeft de auteur zich gebaseerd op citaten van diverse deskundigen die *Wired* via e-mail heeft verkregen. Naast de citaten is het artikel gebaseerd op twee teksten over de app *Girls Around Me*, namelijk: *Girls Around Me: An App Takes Creepy to a New Level* (Bilton, 2012) en *Why you and your girlfriends should stop checking in* (O'Dell, 2012). Beide teksten zijn bedoeld als een wake-upcall betreft veiligheidsrisico's voor gebruikers van sociale en locatiegebaseerde media. Deze teksten zijn gebaseerd op het oorspronkelijk discours: een tekst op de website van *Cult of Mac* (Brownlee, 2012), die de aanleiding is geweest voor het verbannen van de app uit de App Store van iTunes. Het artikel op deze laatste website heeft aangekaart hoe data van gebruikers van sociale media als *Facebook* en *Foursquare*, door de app *Girls Around Me* kan worden gebruikt of misbruikt (Ibidem). Het accent in deze tekst ligt bij het belang van mediawijsheid en de schending van privacy. Hoewel het artikel van *Wired* in lijn is met de eerdere discoursen, legt het meer nadruk op de 'creepy' eigenschappen van locatiegebaseerde apps en op de gewenste beveiligingsmogelijkheden voor apps binnen het debat van veiligheidsrisico's, beveiliging en privacy (Bonnington, 2012). Het artikel versterkt, verdiept en verbreedt hierdoor de grenzen van het bestaande discours.

In deze discursieve dimensie is getoond op welke discoursen dit debat vaart en hoe deze een verschillende rol spelen in de behandeling van het onderwerp locatiegebaseerde diensten in relatie tot privacy. Op dit niveau van de analyse wordt

zichtbaar hoe sociale locational privacy op verschillende manieren is belicht en verschaft zodoende inzichten in bepaalde soort zorgen over privacy bij gebruikers onderling. In relatie tot het discours vrouwen kan privacy in deze gebeurtenis, in termen van Frith worden begrepen als een verlies van handelingsvermogen op de sociale situatie (2012). De betreffende disruptie van privacy, die wordt gepresenteerd als onwenselijk, gaat uit van een informatiesymmetrie tussen de vrouw en andere gebruikers. Hierin wordt de macht, degene die in dit geval meer informatie heeft over de fysieke locatie van de gebruik(st)er, bij de mannelijke gebruiker neergelegd. En wordt de verantwoordelijkheid bij de app developers neergelegd. Aan de hand van de discourses die betrekking op een meer algemene gebruiker wordt controle benaderd vanuit meer technische aspecten van de gebruiker. In de interpretatie van Frith wordt sociale locational privacy gepresenteerd vanuit het perspectief van de gebruiker die controle kan uitoefenen. De kwesties en tactieken die Frith bespreekt om te laten zien hoe gebruikers omgaan met privacy en dit waarderen, sluiten niet aan bij de manier waarop locatiegebaseerde diensten worden besproken in dit debat. In tegenstelling tot Frith wordt de controle op *Wired* benaderd vanuit de technische mogelijkheden (Bonnington, 2012), dit is begrijpelijk gezien de aard van dit nieuwsmedium. Echter gaat *Wired* niet voorbij aan de sociale situaties voor gebruikers onderling maar bespreekt deze, vanuit de verschillende discourses, ook in relatie tot instituties.

3.3 Sociale praktijk

Artikel 1:

Op het niveau van de sociale praktijk zien we dat het artikel *Foursquare Evokes Minority Report with Talk of Automatic Ads* gesitueerd kan worden in de grotere discussie over de zakelijke verwachtingen en de commerciële potentie van locatiegebaseerde diensten en advertenties waarbij privacy een grote rol speelt (Tate, 2013a). Zoals aangegeven in het eerste hoofdstuk, zijn locatiegebaseerde advertenties eerder gepresenteerd als een opkomende technologie met veel commerciële en communicatieve potentie. De verwachtingen van locatiegebaseerde diensten waren relatief hoog en daarbij is locatie-informatie over consumenten voorgesteld als heilige graal voor de marketingbranche (Wilken, R., & Sinclair, J., 2009, p. 440). Desondanks de grotere adoptie van smartphones zijn dergelijke diensten commercieel gezien nog niet echt doorgebroken. De reden hiervoor wordt vaak gezocht in de privacygevoelige aard van deze diensten en advertenties.

