

# *Facebook Locations, inbreuk op privacy of niet?*

Een onderzoek naar informational privacy  
binnen Facebook

<b>Naam:</b>	Raema Letwory
<b>Studentnummer:</b>	3354539
<b>Blok;</b>	3
<b>Studiejaar;</b>	2011/2012
<b>Datum;</b>	21-05-2012
<b>Begeleider;</b>	Michiel de Lange
<b>Onderdeel;</b>	Eindwerkstuk Herkansing
<b>Thema;</b>	Urbane technologieën

## Inhoudsopgave

1. Inleiding.....	3
2. Theorieën over privacy.....	4
Informational privacy .....	4
Relevantie .....	5
3. Analyse.....	7
Location Based Services .....	7
Beschrijving casus.....	8
Facebook en het gebruikersprofiel.....	9
Facebook op de beurs .....	11
4. Conclusie .....	12
5. Discussie.....	13
Literatuur .....	14

## 1. Inleiding

De verdediger van digitale burgerrechten Bits of Freedom heeft onlangs Facebook uitgeroepen als winnaar van de Big Brother Award 2011. Facebook is als bedrijf genomineerd omdat zij ondanks herhaaldelijke missers op privacygebied toch met de gegevens van gebruikers naar de beurs gaan (Van der Kroft, 2012). Facebook is daarmee betrokken bij discussies over privacy binnen moderne media. Maar hoe gaat Facebook om met privacy en wat voor invloed heeft dat op de gebruikers? Om deze vraag te beantwoorden kijken we naar een aantal nieuwe functies binnen Facebook die te maken hebben met locatie. In december 2011 werd Locatiedeeldienst Gowalla overgenomen door Facebook. In Gowalla konden bijvoorbeeld locaties toegevoegd worden aan foto's en was er de mogelijkheid op verschillende plaatsen in te checken. Daarbij zou het voormalig personeel van Gowalla werken aan de Facebook Timeline functionaliteit. De bedoeling was dat Facebook daarmee meer functies voor het delen van locaties kon implementeren (Miltenburg, 2011). Sinds de invoering van de Facebook Timeline zijn er al meer locatiemogelijkheden bijgekomen binnen verschillende facetten van Facebook (Van Hoek, 2012). Hoe er met deze nieuwe mogelijkheden wordt omgegaan door Facebook is van belang voor de invulling van privacy. Dit is omdat de implementatie van nieuwe technologie recente ontwikkelingen blootlegt binnen de structuur van Facebook, en daarmee ook indirect weergeeft hoe Facebook invulling geeft aan privacy. Wanneer het begrip privacy aan bod komt, moet er eerst worden nagedacht over wat het begrip inhoud. Er worden ook veel verschillende begrippen van privacy gehanteerd binnen de nieuwe media. Het begrip van privacy dat hier aan bod komt is *informational privacy*, waarin privacy wordt gezien als het hebben van controle of de mogelijkheid controle uit te oefenen op persoonlijke informatie (Himma & Tavani, 2008). Dit begrip zal in het theoretische kader geoperationaliseerd worden. Vanuit theorieën over *informational privacy* kijken we naar Facebook en of deze de privacy van de gebruikers waarborgt. Daarbij ligt de focus op de *location based* functies die Facebook recent heeft ingevoerd. Eerst wordt uitgelegd hoe *location based services* werken en hoe deze gegevens verzamelen. Vervolgens kijken we naar wat Facebook doet met deze gegevens en wat daarvan de consequenties zijn voor de gebruikers. De manier waarop Facebook omgaat met de specifieke locatiegegevens van gebruikers geeft weer hoe het met de privacy van Facebook gesteld is. De vraag daarbij is dan ook: *Op welke manier gaat Facebook om met de informational privacy van de gebruiker met betrekking tot de recent geïmplementeerde location based services en welke gevolgen heeft dit voor de gebruiker?* Het uitgangspunt daarbij is dat de gegevensopslag bij *location based services* gevoelige informatie over een gebruiker opslaan. Daarbij is het belangrijk voor dezelfde gebruiker om te weten welke invulling Facebook van privacy geeft. Dit heeft namelijk gevolgen voor het gevoel van veiligheid door de gebruiker.

