MARIKE VERSCHOORE DE LA HOUSSAIJE

SOCIALE NETWERKSITES: PRIVACYVRIENDELIJK?

HOE GEBRUIKERS VAN SOCIALE NETWERKSITES HUN PRIVACY BELEVEN EN AANBIEDERS HIEROP INSPELEN

2007/2008

MASTERTHESIS MEDIA & JOURNALISTIEK

BEGELEIDER: MIJKE SLOT MA

AUGUSTUS 2008

SOCIALE NETWERKSITES: PRIVACYVRIENDELIJK?

HOE GEBRUIKERS VAN SOCIALE NETWERKSITES HUN PRIVACY BELEVEN EN AANBIEDERS HIEROP INSPELEN

MARIKE VERSCHOORE DE LA HOUSSAIJE

STUDENTENNUMMER: 307082

VERSCHOOREMARIKE@HOTMAIL.COM

2007/2008

MASTERTHESIS MEDIA & JOURNALISTIEK

MEDIA ALS CULTURELE INDUSTRIE

FACULTEIT DER HISTORISCHE EN KUNSTWETENSCHAPPEN

ERASMUS UNIVERSITEIT ROTTERDAM

TNO ICT

BEGELEIDER: MIJKE SLOT MA

TWEEDE BEGELEIDER: LINDA KOOL MA

TWEEDE LEZER: PROF. DR. SUSANNE JANSSEN

VOORWOORD

Na in totaal 6 jaar studie, waarvan vier jaar bij Inholland en twee jaar aan de Erasmus Universiteit, komt nu het einde van mijn studietijd in zicht. Deze masterthesis is daarvan het bewijs. Het afgelopen half jaar heb ik met veel plezier aan deze thesis gewerkt. Voor het grootste gedeelte van mijn tijd heb ik deze scriptie geschreven op het kantoor van TNO ICT in Delft.

Het waren zes leuke maanden bij TNO en hoewel ik mijn scriptie toch echt alleen moest schrijven, was het een gezellige tijd samen met de collega's. Ik wil hen daarom bedanken voor alle gezelligheid en de interesse in mijn scriptievorderingen. Bovendien wil ik Linda bedanken voor haar literatuuradviezen en vooral inhoudelijke commentaar op mijn thesis. Ik vond het erg leerzaam en bovendien erg leuk om mee te draaien in het project over User Generated Privacy. Ook Mijke Slot, mijn scriptiebegeleider, wil ik bij deze graag bedanken voor haar commentaar. Bij het schrijven van het theoretisch hoofdstuk liep ik op een gegeven moment even vast en Mijke kon mij weer op het goede spoor helpen door even afstand te nemen van alles wat tot dan toe op papier stond. Bovendien wil ik haar bedanken voor de geweldige kans om bij TNO ICT stage te lopen en voor het aandragen van het scriptieonderwerp wat helemaal aansloot bij mijn bachelorscriptie. Ik vond het een mooie uitdaging om verder de diepte in te gaan op het onderwerp privacy in relatie tot sociale netwerksites, waarbij ruim voldoende mogelijkheden over bleven om mijn eigen draai er aan te geven.

Naast mijn stagebegeleidster en scriptiebegeleidster wil ik ook mijn vriend Dustin van Horik bedanken. Super bedankt dat je mee wilde helpen bij de focusgroepgesprekken en het maken van aantekeningen, waardoor ik me kon focussen op het gesprek zelf. Bovendien kon ik zeker wat met je commentaar op de eerste versie van mijn thesis. Ook mijn vader, Ton Verschoore de la Houssaije, wil ik bedanken voor het lezen van mijn scriptie en het voorzien van vooral redactioneel commentaar. Tot slot wil ik bij deze graag mijn ouders bedanken voor de mogelijkheid die zij mij hebben geboden om maar liefst zes jaar lang te studeren. Het was een supertijd, maar nu is het toch echt tijd om deze af te sluiten en te gaan werken.