Het artikel draagt bij aan dit debat en probeert hiervan de koers enigszins te veranderen door de normatieve grenzen van dit debat te verleggen. Zoals uit de discursieve dimensie van de analyse blijkt, tracht het artikel de inzet van automatische (locatiegebaseerde) advertenties door de reclamewereld te normaliseren door gebruik te maken van andere bewoordingen dan in de eerdere discourses (zoals gebruikt in het interview en de presentatie van verantwoordelijke van Foursquare). Het versterkt hierbij de positie van Foursquare als belangrijke speler op het gebied van locatiegebaseerde

diensten. Bezien vanuit de ideeën over institutionele locational privacy is opgevallen dat privacy – als bedreiging voor commercieel succes – is vermomd en geherstructureerd tot ‘communicatieprobleem’. Dit wordt onder andere gedaan door het woord privacy niet te gebruiken en niet als het eigenlijke probleem te situeren. In plaats daarvan wordt de uitdaging voor het succes van locatiegebaseerde diensten en advertenties gerelateerd aan de manier van communiceren over automatische advertenties. Dit betekent dat er op gebied van institutionele locational privacy meer macht bij de adverteerder wordt neergelegd. Omdat de tekst dit in de vorm van een advies als feitelijkheid presenteert kan de tekst zodoende aanzetten tot verandering in de communicatie over locatiegebaseerde advertenties bij adverteerders. Doordat de rol van de gebruiker in relatie tot het discours van de reclamewereld enigszins afwezig blijft, wordt het handelingsvermogen of agency van de gebruiker over zijn of haar privacy in deze constructie beperkt tot het wél of niet zijn van een loyale consument.

De auteur is in dit netwerk van discourses gestapt met de commerciële belangen van *Wired* en promotionele belangen voor eigen werk (denk hierbij aan zijn boeken maar ook rol op andere nieuwsmedia). *Wired* dient een commercieel belang en tracht binnen haar beoogde lezerspubliek zoveel mogelijk (website)bezoekers te bereiken. Dit artikel doet dit door de aanlokkelijke titel van de URL en pakkende titel voor het artikel die zich goed lenen voor sociale media (zie bijlage 1). De auteur heeft getracht in te spelen op de statusverhogende kwaliteiten van de URL en titel waardoor lezers hun kennis en/of interesse kunnen etaleren. Met dit artikel heeft de auteur en daarbij het blog *Wired* gepositioneerd als autoriteit op het gebied van media, cultuur en business. Er is hierbij ingespeeld op de bekendheid van Foursquare en ingespeeld op de behoefte aan innovatieve adverteermogelijkheden op gebied van locatiegebaseerde diensten.

Artikel 2:

De ontwikkeling en adoptie van locatiegebaseerde diensten wordt gezien als een continue onderhandeling van diverse complexe sociale processen en factoren. De gebeurtenissen die in de artikelen van dit onderzoek zijn besproken betreffen vooral de onderhandeling op het vlak van de acceptatie en afwijzing van locatiegebaseerde applicaties in relatie tot privacykwesties.

De manier waarop locatiegebaseerde apps in relatie tot privacy discursief worden behandeld is van invloed op de manier waarop deze apps worden gebruikt en daarbij hoe privacy wordt beschouwd en beschermd. Dit blijkt ook uit een van de teksten (Brownlee, 2012), waarop het artikel *How Location-Based Apps Can Stave Off the ‘Creepy Factor’* onder andere is gebaseerd. De discursieve praktijk heeft hierbij de sociale praktijk op een zodanige wijze beïnvloed dat dit consequenties had zoals de (tijdelijke) verwijdering van de app *Girls Around Me* uit de App Store en een verscherping van toezicht op het gebruik van de Foursquare Api van derde partijen door Foursquare.

Het blogartikel op *Wired.com* draagt bij aan deze discussie door de gebeurtenis rondom de app *Girls Around Me* te situeren in een grotere context van het gebruik van

locatiegebaseerde applicaties in relatie tot controle van privacy of het gebrek hieraan. Het artikel draagt bij aan de praktijk van de onderhandeling van de grenzen van wat onacceptabel is voor gebruikers op het gebied van locatiegebaseerde apps en daarbij ook wat acceptabel is. Hoewel er regelgeving is voor privacy met betrekking tot het gebruik van mobiele apps, kan het voorkomen dat deze toch tekortschiet in de bescherming van privacy van gebruikers. Privacy is een complex begrip en daarbij ontwikkelt de markt van de mobiele apps zich in hoog tempo. Vanuit de gebeurtenis rondom de app *Girls Around me*, waarbij het gebruik locatiegegevens in principe niet illegaal was, wordt een presentatie gegeven van wat de lezer in het kader van locational privacy als een onwenselijke situatie in het gebruik van locatiegebaseerde apps zou kunnen zien. Middels de term “creepy” wordt in het artikel lading gegeven aan sociale locational privacy in de zin van veronderstelde onwenselijke situaties. Hierbij wordt de privacygevoeligheid de veiligheidsrisico’s in het gebruik van locatiegebaseerde diensten benadrukt. Omdat de gebeurtenis, een kwestie van een informatie-asymetrie probleem, in het licht van ongelijke vrouw-manverhouding wordt gepresenteerd kan dit sociaal-politieke consequenties hebben voor de manier waarop privacykwesties bij locatiegebaseerde diensten kunnen worden begrepen. De behandelde concepten in het theoretisch raamwerk bieden geen zicht op de wijze waarop zaken als gender hierin een rol kunnen spelen.