## 2. Theorieën over privacy

### Informational privacy

Sinds de komst van nieuwe media zijn wetenschappers al bezig met privacy en verantwoordelijkheid. Dit heeft te maken met het feit dat nieuwe technologieën kwesties over individuele vrijheid veranderen en problematiseren. Voornamelijk het internet, waarbij veelal gegevens publiekelijk worden vrijgegeven en opgeslagen, roept discussie op over vrijheid van informatie en de bescherming van het individu. Daarbij is het de vraag wiens verantwoordelijkheid het is om individuele bewegingsvrijheid te waarborgen. Of het de verantwoordelijkheid is van de individuele gebruiker, die van de overheid, of die van de makers en hoe deze is geconstrueerd is daarbij van belang, omdat dit zaken zijn die de discussie over privacy vormgeven (Verbeek, 2009). Privacy is hierdoor ook een begrip dat vele betekenissen heeft. Verschillende partijen hanteren een verschillend begrip van privacy. Hier wordt er echter specifiek gefocust op *informational privacy*. *Informational privacy* heeft effect op persoonlijke data die zowel opgeslagen als gecommuniceerd wordt tussen verschillende partijen door middel van e-mail, telefoon, en draadloze communicatiesystemen (Himma & Tavani, 2008).

Er zijn drie hoofdtheorieën binnen de *informational privacy* theorie te vinden. Ten eerste is er de *Restricted Acces Theory* waarbij een persoon privacy heeft wanneer deze in staat is om toegang van anderen tot zijn of haar gegevens te beperken (Himma & Tavani, 2008). Een probleem bij deze theorie is dat de rol van degene die controle uitoefent op de informatie onderschat wordt. Er wordt vanuit gegaan dat de gebruiker privacy heeft wanneer deze zijn gegevens afgeschermd heeft voor de buitenwereld. Daarbij wordt er voorbijgegaan aan het feit dat de gebruiker zelf gevoelige informatie vrijgeeft.

Ten tweede is er de *control theory* waarbij iemands privacy direct gelinkt is aan de controle die deze persoon heeft over de informatie die hij vrijgeeft. Problemen daarbij zijn als eerst dat er geen onderscheid wordt gemaakt in de mate van controle die de gebruiker heeft en ten tweede is dat er geen rekening wordt gehouden met over welke informatie controle moet plaatsvinden (Himma & Tavani, 2008). De mate van controle wordt hier bepaald door de manier waarop de interface het mogelijk maakt om controle uit te oefenen. Dit ligt vast in de privacyinstellingen. Ook kunnen niet alle soorten informatie geheim gehouden worden. Bij het gebruik maken van Facebook kan een gebruiker wel alle gegevens afschermen voor anderen, maar er wordt wel bekend gemaakt dat je een profiel hebt.

Ten derde is er de *Restricted Acces/Limited Control Theory* die hier zal worden afgekort als de RALC Theory. Hierbij wordt er onderscheid gemaakt tussen het concept privacy en het beheer

van privacy. Het concept definieert zich in termen van beperkte toegang tot gegevens, en het beheer houdt zich bezig met het opstellen van grenzen om beperkte controle voor individuen te bewerkstelligen. Binnen deze theorie wordt privacy gedefinieerd binnen specifieke situaties in verband met andere partijen. Bij deze theorie is het belangrijk om zones op te stellen die zorgen dat de gebruikers om anderen te beperken om bij persoonlijke informatie te komen. Zo hoeft de gebruiker geen volledige controle te hebben, maar moet deze wel de mogelijkheid hebben gegevens voor andere partijen af te schermen (Himma & Tavani, 2008). Binnen sociale media zorgen de sites voor een aantal privacy beschermende maatregelen.

Norman Mooradian (2009) vindt echter dat de architectuur van deze sites gebruikers een vals gevoel van veiligheid geeft. De meeste gebruikers zouden zich namelijk niet bewust zijn van het feit dat hun gegevens bewaard worden op de servers van het bedrijf, in dit geval Facebook. De meeste van deze sites worden beheerd door bedrijven waarbij het businessmodel is gebaseerd op het verzamelen van informatie voor marketing doeleinden. Mooradian stelt daarbij dat de meeste gebruikers naïef zijn en denken dat hun informatiestromen beperkt blijven tot de omgeving van de site (Mooradian, 2009, p.168).