Marike Verschoore de la Houssaije,
Rotterdam, augustus 2008

SAMENVATTING

Zowel privacy als sociale netwerksites zijn op dit moment in onze maatschappij onderwerp van gesprek. Daarbij wordt vaak een negatieve invalshoek gekozen. Ook onderzoek naar privacy binnen sociale netwerksites richt zich vooral op mogelijke risico's en gevaren. Het gebruikersperspectief wordt daarin niet tot nauwelijks meegenomen. In dit onderzoek wordt het gebruikersperspectief juist als uitgangspunt genomen. Doelstelling van dit onderzoek was in de eerste plaats de theorie over privacy verder te (helpen) ontwikkelen door inzicht te geven in de mate van overeenstemming tussen privacybeleving en traditionele privacytheorieën. Bovendien was het formuleren van aandachtspunten op basis van onderzoek naar de verschillen tussen privacybeleving van gebruikers en privacywaarborging door aanbieders een doelstelling van dit onderzoek.

De aandacht gaat in dit onderzoek uit naar de volgende vragen: Hoe beleven gebruikers privacy in online sociale netwerken? Zijn zij bezorgd over hun privacy? En zo ja, waar ontbreekt het dan aan? Zijn aanbieders zich hier bewust van en zo ja, hoe gaan zij er dan mee om? Dit resulteert in de volgende hoofdvraag:

'Hoe beleven gebruikers van sociale netwerksites hun online privacy en in hoeverre spelen aanbieders van sociale netwerksites hierop in?'

Gekozen is om bovenstaande vraag te beantwoorden door middel van de casestudy als onderzoeksmethode. Voordat er een keuze gemaakt kon worden voor de case, is deskresearch uitgevoerd. Dit onderzoek is uitgevoerd door middel van literatuuronderzoek van drie sociale netwerksites, namelijk Myspace, Hyves en Facebook. Gekozen is om Hyves te bestuderen, aangezien Hyves in Nederland verreweg de meest populaire sociale netwerksite is en een groot draagvlak heeft onder internetgebruikers van verschillende leeftijden. Bovendien verschillen de type diensten en tools die de site aanbiedt niet wezenlijk van die van Facebook of Myspace.

Bovenstaande vraag bestaat uit twee gedeelten, die elk hun eigen subdeelvragen hebben en ook een andere methode van onderzoek tot gevolg hebben. Voor deelonderzoek 1, een onderzoek naar de waarborging van privacy door de aanbieder is een inhoudsanalyse uitgevoerd. Bovendien zijn diverse bronnen en een interview als aanvulling gebruikt. Voor deelonderzoek 2, het gebruikersonderzoek, is gebruik gemaakt van focusgroep-gesprekken als belangrijkste bron van dataverzameling. Twee focusgroepgesprekken vonden plaats, waarbij onderscheid is gemaakt naar leeftijd van respondenten. Zowel zes personen in de leeftijd van 13 tot en met 18 jaar als zes personen in de leeftijd van 24 tot en met 31 jaar deden mee aan het onderzoek.

Geconcludeerd is dat de traditionele theorieën over privacy ook in de digitale wereld nog steeds standhouden. Gebruikers van Hyves vinden zowel de ruimtelijke, relationele als de informationele dimensie belangrijk binnen Hyves. Gebruikers willen soms graag met rust gelaten worden, zitten niet altijd te wachten op bepaalde sociale contacten en willen graag controle houden over de sociale contacten. Bovendien willen de gebruikers hun

persoonlijke gegevens beschermen. Toch gaat de meeste aandacht uit naar de informationele dimensie, wat natuurlijk bij een sociale netwerksite, waarbij het delen en communiceren van informatie één van de belangrijkste zaken is, niet vreemd is.

Een tweede belangrijke conclusie is dat de 24- tot en met 31-jarigen over het algemeen een breder perspectief hanteren ten aanzien van privacy dan de 13- tot en met 18-jarigen. Dit komt tot uiting in de waarden en risico's die zij noemen. Bovendien blijken de ouderen zich vooral te richten op de buitenwereld zoals werkgevers en commerciële bedrijven, wanneer over privacy en risico's wordt gesproken, terwijl de omgeving van de jongere groep beperkt blijft tot hun vriendenkring. Waarschijnlijk heeft dit met leeftijd en interesses te maken. Bovendien is er een verschil in privacybewustzijn en privacybezorgdheid tussen en binnen verschillende leeftijdsgroepen. Bovenstaande conclusie zal, zo mag verwacht worden, ook gelden voor andere sociale netwerksites.