Op het niveau van de sociale praktijk kan er worden geconcludeerd dat er op discursieve wijze machtsposities worden uitgedaagd en verstevigd. Zo wordt de geschetste oplossing voor een betrouwbare app, gerelateerd aan de app developer en beheerder. Met andere woorden wordt de macht bij de ontwikkelaar of beheerder wordt neergelegd wat duidt op een ongelijke machtsverdeling tussen individuele gebruikers en instituties. Daarnaast impliceert dit dat ervaringen of tactieken die Frith rondom sociale locational privacy beschouwd (2012), hier gereduceerd raken te worden tot het gebruik van beveiligingstechnieken. Dat de verantwoordelijkheid voor privacykwesties hierdoor grotendeels bij app developers wordt neergelegd, betekent ook dat er enigszins voorbij wordt gegaan aan de angsten die gebruikers hebben voor medegebruikers. Hoewel er in dit artikel medegebruikers als daders zijn getypeerd, worden zij hiervoor niet verantwoordelijk gehouden. Hieruit is op te maken dat *Wired* zodoende in de behandeling van sociale locational privacy bijdraagt aan het institutionele karakter van locational privacy, zoals was gesuggereerd in de inleiding.

Reflectie

In dit hoofdstuk is duidelijk geworden hoe er in de behandelde blogartikelen een invulling wordt gegeven aan institutionele als sociale locational privacykwesties en hoe *Wired* daar aan een bijdrage levert. Tevens is er derhalve van het concept locational privacy een tastbaar idee gegeven. Er is gebleken dat zowel concepten als institutionele als sociale locational privacy nuttig zijn om aandacht te besteden aan de complexiteit en meervoudigheid van privacy. Het vertrekpunt privacy als “control over situations” helpt

hier bijvoorbeeld om de verschillende zorgen en overwegingen van gebruikers bij sociale locational privacy inzichtelijk te maken. Het heeft daarbij vooral inzicht gegeven in de manier waarop het handelingsvermogen van gebruikers wordt beïnvloed in verschillende situaties. Hoewel dit concept het mogelijk maakt om de aandacht te vestigen op sociale kwesties bij gebruikers onderling, moet er hierbij ook een kanttekening worden gemaakt. Door de ruime opvatting van contextualiteit bij locational privacy en focus op hoe controle kunnen uitoefenen, biedt de benadering weinig richtlijnen om de verantwoordelijkheid van (mede)gebruikers en instanties bij deze privacykwesties te duiden. In de praktijk van de blogartikelen is gebleken dat de verantwoordelijkheid bij de privacykwestie met betrekking informatie-asymmetrieprobleem bij gebruikers onderling, werd toegeschreven de app-developers in plaats van bij de mede-gebruiker. De benadering van Solove op privacy, die situaties beoordeeld aan de hand van disrupties zou hier wellicht meer inzicht in kunnen geven. Het begrip controle in de interpretatie van Frith gaat uit van een bepaalde 'empowerment' van gebruikers op hun privacy. De praktijk van het blog leert dat om privacy te duiden ook richtlijnen nodig zijn om deze disrupties te beoordelen.

Hoewel er meer aspecten kunnen worden behandeld, wil ik mij tot besluit beperken tot een laatste opmerking naar aanleiding van het concept institutionele locational privacy. De perspectieven met betrekking tot typen advertenties en kwesties hebben voor dit blogartikel enige duiding gegeven, echter ontbeert het concept institutionele locational privacy handvatten om de verbinding tussen "controle op sociale situaties" met institutionele privacykwesties beter te begrijpen (Frith, 2012). Hetgeen bijvoorbeeld van belang is om onder meer de ongelijke machtsverdeling tussen gebruikers en zakelijke instituties te kunnen duiden.

Conclusie

Om het debat over locatiegebaseerde (commerciële) diensten in relatie tot privacy te kunnen duiden en te onderzoeken op welke manier er invulling wordt gegeven aan institutionele en sociale locational privacy, heb ik eerst vanuit de literatuur gekeken naar concepten van privacy uit verschillende disciplines. Er is gebleken dat locatiegebaseerde diensten bestaande noties van privacy uitdagen (bijvoorbeeld door noties die een onderscheid maken naar publiek en privé; of noties die geen acht te slaan op de fysieke medium-specifieke eigenschappen locatiegebaseerde diensten in relatie tot de digitale eigenschappen). Er is aan de hand van Raynes-Goldie beargumenteerd dat er daarom behoefte is aan een contextueel begrip van privacy waarbij ook rekening wordt gehouden met de context van gebruikers onderling (2012). Dit is van belang omdat concepten uitgaande van informatiele privacy alleen licht werpen op het gebruik van (locatie-)informatie door instituties zoals bedrijven of overheden, en uitdagingen bij gebruikers onderling negeren. Aan de hand van de benadering locational privacy van is door Frith verondersteld dat institutionele alsmede sociale kwesties kunnen worden begrepen vanuit de contextuele definitie van boyd waarbij privacy wordt beschouwd als “controle op sociale situaties” (2008). Een centrale notie in de benadering van Frith is ‘agency’ ofwel handelingsvermogen over de wijze waarop gebruikers van locatiegebaseerde diensten de informatie delen en in welke context deze wordt verspreid (2012).