## **Relevantie**

Binnen de RALC theorie bestaat een onderscheid tussen natuurlijke privacy en normatieve privacy. Kenmerken voor dit onderscheid is het verschil tussen privésituaties waarin privacy nagenoeg vanzelfsprekend is en openbare situaties die beschermd zijn door regels en wetten waarin inbreuk kan worden gemaakt op de privacy van een individu. In de normatieve vorm is er controle nodig over de gegevens van individu die bewerkstelligd wordt door keuze, toestemming en correctie. Deze zijn ook weer context afhankelijk (Himma & Tavani, 2008). Op Facebook vindt er een vorm van normatieve privacy plaats. Facebook bezit namelijk informatie van zijn gebruikers. De gebruikers hebben daarbij controle over de gegevens die ze vrijgeven. Dit is echter alleen in beperkte mate mogelijk. Om lid te worden van Facebook moet je eerst een profiel aanmaken. Daarvoor is het vereist bepaalde informatie vrij te geven, zoals een geboortedatum. Hiermee geeft de nieuwe gebruiker Facebook toestemming om deze gegevens op te slaan en eventueel te gebruiken. Deze gegevens kunnen daarbij wel ingezien worden door de gebruiker zelf. In hoeverre heeft de gebruiker dan controle over wat Facebook met deze gegevens doet? En wanneer is de privacy van de gebruiker dan geschonden?

De procedures die worden gebruikt door de informatie industrie voor het verzamelen en gebruiken van persoonlijke informatie bepalen of individuele privacy is geschonden (Gindin, 1997. p.13). Hiervoor zijn stappen voor ondernomen binnen de bedrijven. Facebook doet dit in de vorm

van privacyinstellingen. Facebook geeft daarbij aan dat zij alleen gegevens gebruiken wanneer de gebruiker daar toestemming voor heeft gegeven. Het businessmodel van Facebook stelt dat gegevens van gebruikers verwerkt mogen worden voor commerciële doeleinden onder voorbehoud van persoonlijke privacyinstellingen van de gebruiker (Facebook beleid inzake gegevensgebruik, 2011 ). En toch geven Facebook gebruikers veel informatie vrij op de site. Is dat naïviteit van de gebruiker of is deze simpelweg niet op de hoogte van dit gegeven? De zoals Mooradian (2009) voorgestelde naïviteit ligt juist in die onwetendheid. De privacyinstellingen van Facebook misleiden in dit geval de gebruikers. De privacyinstellingen gelden namelijk alleen voor informatie van en tussen gebruikers. Deze zorgen ervoor dat informatie van de ene gebruiker wel of niet te zien is voor de andere gebruikers. Het heeft niets te maken met de informatie die Facebook over de gebruikers verzameld. Wat dat betreft kunnen de gebruikers meer inzicht gebruiken in de structuur van Facebook met betrekking tot het gebruik van persoonlijke informatie van de gebruiker. De gebruikers voelen zich veilig vanwege de privacyinstellingen die Facebook hanteert. Als gebruikers zich veilig achten, zullen zij zich minder druk maken over wat er met hun gegevens gebeurt. Gebruikers passen zich aan de structuur van het medium aan, zodat ze alleen informatie vrijgeven aan de gebruikers die ze willen (Boyd, 2008). Inzicht in de structuur van Facebook is dus nodig. Vooral nu er nieuwe functionaliteiten worden toegepast waarin gebruikers gegevens over hun locatie vrijgeven. Elke keer als Facebook een nieuwe functie implementeert veranderen de privacyinstellingen. Dit is te zien in de beschrijving van de casus. Deze privacyinstellingen staan daarbij automatisch op 'standaard'. Binnen deze standaard zijn gegevens toegankelijk voor alle gebruikers. Er is dus de noodzaak om deze eerst aan te passen voordat je begint met het actief gebruiken van een nieuwe functie. Hierdoor wordt het belangrijk om de gebruiker op de hoogte te houden van de implicaties voor hun privacy wanneer nieuwe functies worden aangeboden.

In de analyse komen deze functionaliteiten terug onder de naam *location based services*. Eerst wordt beschreven wat *location based services* zijn en hoe deze werkzaam zijn op Facebook. Vervolgens zal ik me bezig houden met de manier waarop Facebook de privacy van de gebruikers probeert te bewerkstelligen. Dit zal geplaatst worden in de theorieën over informational privacy om te zien hoe Facebook privacy ziet. Dit heeft natuurlijk gevolgen voor de gebruikers. De gebruikers zijn immers degene die zich aanmelden om gebruik te maken van de services van Facebook. Het is voor de gebruiker dan ook van belang om te weten hoe hun gegevens worden gebruikt en welke aannames daar aan ten grondslag liggen om veilig gebruik te kunnen maken van Facebook.