Tot slot kan geconcludeerd worden dat de privacywaarborging binnen Hyves voldoende is, maar dat er wel verbeterpunten zijn. Daarom zijn een aantal aandachtspunten geformuleerd voor Hyves. Ook voor gebruikers van Hyves zijn enkele aanbevelingen opgesteld. Beide zijn in onderstaand overzicht opgenomen.

Aandachtspunten voor Hyves	**Aandachtspunten voor gebruikers**
• Zorg voor transparante en open communicatie naar gebruikers.	• Let op welke gegevens je online zet en voor wie deze beschikbaar zijn.
• Verbeter en behoud de veiligheid binnen Hyves.	• Geef nooit je wachtwoord aan een ander.
• Verbeter de controle(mogelijkheden) door gebruikers.	• Lees de privacypolicy en gebruiksvoorwaarden door.

INHOUDSOPGAVE

1. INLEIDING

Je krijgt een mailtje van Hyves: 'Let's Hyve! X wil je toevoegen als vriend op Hyves. Klik hier om de uitnodiging te accepteren of te weigeren'. Je klikt op de link en accepteert de uitnodiging. Ook al ken je deze persoon niet zo goed in het echte leven, je vertrouwt hem of haar, want jouw persoonlijke informatie blijft binnen de muren van jouw persoonlijke profiel. Toch? (Riphagen, 2008:1)

1.1 Aanleiding

Zowel privacy als sociale netwerksites zijn op dit moment in onze maatschappij onderwerp van gesprek. In steeds meer domeinen wordt namelijk gebruik gemaakt van web 2.0 diensten, zoals sociale netwerksites, waarbij het uitwisselen, delen, creëren en communiceren van informatie centraal staat (Kool, 2007). Door nieuwe ontwikkelingen is de mogelijkheid om informatie op internet te plaatsen en te delen gemakkelijker geworden. Ook het publiceren van bijvoorbeeld persoonsgegevens op een website, discussieforum of in een online dagboek is gemakkelijker geworden en gebeurt sneller. Dit kan gevolgen hebben voor de privacybeleving van internetgebruikers.

Door onderzoeksbureaus worden deze ontwikkelingen vaak vanuit een negatieve invalshoek bekeken, waarbij uitsluitend oog is voor de mogelijke privacybedreigingen of risico's. Een voorbeeld van een bedreiging voor privacy is de toegankelijkheid van persoonlijke, soms zeer intieme informatie voor onbekende personen op sociale netwerksites. Deze informatie kan door anderen gebruikt worden op een voor de gebruiker ongewenste manier. Gutwirth (1998) merkte dit tien jaar geleden al op: 'Duizelingwekkend is het aantal handelingen van een individu dat tegenwoordig één of ander digitaal spoor achterlaat en bijgevolg ook op één of andere wijze retraceerbaar is. De massieve verwerking van persoonsgegevens dreigt ons geheel transparant en controleerbaar te maken' (Gutwirth, 1998:16). Sindsdien is de aandacht voor de bescherming van de gebruiker en daarmee de waarborging van privacy steeds vaker punt van aandacht. Verschillende betrokken partijen zijn zich bewust van de mogelijke risico's, zoals het College Bescherming Persoonsgegevens (CPB) dat eind 2007 enkele richtlijnen heeft opgesteld (CPB, 2007).

De hierboven geschetste ontwikkelingen roepen nieuwe vragen op over de waarborging van privacy in social computing omgevingen. Met social computing omgevingen worden omgevingen bedoeld waarbinnen het sociale aspect van delen en creëren van kennis en informatie centraal staat zoals bij blogs, wiki's en sociale netwerksites het geval is. Veel onderzoeken gaan in op privacyrisico's en bedreigingen voor gebruikers, maar ervaren gebruikers dit ook zo? Zien zij bovenstaande ontwikkelingen wel als gevaar of zien zij vooral de mogelijkheden van het delen, creëren en communiceren van informatie? In dit onderzoek staat de gebruiker dan ook centraal. Aandacht zal worden gegeven aan de volgende vragen: Hoe beleven gebruikers privacy in online sociale netwerken? Zijn zij bezorgd over hun privacy en zo ja, waar ontbreekt het dan aan? Zijn aanbieders zich hier bewust van en zo ja, hoe gaan zij hier dan mee om?