Met deze interpretatie van locational privacy als basis heb ik middels een kritische discoursanalyse onderzocht hoe er op *Wired.com* invulling wordt gegeven aan institutionele locational privacy en sociale locational privacy aan de hand van twee blogartikelen die de kwesties op dit vlak respectievelijk behandelen. Getoond is hoe beide artikelen bijdragen aan de normatieve grenzen van wat acceptabel of juist onacceptabel is op gebied van locatiegebaseerde diensten in relatie tot privacy. Hierbij is gebleken dat er in het eerste blogartikel *Foursquare Evokes Minority Report with Talk of Automatic Ads* een bepaalde invulling aan institutionele locational privacy is gegeven vanuit het discours van de reclamewereld over “automatic ads” (Tate 2013.a). Hierbij is privacy als kwestie, zonder dat de term genoemd wordt, rondom een kapitalistische sfeer geherarticuleerd van een commerciële bedreiging in termen van het “risico om klanten te verliezen”, tot een ‘communicatieprobleem’. Door privacy als controleerbaar probleem te presenteren heeft *Wired.com* in het debat over institutionele locational privacy bijgedragen aan een ongelijke machtsverdeling tussen zakelijke instituties en individuele gebruikers (die hier als consumenten zijn geportretteerd). Aan de hand van de notie handelingsvermogen inzake de sociale situatie is geïllustreerd dat privacy voor gebruikers in deze constructie is beperkt tot het wél of niet zijn van een loyale consument. Geconcludeerd is dat de gebeurtenis institutionele locational privacy belicht op een wijze die enigszins in contrast staat met de interpretatie van Frith(2012). Er kan tot slot worden afgevraagd in hoeverre er een verband is tussen enerzijds een

dergelijke invulling van privacy en anderzijds de beperkte kennis bij gebruikers over institutionele locational privacy? Verondersteld kan worden dat het vermommen van privacy in het institutionele locational debat, de informatie-asymmetrie tussen gebruikers en bedrijven bevordert en van invloed kan zijn op de controle van de gebruiker op de sociale situatie.

Ten aanzien van sociale locational privacy is in de analyse van het tweede artikel: *How Location-Based Apps Can Stave Off the 'Creepy Factor'* getoond hoe sociale locational privacy in termen van 'creepy' wordt ingevuld in relatie tot het gebrek aan controle over privacy vanuit de gebeurtenis rondom de app Girls Around Me en daarmee bijdraagt aan de onderhandeling van normatieve grenzen over wat onacceptabel is voor gebruikers (Bonnington, 2012). Ik heb hierin laten zien hoe locatiegebaseerde diensten daarbij in relatie tot privacy in verband zijn gebracht met een informatie-assymetrie probleem waarbij sprake is van een ongelijke man/vrouw-verdeling. Middels het concept handelingsvermogen is in kaart gebracht hoe de controle, op *Wired.com*, daarbij gereduceerd wordt tot beveiligingstactieken die app developers aanbieden. Geconcludeerd kan worden dat, doordat de verantwoordelijkheid voor sociale locational privacy wordt neergelegd bij de app developers in plaats van de medegebruikers, er in dit debat dus enigszins snel voorbij wordt gegaan aan de sociale kwesties die gebruikers onderling betreffen. Hieruit is op te maken dat *Wired* zodoende in de behandeling van sociale locational privacy bijdraagt aan het institutionele karakter van locational privacy. Middels de analyse van het debat op *Wired.com* is een tastbaarder idee gegeven van de benadering locational privacy waaruit is op te maken dat de discrepantie tussen institutionele en sociale locational privacy, zoals in de inleiding is beschreven, in stand wordt gehouden.

In de analyse is gebleken dat de benadering van locational privacy volgens Frith niet is bedoeld als theorie (2012, p. 105), echter blijkt dit wel nuttig als kapstok om de dynamiek van privacy te vangen vanuit de focus voor het handelingsvermogen van de gebruiker en aandacht voor de sociale situatie bij gebruikers onderling en of bij zakelijke instituties. Zichtbaar is geworden dat deze ruime opvatting van context bij privacy desondanks een gelimiteerde waarde heeft om de verantwoordelijkheid van (mede)gebruikers en instanties bij deze privacykwesties te beoordelen. De praktijk van het blog wijst uit dat om misstanden met betrekking tot locational privacy te kunnen duiden ook richtlijnen nodig zijn om de 'disrupties' in sociale situaties te kunnen begrijpen. Dit sluit aan op de kritiek die Solove heeft op perspectieven van privacy die een te ruime opvatting hebben van privacy (2008). Om de benadering van locational privacy meer handvatten te bieden zou onderzoek naar een verdere operationalisering van de context een uitkomst bieden, dit zou een goed vervolg zijn om de misstanden bij privacy beter te kunnen duiden.