### 3. Analyse

#### Location Based Services

Er zijn verschillende soorten *location based services* (LBS). Er zijn daarbij *person-oriented LBS* en *device-oriented LBS*. *Person-oriented services* richten zich op het positioneren van een persoon, zoals een applicatie die vrienden zoekt. Meestal kan de gelokaliseerde persoon enige controle uitoefenen op de service. *Device-oriented services* staan los van de gebruiker, zoals een GPS-tracker in een voertuig ten behoeve van diefstalpreventie. Deze kunnen ook gericht zijn op een persoon, maar kan vooral gebruikt worden om een object of een groep mensen te traceren. Op deze service kan meestal geen controle worden uitgeoefend. Naast deze classificatie worden er ook twee type constructies onderscheiden, namelijk *push* en *pull services*. *Push services* impliceren dat de gebruiker informatie ontvangt, ten gevolge van de plaats waar deze zich bevindt, zonder de informatie zelf te hebben opgevraagd. Deze informatie kan naar de gebruiker gestuurd worden wanneer deze vooraf toestemming heeft gegeven als onderdeel van een abonnement of zonder expliciete toestemming zoals reclame. *Pull services* geven aan dat de gebruiker wel actief op zoek moet naar informatie. Deze informatie kan locatie versterkend werken, zoals bij het vinden van een pinautomaat (Schiller & Voisard, 2004).

De LBS binnen Facebook vallen onder de noemer *person-oriented services*, omdat Facebook erop gericht is personen met elkaar in contact te brengen. De gebruiker vult op Facebook zelf zijn positie in, in een daarvoor bestemd vakje. De gebruiker die gepositioneerd wordt is daarbij zelf verantwoordelijk voor zijn positionering. Dit gegeven kan op elk tijdstip toegevoegd of verwijderd worden, waarmee de gebruiker volledige controle heeft. De gebruiker ontvangt op zijn profiel de gegevens van zijn locatie. Ook de vrienden van deze gebruiker krijgen dit gegeven te zien. In dat opzicht is het een *push service*, op het profiel worden immers meteen deze gegevens weergegeven. Tegelijkertijd kan de gebruiker binnen Facebook op zoek gaan naar informatie over deze locatie, Facebook heeft namelijk informatie verzameld over deze locatie en toont deze op een aparte pagina. Dit maakt de extra informatie over de locatie een *pull service*. Niet alleen de gebruiker zelf, maar ook andere gebruikers kunnen informatie opzoeken over de locatie die is vrijgegeven. Dus voor informatie moet de gebruiker wel specifiek op zoek. Hierdoor vallen de Facebook LBS onder *pull services*.

Dit is vanuit het standpunt van de gebruiker gezien. Waar deze onderhevig is aan de privacyinstellingen, gaat Facebook als bedrijf heel anders met de locatiegegevens om. Facebook krijgt deze gegevens aangeleverd van de gebruikers, waarnaar deze gegevens opgeslagen worden. Zodra de gebruiker toestemming geeft of heeft gegeven, worden deze gegevens doorgespeeld.

Vanaf de kant van Facebook is het een *push service*. Het verschil in deze is van belang, vanwege de informatiestromen die worden gegenereerd door middel van de architectuur van Facebook. Enerzijds gaat er een informatiestroom naar andere gebruikers, anderzijds is er een informatiestroom richting Facebook en zijn adverteerders. Zoals eerder is gezegd heeft de architectuur van een site als Facebook gevolgen voor het gevoel van veiligheid voor de gebruiker (Boyd, 2008).

### **Beschrijving casus**

Voorheen was het zo dat je bij Facebook een smartphone nodig had om in te loggen op een bepaalde locatie. Met de Places functie kon de gebruiker 'inchecken' op een bepaalde locatie, waardoor andere gebruikers kunnen zien waar deze ene gebruiker zich bevindt. Een nieuwe functionaliteit van Facebook maakt het nu mogelijk om aan alle posts een locatie toe te voegen. Daarbij is geen smartphone meer nodig (Facebook blog, 2012). Mogelijkheden om een locatie te delen zijn; waar je bent geweest, waar je nu bent, en waar je naartoe gaat. Dit houdt in dat je locatie kunt toevoegen aan geplaatste foto's, je kunt bij elke post een locatie toevoegen zodat men weet waar je bent, en je kunt jezelf inchecken op plaatsen waar je vrienden zijn geweest of waar je naartoe gaat. Er zijn twee manieren om een locatie toe te voegen. Ten eerste kun je op de locatieknop klikken waarmee er een door jou gekozen standaard locatie toegevoegd wordt aan al je posts. Hiervoor kun je een plaatsnaam of gebied invullen. Op basis daarvan bepaald Facebook waar jij je bevindt. Elke keer dat een gebruiker post verschijnen er ook locatiegegevens zolang deze optie is ingeschakeld. Ten tweede kun je een specifieke locatie toevoegen aan een eerdere post (Facebook beleid inzake gegevensgebruik, 2012). Om een specifieke locatie toe te voegen kan je klikken op een pictogram dat zich onder het invoerkader bevindt. Hierbij kan je een plaats of een evenement invullen. Daarbij kan je ook vrienden toevoegen aan deze locatie. Vrienden kunnen jou ook toevoegen aan een plaats of evenement. Wanneer je toegevoegd bent door je vrienden wordt dit ook zichtbaar in je eigen tijdlijn.

Als gebruiker kun je zelf bepalen wie jou locatiegegevens ziet en wie jou toe kan voegen. Daar zijn twee manieren voor. Ten eerste kun je via je privacyinstellingen instellen wie jouw algemene gegevens en tevens locatiegegevens kan zien, alleen je vrienden, vrienden en vrienden van vrienden, of iedereen. Deze instellingen worden dan de standaard voor op je profiel. Daarnaast kun je een controle inschakelen voor je profiel. Dit gebeurt ook via de algemene privacyinstellingen. Als deze instelling is uitgeschakeld worden alle tags meteen goedgekeurd. Een locatie tag kan ook gewoon door de gebruiker verwijderd worden (Facebook beleid inzake

gegevensgebruik, 2012). Deze privacyinstellingen zijn standaard totdat de gebruiker deze instellingen specificeert.

Het volgende deel gaat in op de informatiestromen van de vrijgegeven locatiegegevens. Daarbij wordt duidelijk gemaakt hoe gegevens worden opgeslagen en de mate van controle die de gebruiker daarop kan uitoefenen. De vraag daarbij is of de gebruikers dan nog *informational privacy* hebben. Deze informatiestromen kunnen inzicht geven in hoe privacy werkt binnen Facebook en welke aannames te grondslag liggen aan het privacybeleid.

### **Facebook en het gebruikersprofiel**

De vraag is wat er gebeurt met locatiegegevens wanneer een gebruiker deze vrijgeeft. Facebook slaat deze gegevens op. Dit is onderdeel van de algemene voorwaarden waaronder een gebruiker gebruik mag maken van Facebook. Facebook is dus te allen tijde gemachtigd om gegevens op te slaan. In ruil daarvoor kan de gebruiker aan zijn vrienden bekend maken waar hij zich bevindt. Deze gegevens komen in zijn of haar profiel te staan. De gebruiker is daarbij gemachtigd om deze gegevens te verwijderen. Facebook heeft deze gegevens echter al opgeslagen. Wanneer een gebruiker gebruik wil maken van een applicatie kan deze app vragen of de gebruiker akkoord gaat met de verwerking van zijn locatiegegevens. Dit is onderdeel van de algemene voorwaarden voor het gebruik van een dergelijke app. In ruil voor het gebruik van de app, geeft de gebruiker inzicht in zijn locatiegegevens. Wat er met deze gegevens gebeurd is nu uit handen van de gebruiker. In feite heeft de gebruiker nu zijn gegevens verkocht aan een derde, welke zal bestaan uit een bedrijf met een contract met Facebook. De gebruiker heeft daarbij wel controle of deze locatiegegevens wil delen of niet. Ook kan de gebruiker controle uitoefenen op welke andere gebruikers deze gegevens zien. Dit kan door middel van het instellen van de standaard privacyinstellingen van het gebruikersprofiel. Wanneer de gebruiker echter toestemming geeft om zijn gegevens te gebruiken, heeft de gebruiker daar geen controle meer over. Om deze gegevens te gebruiken moet de gebruiker wel expliciet zijn toestemming hebben gegeven. Zo heeft de gebruiker controle over het vrijgeven van zijn gegevens, niet over wat er vervolgens met die gegevens gebeurt. De gebruiker heeft dus *informational privacy* totdat deze de gegevens besluit uit handen te geven. Facebook heeft daarbij wel maatregelen genomen om de gebruiker op de gang van zaken te attenderen. Volgens de RALC theorie is dit voldoende om de *informational privacy* te waarborgen.