De methode en onderzoeksbriil van de kritische discoursanalyse die ik in dit onderzoek heb ingezet, heeft mij de mogelijkheid gegeven om naar de discursieve constructie van locatiegebaseerde diensten en privacy te kijken en sociale (machts)relaties bloot te leggen. Met behulp van deze methode heb ik inzicht kunnen geven in de manier waarop taal bij ontwikkelingen op het gebied van locatiegebaseerde

diensten werkt, en gedemonstreerd hoe het begrip privacy in relatie tot deze diensten discursief vorm krijgt en opschuift in de behandelde discoursen. Ook heeft de kritische discoursanalyse van de communicatieve gebeurtenis inzicht verschaft in het proces van de adoptie van een (relatief) nieuw medium en het denken hierover in relatie tot privacy.

Voor de kritische discoursanalyse in dit onderzoek heb ik bepaalde keuzes gemaakt. Aan de hand van de principes van Fairclough heb ik de keuze voor twee blogartikelen gemaakt (1992). Dit heeft een bepaalde diepte in het onderzoek mogelijk gemaakt. Hierbij dient te worden opgemerkt dat de keuze voor *Wired.com* als onderzoeksobject daardoor consequenties heeft voor resultaten van dit onderzoek aangezien dit een bepaalde interpretatie geeft van het discours over locatiegebaseerde diensten en privacy.

Voor verder onderzoek zou een grotere selectie artikelen of blogs meer mogelijkheden bieden waarbij artikelen op het gebied van overheidsinstanties een interessante toevoeging kunnen zijn. De gekozen methode volgens Fairclough heeft dit onderzoek gelimiteerd tot enkele teksten waardoor dit niet mogelijk was (1992). Daarnaast zou een receptieonderzoek, op het analyiseniveau van de discursieve praktijk, van toegevoegde waarde kunnen zijn om te exploreren hoe (verschillende) lezers de teksten interpreteren (Jorgensen & Philips, 2002, p. 82).

Tot besluit, zou het voor de verdere ontwikkeling van het concept locational privacy en een beter begrip van dit onderwerp nuttig zijn om meer aandacht te vestigen op de rol van overheidsinstanties, is het waardevol om de sociale context specifiek te operationaliseren, is het van belang om verder onderzoek te doen naar de manier waarop ongelijke machtsrelaties – zoals tussen consumenten en zakelijke instanties en mannelijke en vrouwelijke gebruikers – een rol spelen bij het handelingsvermogen in sociale situaties van gebruikers.

Bibliografie

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In IEEE Symposium on *Security and Privacy*, p. 15.

Berg, H. van, (2004). *Discoursanalyse*. KWALON 26, 9(2), pp. 29-40.

Bilton, N. (2012, 30 maart) Girls around me that takes creepy to a new level. *Bits. New York Times*. Geraadpleegd op 11-10-2014, van: http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/?_r=0.

Blumberg, A. J., & Eckersley, P. (2009). On locational privacy, and how to avoid losing it forever. *Electronic Frontier Foundation*. Geraadpleegd op 27-05-2014, van: www.eff.org/files/eff-locational-privacy-bulgarian.pdf.

Boeije, H. R., (2010), *Analysis in qualitative research*. Londen: Sage.

Bonnington, C. (2012, 3 april). How location-based apps can stave off the 'creepy factor'. *Wired*. Geraadpleegd op 28-01-2014, van: www.wired.com/2012/04/location-based-app-creepiness/.

Bottger, C. (2013, 12 december). Foursquare's exec on why location is the new cookie. *PSFK SF 2013*. Geraadpleegd op 25-05-2014, van: www.psfk.com/2013/12/bradley-voytek-uber-data-science.html

boyd, d. (2008). Why youth <3 social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media*, pp. 119–142. Cambridge, MA: The MIT Press.

boyd, d. (2011). Debating privacy in a networked world for the WSJ. *Social Media Collective*. Geraadpleegd op 27-05-2014, van: www.socialmediacollective.org/2011/11/20/debating-privacy-in-a-networked-world-for-the-wsj/.

Brownlee, J. (2012, 30 maart). This creepy app isn't just stalking women without their knowledge, it's a wake-up call about facebook privacy. *Cult of Mac*. Geraadpleegd op 11-10-2014, van: www.cultofmac.com/157641/this-creepy-app-isnt-just-stalking-women-without-their-knowledge-its-a-wake-up-call-about-facebook-privacy/?utm_medium=twit&utm_campaign=spread-us.

Cacciatore, M. A., Anderson, A. A., Choi, D. H., Brossard, D., Scheufele, D. A., Liang, X., Ladwig, J., Xenos, M., & Dudo, A. (2012). Coverage of emerging technologies: A comparison between print and online media. *New Media & Society*, 14(6), pp. 1039-1059.

Carpentier, N., & De Cleen, B. (2007). Bringing discourse theory into media studies: The applicability of discourse theoretical analysis (DTA) for the study of media practices and discourses. *Journal of Language & Politics*, 6(2), pp. 265-293.