Daarnaast bepaald Facebook in welke omgeving de gebruiker zich bevindt. Wanneer Facebook bijvoorbeeld GPS gegevens ontvangt worden deze gecombineerd met andere locatiegegevens die Facebook over je heeft. Facebook combineert daarbij alle locatiegegevens die

bekend zijn van jou en je vrienden om gericht *services* aan te bieden. Ook ontvangt Facebook gegevens van het type apparaat dat je gebruikt om Facebook te openen. Locatie en GPS coördinaten zijn gegevens die ze daarbij ontvangen. Deze gegevens gebruiken ze om te bepalen of er vrienden in de buurt zijn. Facebook ontvangt in feite alles wat een gebruiker doet, op welk tijdstip, op welk apparaat, op welke locatie (Facebook beleid inzake gegevensgebruik, 2012). Deze gegevens worden gebruikt om de *services* van Facebook gericht te maken. Facebook stelt daarbij dat de gebruiker de eigenaar blijft van zijn gegevens, en dat Facebook alleen gegevens gebruikt als ze daar toestemming voor hebben gekregen of je daarvan op de hoogte te hebben gesteld of wanneer je gegeven zijn geanonimiseerd (Facebook beleid inzake gegevensgebruik, 2012). Facebook geeft daarmee aan dat de gebruiker niet expliciet toestemming hoeft te geven voor het gebruik van zijn gegevens. In hoeverre hebben de gebruikers dan nog controle over hun gegevens? Het op de hoogte stellen van de gebruikers over mogelijke gevolgen voor privacy wordt gedaan middels het privacybeleid. Er wordt dus van de gebruiker verwacht dat deze op de hoogte is van het privacybeleid binnen Facebook om controle uit te kunnen oefenen op hun gegevens. Daarbij kunnen ze hun gegevens wel afschermen voor andere gebruikers, maar niet voor Facebook zelf. De gebruikers hebben hier controle over welke informatie met betrekking tot locatie ze plaatsen, dit is immers geen vereiste. Zo kan de gebruiker bepalen welke informatie deze vrij wil geven. In deze zin is er sprake van privacy binnen de *restricted acces theory*. Daarnaast hebben de gebruikers controle over wie deze gegevens mag zien. Volgens de *control theory* is er ook sprake van privacy. Binnen de RALC theory ligt de privacy van de gebruiker complexer. Aan de ene kant is er het controle deel. Hierin wordt Facebook verantwoordelijk gehouden om de gegevens van de gebruiker af te schermen voor anderen. Facebook doet dit op dezelfde wijze in omgang met andere bedrijven door de gegevens van de gebruiker te anonimiseren. Dit valt echter niet binnen het onder controle houden van de informatiestroom van de gebruikers. Hier bevinden we ons in het beheer van de informatie. Facebook heeft wel het privacybeleid om de gebruikers op de hoogte te houden van informatiestromen. Nog steeds hebben de gebruikers hun *informational privacy*.

Vrienden kunnen ook locatiegegevens toevoegen aan posts van een gebruiker. Meestal gebeurt dit door middel van het zogenoemde taggen. Hiermee kunnen gebruikers een andere gebruiker aanduiden door hun gebruikersnaam in te vullen bij een post. Een tag is in feite een verbinding naar het profiel bijbehorende de gebruikersnaam. Het probleem hierbij is dat andere gebruikers wel een ongevraagd gevoelige informatie kunnen delen. Facebook heeft dit proberen op te lossen door twee verschillende controlemaatregelen te implementeren. Dit kan via de standaardinstellingen of door een individuele controlemogelijkheid in te stellen. Binnen de

standaardinstellingen kan een gebruiker bepalen welke andere gebruikers deze informatie kunnen delen, en welke gebruikers dit kunnen zien. Via de privacyinstellingen kan de gebruiker ook een optie inschakelen waarmee de getagde berichten van andere gebruikers eerst goedgekeurd moeten worden voordat ze zichtbaar worden. Zodra deze gegevens zichtbaar worden kan Facebook deze gegevens gebruiken om jou en je vrienden in verband te brengen. Zo kunnen andere gebruikers zien wie vrienden van jou zijn. Tegelijkertijd kunnen de vrienden van je vrienden ook zien dat jij daar bent geweest. Op deze manier heeft de gebruiker geen controle over welke informatie er over hun wordt vrijgegeven. Binnen de *restricted access theory* kan er op deze manier geen sprake van privacy zijn. De gebruiker heeft echter wel volledige controle over wat er vervolgens met deze gegevens gebeurt ten opzichte van andere gebruikers. In deze specifieke situatie heeft Facebook ervoor gezorgd dat gebruikers wel altijd zelf kunnen beslissen welke informatie ze vrij geven, ongeacht welke gebruiker deze informatie post. Facebook heeft deze gegevens echter al in bezit. Hier heeft Facebook er echter al voor gezorgd dat er specifieke maatregelen te nemen zijn om deze locatiegegevens af te schermen voor andere gebruikers. In die zin is binnen de RALC theorie de privacy van de gebruiker gewaarborgd.

### **Facebook op de beurs**

Wat zijn dan de gevolgen voor de gebruiker wanneer Facebook een beursgenoteerd bedrijf is? Op de aandelenbeurs kunnen mensen en bedrijven aandelen kopen in Facebook. Op deze manier kunnen aandeelhouders advertenties plaatsen op Facebook. De gebruiker ondervindt hier de gevolgen van. Er wordt namelijk gespeculeerd over de stijging van advertenties door aandeelhouders (Zantingh, 2012). Dit ligt in het idee dat de aandeelhouders elk jaar meer winst willen zien. Daarbij zijn op de dag van de beursgang de hooggespannen verwachtingen van Facebook niet uitgekomen, de koers verliep moeizaam. Daarnaast is het zo dat Facebook nog steeds voor 80% afhankelijk is van advertenties. Mocht het zo zijn dat de aandelen van Facebook geen winst opleveren, zal Facebook de advertenties moeten opschroeven (Reijnders, 2012). Eerder is naar voren gekomen dat Facebook allerlei informatie van gebruikers verzameld om gericht advertenties te tonen. Deze zijn echter nog niet optimaal ingezet, mobiele advertenties zijn namelijk nog niet mogelijk. Op deze manier zou Facebook nog meer gegevens kunnen doorspelen om deze advertenties aan te passen op de Facebook gebruiker. Meer bedrijven hebben dan de toegang tot jouw geanonimiseerde persoonsgegevens. De gebruikers van Facebook moeten hier rekening mee houden willen ze hun gegevens optimaal beschermen.

## 4. Conclusie

Facebook illustreert met de manier van omgang met *location based services* en de opslag en verwerking van deze gegevens dat privacy geen eenvoudig begrip is binnen het medium. Er is namelijk veel informatie te vinden over privacy ten opzichte van andere gebruikers. Dit staat onder het kopje 'privacy' in het Facebook reglement. Wanneer je echter wil weten hoe het zit met privacy vanuit Facebook met betrekking tot je gegevens is dit te vinden onder het beleid inzake gegevensgebruik. Zoals we hebben gezien blijft privacy niet alleen beperkt tot gebruikers onderling. Het privacybeleid heeft wat dat betreft een gebrek aan transparantie binnen het beleid. De gebruiker moet dus extra moeite doen, wil hij of zij op de hoogte zijn van wat Facebook heeft geregeld met betrekking tot privacy. Daarnaast wordt het begrip privacy door Facebook wel gebruikt, maar wordt er nergens expliciet vastgesteld hoe Facebook er invulling aan geeft. Wat Facebook verstaat onder privacy hoeft niet hetzelfde zijn als wat de gebruikers verstaan onder privacy (Boyd, 2008).

Er is hier sprake van een privacyparadox. Hierbij wisselen gebruikers gegevens uit onder elkaar om hun sociale banden aan te halen. Tegelijkertijd wordt deze informatie verzameld en doorgespeeld naar bedrijven en aan andere instanties. Om deze paradox op te lossen binnen sociale media is bewustzijn belangrijk (Barnes, 2006). Een besef van wat er precies met je gebruiksgegevens gebeurd is dus belangrijk in het bestrijden van kwesties met betrekking tot privacy. Facebook geeft aan dat de gebruikers zelf verantwoordelijk zijn voor hun privacy op het profiel. Facebook heeft namelijk de privacyinstellingen standaard op 'iedereen' staan waarbij geposte gegevens voor alle gebruikers zichtbaar zijn tenzij de gebruiker dit veranderd. Facebook omzeilt zo volledig besef van wat er met gebruikersgegevens gebeurd door het privacybeleid ondoorzichtig te maken, waardoor het een hele klus is om te weten hoe het werkt. Daarbij zijn de meeste gebruikers naïef om te denken dat de privacyinstellingen beschermen tegen het gebruik van gegevens door het bedrijf zelf (Mooradian, 2009). Daarnaast is het doel van de sociale media gebruikers om gegevens te delen met anderen. Dat maakt het heel lastig om te bepalen waar de grens ligt van het hebben van privacy en het schenden ervan. Facebook heeft met het beleid en de privacyinstellingen voor *informational privacy* gezorgd. Er zijn echter zaken die dit compliceren voor de gebruiker. Dit ligt vooral in het gebrek aan transparantie in het beleid. Om *informational privacy* te hebben moeten de gebruikers op de hoogte zijn van het beleid willen ze bewuste keuzes maken om hun gegevens te beschermen. Bewustzijn kenmerkt een zekere controle over de informatiestroom aan gegevens. Daarnaast worden deze zaken complexer wanneer een meer nieuwe LBS geïmplementeerd worden. Hiervoor moeten namelijk weer nieuwe