Connect. (2013). *Appsology*. Geraadpleegd op 11-10-2014, van: <http://connectapp.mobi>.

Damiani, M. L. (2014). Location privacy models in mobile applications: conceptual view and research directions. *Geoinformatica*, pp. 1-24.

Deacon, D., Pickering, M., Golding, P., & Murdock, G. (1999). *Researching communications: A practical guide to methods in media and cultural analysis*. New York: Oxford University Press.

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15, pp. 83-108.

de Souza e Silva, A. (2006). From cyber to hybrid: Mobile technologies as interfaces of hybrid spaces. *Space and culture*, 9(3), pp. 261-278.

de Souza e Silva, A., & Frith, J. (2010). Locational privacy in public spaces: Media discourses on location-aware mobile technologies. *Communication, Culture & Critique*, 3(4), pp. 503-525.

Dhar, S., & Varshney, U. (2011). Challenges and business models for mobile location-based services and advertising. *Communications of the ACM*, 54(5), pp. 121-128.

Dijk, T. van. (1997). The study of discourse. In T. Dijk, van (Ed.), *Discourse as Structure and Process: A Multidisciplinary Introduction* (pp. 1-34). Londen: Sage.

Dourish, P., & Bell, G. (2011). *Divining a digital future: Mess and mythology in ubiquitous computing*. Cambridge, MA: Mit Press.

Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. *Dynamic & mobile GIS: investigating change in space and time*, 3, pp. 35-51.

Entman, R. M., Matthes, J., & Pellicano, L. (2009). Nature, sources, and effects of news framing. In: Wahl-Jorgensen, K., & Hanitzsch, T. (Eds.). *Handbook of Journalism Studies* (pp. 175-190). Philadelphia: Lawrence Erlbaum.

Fairclough, N. (1992). *Discourse and social change*. Cambridge: Polity Press.

Fairclough, N. (1995). *Media Discourse*. Londen: Edward Arnold.

Fairclough, N. (2012). Critical discours analysis. *International Advances in Engineering and Technology*, 7, pp. 452-487. Geraadpleegd op 11-10-2014, van: <http://scholarism.net/FullText/2012071.pdf>.

Fieschi, C. (2007). The social value of privacy. An open society depends on individuals rediscovering social value of privacy. *UK Confidential Report*. Geraadpleegd op 27-05-2014, van: www.demos.co.uk/publications/ukconfidential.

Fisher, E. (2010). *Media and new capitalism in the digital age: The spirit of networks*. New York: Palgrave Macmillan.

- Frith, J. H. (2012). Constructing location, one check-in at a time: examining the practices of Foursquare users (Proefschrift). North Carolina State University.
- Gordon, E., & de Souza e Silva, A. (2011) *Net Locality: Why location matters in a networked world*. Boston: Wiley-Blackwell.
- Jørgensen, M., & Phillips, L. (2002). Discourse analysis as theory and method. Londen: Sage Publications.
- Lange, M. de. (2010) *Moving Circles: Mobile media and playful identities* (Proefschrift). Rotterdam: Erasmus Universiteit Rotterdam.
- Manovich, L. (2002). The Poetics of Augmented Space. *Lev Manovich Official Website*. Geraadpleegd op 27-05-2014, van: www.manovich.net.
- Milgram, P., & Colquhoun, H. (1999). A taxonomy of real and virtual world display integration. In Y. Ohta & H. Tamura (Eds.) *Mixed reality: Merging real and virtual worlds* (pp. 5-30). New York: Springer.
- Minch, R. (2011). Issues in the development of location privacy theory. *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. pp. 1-10.
- Mooradian, N. (2009). The importance of privacy revisited. *Ethics and information technology*, 11(3), 163-174.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review Association*, 79(119), pp. 101- 39. Geraadpleegd op 25-05-2014, van: www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf.
- Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.
- O'Dell, J. (2012, 30 Maart). Why you & your girlfriends should stop checking in. *Venturebeat*. Geraadpleegd op 10-11-2014, van: <http://venturebeat.com/2012/03/30/i-hate-all-apps-bah-humbug/>.
- Orwell, G. (2013 [1949]). *1984* (49^e druk). Utrecht: Arbeiderspers.
- Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 4(4) pp. 323-333.
- Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1). Geraadpleegd op 25-05-2014, van: <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432>.
- Raynes-Goldie, K. (2012). *Privacy in the Age of Facebook: Discourse, Architecture, Consequences* (Proefschrift). Perth: Curtin University.

Solove, D. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, 44, pp. 745-772.

Solove, D. (2008). *Understanding privacy*. New York: Harvard University Press.

Spielberg, S. (2002) *Minority Report*. 20th Century Fox.

Sui, D. Z. (2004). The media and the messages of location-based services (LBS): Death of distance or the revenge of geography?. *Geographic Information Sciences*, 10(2), pp. 166-174.

Tate, R. (2013a, 16 december). Foursquare evokes minority report with talk of automatic ads. *Wired*. Geraadpleegd op 28-01-2014, van: www.wired.com/2013/12/futuristic-advertising-at-foursquare/.

Tate, R. (2013b, 9 december). The Brilliant hack that brought fourquare back from the death. *Wired*. Geraadpleegd op 25-05-2014, van: www.wired.com/2013/12/the-brilliant-foursquare-hack/.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5) pp. 193-220.

Wilken, R., & Sinclair, J. (2009). 'Waiting for the kiss of life': Mobile media and advertising. *Convergence: The International Journal of Research into New Media Technologies*, 15(4), pp. 427-445.

Wilken, R. (2012). Locative media: From specialized preoccupation to mainstream fascination. *Convergence: The International Journal of Research into New Media Technologies*, 18(3), pp. 243-247.

Zeffiro, A. (2012). A location of one's own: A genealogy of locative media. *Convergence: The International Journal of Research into New Media Technologies*, 18(3), pp. 249-266.

Zickuhr, K. (2013, 12 september). Location-based services. Pew Internet and American Life Project. *Pew Research Center*. Geraadpleegd op 24-05-2014, van: <http://pewinternet.org/Reports/2013/Location.aspx>.

Bijlagen

Bijlage 1:

Foursquare Evokes *Minority Report* With Talk of Automatic Ads

BY RYAN TATE 12.16.13 | 6:30 AM | PERMALINK

[Share](#) 1 [Tweet](#) 3 [+1](#) 10 [in Share](#) [Print](#)



Foursquare says it wants to recreate the sort of automatic advertising you see in Steven Spielberg's *Minority Report*. But is that really a good idea? Image: 20th Century Fox

Foursquare CEO Dennis Crowley walked into the J.Crew store on New York's Prince Street, armed with an experimental version of the company's popular mobile app. The app is now smart enough to track his whereabouts, and as he entered the store, it automatically showed him a special offer that said he could save \$20 if he spent at least \$100 with his American Express card.

In other words, it sent him an AMEX ad because it knew he was at J.Crew. "We have all these specials on Foursquare, and we can make people more aware of them," he told us during an interview this fall, not long after his visit to the SOHO store. "We're really good at recommending places to people, and you can imagine some of that is paid promotions at some point."

'WE'RE REALLY GOOD AT RECOMMENDING PLACES TO PEOPLE, AND YOU CAN IMAGINE SOME OF THAT IS PAID PROMOTIONS AT SOME POINT'

– DENNIS CROWLEY

That's not how the public version of the app works today. Though Foursquare recently rolled out a new version of its mobile service that closely tracks your movements and delivers suggestions regardless of whether you "check in" to the app or not, these automatic suggestions don't include paid ads, and officially, the New York-based startup says it has "no plans at the moment to push ads through real-time notifications." But when we spoke to Crowley, he clearly indicated that, somewhere down the road, it will.

It's only what you'd expect. After all, this is a maturing company that's hungry for revenue. The question is whether Foursquare can deliver these automatic ads without turning people off. It faces the eternal conundrum that plagues all ad-driven business — while trying to win people's money, you may just get them angry — but this problem becomes particularly acute when you're tracking people on mobile phones.

Today, the company only delivers ads if you actively check-in to the app. But Crowley has always seen check-ins as a stop-gap solution. When he first dreamed up Foursquare thirteen years ago, he envisioned something that sent you stuff unbidden, and now, thanks to a clever hack from his engineering team, that's what he has. The new Foursquare delivers tips based not only on where you are, but also your movement patterns, the activity of your friends, and comments left by other Foursquare users.

To his credit, Crowley told us that he wants to improve the unpaid notifications before delivering ads in the same way. But it will happen. He wasn't testing that AMEX ad just for fun.

The stakes are high. On the one hand, after \$112 million in funding and scant revenue, the company needs to get both users and advertisers to engage more frequently with its app, and delivering unsolicited ads could be just the thing it needs. More than any other company, Foursquare understands how to pinpoint exactly where a user is and what type of information they might want at that very moment.

Of course, the company could also creep users out by tracking them too closely or annoy them with spammy ads — or both. Many of Foursquare's 40 million registered users have already given the app a chance and then dropped it. If the company blows its second chance, there probably won't be a third.

Foursquare senior brand partner Brian Williamson seemed to acknowledge this tension between convenience and creepiness during a recent talk at [an event sponsored by the consultancy PSFK](#). He touted Foursquare's huge data trove, including more than 4.5 billion check-ins over the years, as well as the company's new automatic notification technology, but then came a little joke.

"With the new iOS phones, [and] with the new Android phones, we are able to measure where people are regardless of where they check-in," Williamson said. "I'll let you soak that in and get real scared for a second." Yes, the audience laughed, but there comes a point where this isn't that funny.