privacyoverwegingen gedaan worden vanuit Facebook. De gebruiker moet deze dan weer in gebruik nemen, wat de transparantie van het beleid niet bevordert.

## 5. Discussie

Wanneer er een discussie woedt over privacy is het maar de vraag hoe de verschillende partijen privacy interpreteren. In dit paper heb ik gekozen voor *informational privacy*, omdat dit zich specifiek concentreert op informatie-uitwisseling. Daarbij wordt voorbijgegaan aan de aannames die de verschillende partijen, gebruikers en Facebook zelf, hebben over privacy. Om een compleet beeld te schetsen over privacy binnen Facebook is het daarom nodig om een onderzoek te houden onder de gebruikers om te duiden hoe deze privacy op Facebook ervaren. De ervaring van privacy ligt namelijk bij het gevoel dat de gebruiker heeft bij de mate van veiligheid bij zijn gegevens. Ook Facebook moet nader bekeken worden, omdat naar voren is gekomen dat de betekenis van privacy niet expliciet genoemd wordt. Dit kan opgehelderd worden door middel van een discoursanalyse van Facebook privacyschandalen in de media.

De gang naar de beurs zorgt ook voor nieuwe ontwikkelingen rond het gegevensgebruik van Facebook. Er wordt al gespeculeerd over het transparant maken van Facebook met betrekking tot het privacybeleid. Investeerders zouden namelijk niet zitten te wachten op een privacyschandaal (Zantingh, 2012). Het is nu nog te vroeg om er iets over te zeggen, maar dit gaat zeker gevolgen hebben voor de manier waarop gebruikers hun privacy gaan zien.

## Literatuur

- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9).
- Boyd, D. (2008). 'Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence', *Convergence* 14, 13-20.
- Facebook beleid inzake gegevensgebruik. (2011). Bekeken op: 16-05-2012.  
<https://www.facebook.com/about/privacy/>
- Facebook blog. (2012). Bekeken op: 16-05-2012.  
<https://blog.facebook.com/blog.php?post=10150251867797131>
- Gindin, S. (1997). *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*. San Diego, San Diego Law Review.
- Himma, K. E., & Tavani, H. T. (Eds.). (2008). *The handbook of information and computer ethics*. Hoboken, NJ: Wiley
- Hoek, Van C. (2012, maart 12). Locatiedienst Gowalla 3 maanden na overname Facebook offline. Gehaald van: <http://www.nu.nl/internet/2761189/locatiedienst-gowalla-3-maanden-overname-facebook-offline.html>
- Kroft, Van der D. (2012, maart 8). Winnaars Big Brother Awards bekend. Gehaald van: <https://www.bof.nl/2012/03/08/winnaars-big-brother-awards-bekend/>
- Miltenberg, O. (2011, december 3). Facebook heeft locatiedeeldienst Gowalla overgenomen. Gehaald van: <http://tweakers.net/nieuws/78517/facebook-heeft-locatiedeeldienst-gowalla-overgenomen.html>
- Mooradian, N. (2009) 'The Importance of Privacy Revisited', *Ethics and Information Technology* 11: 163-174.
- Reijnders, M. (2012, mei 18). Beursgang Facebook slecht voor iedereen. Gehaald van: <http://www.bright.nl/beursgang-facebook-slecht-voor-iedereen>
- Schiller, J. & Voisard, A. (2004). *Location-Based Services*. San Fransisco, Morgan Kaufmann Publishers.
- Verbeek, P. P. (2009). *Leven als bouw pakket. Ethisch verkennen van een nieuwe technologische golf*, 48 - 73. Kampen: Uitgeverij Klement.
- Zantingh, P. (2012, mei 18). Facebook gaat vandaag naar de beurs. Wat gaat het alle partijen opleveren? Gehaald van: <http://www.nrc.nl/nieuws/2012/05/18/facebook-gaat-vandaag-naar-de-beurs-en-dan/>