Williamson went on to make a comparison between the automatic ads that Foursquare could deploy and the science fiction movie *Minority Report*, in which Tom Cruise is [greeted with personalized suggestions](#) of a more complex nature. "You could see where this could go for retailers," Williamson said. "The power of how they could use this — to say: 'Hey, are you near my store? Here's something you should check out' — harkens back to *Minority Report*, where a mannequin is physically talking to Tom Cruise as he is walking by a store. It's getting close to that. This is like the first early step of that."

The thing is, *Minority Report* showed us just how horrifying that world can be. Cruise's character can't walk more than a few steps through a mall without getting heckled by countless video posters.

Crowley insisted during our interview that this sort of thing won't happen, that Foursquare wants to give you something valuable in exchange for the privilege of tracking your movements. And if the company is to succeed, it will have to. But that doesn't mean it will. Perhaps Crowley should start by telling his brand managers to stop comparing Foursquare to some dark, dystopian vision of the future.

Bijlage 2:

How Location-Based Apps Can Stave Off the 'Creepy Factor'

BY CHRISTINA BONNINGTON 04.03.12 | 5:57 PM | [PERMALINK](#)

[f Share](#) [0](#) [t Tweet](#) [0](#) [g+1](#) [8](#) [in Share](#) [Pin It](#)



Is a mysterious stranger scoping you out based on your social media check-ins? *Photo: Jon Snyder/Wired.com* [📷](#)

Sometimes an app pushes the boundaries of what's socially acceptable — and it fails miserably. Such is the case with the most recent offender, the check-in-based pariah called Girls Around Me.

"In the mood for love, or just a one night stand?" the app's website asks. The query wouldn't be problematic if the app supported an opt-in dating service. But it doesn't. It's an app that was using public information from Foursquare check-ins and Facebook to provide voyeuristic, opportunistic gentlemen the chance to scope out local women.

"Was" is an operative word here. Foursquare pulled its API access because Girls Around Me was just too creepy (and violated their terms).

And so enters the controversy: All of the location data siphoned down by the app was willingly surrendered by Foursquare users. But the way the app used that data was inherently creepy, and highlighted the potential security risks of broadcasting one's location across social media.

"Context is everything," EFF digital rights analyst Rebecca Jeschke told Wired via email. "This may not be illegal, but app developers should note the public outcry — the consensus here is that this is, in fact, socially unacceptable and super creepy."

But what is creepy? What precisely makes us feel creeped out about an app?

"I think it's anything that allows somebody who you don't know, or don't interact with, or don't want to interact with, to retrieve more information about you than you're comfortable with," Kevin Mahaffey, CTO and co-founder of Lookout Mobile Security told Wired. "That's the trigger that borders on creepy in people's minds."

Color was another app that transitioned from cool to ick as users realized nearby strangers would be able to view their photos on the social network — and they could potentially get an eyeful of whatever that person wanted to share, as well.

Nick Doty, a Ph.D. student studying privacy and web standards at UC Berkeley's School of Information, pointed out a few themes that arise among "creepy" apps.

"In some cases, it may just be a sense of surprise. The user isn't aware information is being used in a particular way, and when they realize it's being shared or used differently, that can feel like a violation," Doty said. "In other cases, it can be the context. Information is shared in one context and reused in another one that's unexpected or has a different implication."

Girls Around Me is just one example of that fractured context scenario. Users willingly shared their information within Foursquare or Facebook, but were potentially unaware that this data could be used by third-party party boys.

Over-reaching advertising can also creep us out, Doty says. Say you're using a restaurant search app, and you're aware that it's using your GPS location to help find businesses near you. You're OK with that. But perhaps the app doesn't also tell you that it's using your location for another purpose: to help advertisers better create a profile of you for targeted advertising.

"That's a pretty common problem — these secondary uses that don't seem related to the app's functionality," Doty said.

Thus, transparency and user control are key to keeping an app from coming across as untrustworthy or creepy. Developers already have the tools to make sure users are aware of geolocation features in apps, and it's incumbent on them to use them.

For apps that constantly transmit data, like [Find My Phone](#), it would be helpful to regularly send texts or emails notifying the device owner of the continued data monitoring, Doty suggests, as tools like this are sometimes used by abusive ex-partners.

Mobile devices could also employ "ambient notice" features to let users know when location data is being shared. For example, when you're using your iPhone's compass, you can see the phone's arrow symbol and know your device is currently using that feature. Similar signposting could be used for location services.

And, of course, dialog boxes that pop up upon first downloading an app give users a chance to opt-out of location data sharing. These could be augmented to disclose greater detail on what information is collected, and where it might end up. In fact, there are efforts to develop a voluntary code of conduct for location-based apps, according to Mark Uncapher, director of regulatory and government affairs at the Telecommunications Industry Association.

As for Girls Around Me, after Foursquare revoked access to its API, the app developers removed it from the App Store. But the app will be back, apparently. Product lead Vlad Vishnyakov told Wired via email that his company will be changing the application name to be gender neutral, and will make the app design "less provocative," among other changes to meet Foursquare's API requirements.

"Addressing these concerns is an important part of having a successful business model in the space," Uncapher told Wired. "Consumers need to feel comfortable sharing information or they won't share it."