Voor deze invalshoek is gekozen, omdat de meeste studies en onderzoeken niet specifiek ingaan op de privacybeleving van burgers of gebruikers, maar veel vaker onderzoek verrichten naar de mogelijke 'gevaren', waarbij vanuit een normatief standpunt wordt geredeneerd. Onder andere studies van Solove (2006), Jones & Soltron (2005) en ENISA (Hogben, 2007) zijn voorbeelden hiervan.

Dit onderzoek zal zowel ingaan op de mogelijke gevaren en risico's als de privacybeleving van gebruikers. Beide kanten worden belicht, waarbij het gebruikersperspectief domineert. Een grote rol is hierin weggelegd voor de jongeren. Jongeren zijn namelijk minder ongerust over hun privacy dan ouderen zoals blijkt uit het onderzoek van PEW Internet (Lenhart & Madden, 2007) en Digibewust (2007). Het Amerikaanse onderzoek van PEW internet (Lenhart & Madden,2007) en het Nederlandse onderzoek van Digibewust (2007) tonen aan dat jongeren in de leeftijd van 12 tot 18 jaar veel gegevens openbaar maken op sociale netwerksites. De vraag rijst of dit mogelijk het effect is van hoe zij hun privacy ervaren. Bovendien is het interessant om de vergelijking met een iets oudere doelgroep te trekken. Verwacht wordt dat zij anders met hun privacy omgaan, omdat zij privacy anders ervaren.

1.2 Doelstelling en relevantie

In dit onderzoek zal op bovenstaande vragen worden ingegaan waarbij vooral de mening van de gebruikers en hun privacybeleving centraal staat. Het onderzoek maakt daarmee deel uit van een project van TNO Informatie- en Communicatietechnologie naar User-Generated Privacy. De doelstelling van dit project is onder andere het verkennen en in kaart brengen van nieuwe vormen van privacywaarborging in web 2.0 omgevingen waarbij de nadruk ligt op de (controle-) mogelijkheden voor de gebruiker om zijn of haar privacy te beschermen. Deze masterthesis kent een nadrukkelijke samenhang met dit project, maar richt zich daarbinnen wel specifiek op sociale netwerksites. Doelstelling van dit onderzoek is in de eerste plaats de theorie over privacy verder te (helpen) ontwikkelen door inzicht te geven in de mate van overeenstemming tussen privacybeleving en traditionele privacytheorieën. Bovendien is het formuleren van aandachtspunten op basis van onderzoek naar de verschillen tussen privacybeleving van gebruikers en privacywaarborging door aanbieders een doelstelling van dit onderzoek.

De praktische relevantie van dit onderzoek is te vinden in het op gang brengen (of versnellen) van een bewustwordingsproces onder vooral jonge gebruikers over de omgang met privacy op sociale netwerksites. Voor gebruikers zelf kan het bijvoorbeeld relevant zijn om te weten hoe bedrijven omgaan met het waarborgen van privacy. Daarnaast kan verondersteld worden dat het belangrijk is dat gebruikers zich bewust zijn van de aard van gegevens die zij verstrekken aan bedrijven of op websites plaatsen, waardoor desgewenst de gevolgen van eventuele privacyrisico's beperkt kunnen worden. Kortom, de privacywaarborging van gebruikers door aanbieders zal worden vergeleken met hoe gebruikers hun privacy beleven en zal leiden tot aandachtspunten voor de aanbieders van sociale netwerksites. De wetenschappelijke relevantie komt ook naar voren in de doelstelling. In dit onderzoek wordt namelijk getracht de theorie over privacy verder te

ontwikkelen door de vergelijking te maken tussen privacybeleving van gebruikers op dit moment en de traditionele theorieën.

1.3 Hoofdvraag en deelvragen

Het voorgaande resulteert in de volgende hoofdvraag:

'Hoe beleven gebruikers van sociale netwerksites hun online privacy en in hoeverre spelen aanbieders van sociale netwerksites hierop in?'

Bovenstaande vraag bestaat uit twee gedeelten (de deelvragen), die elk hun eigen subdeelvragen hebben. De twee deelvragen worden beantwoord aan de hand van casestudyonderzoek. De methoden van onderzoek, die binnen deze casestudy worden gehanteerd, komen in hoofdstuk vijf uitgebreid aan de orde.

1. ***In hoeverre waarborgen aanbieders van sociale netwerksites de privacy van gebruikers binnen deze sites?***

a. Hoe waarborgen aanbieders de privacy van gebruikers op dit moment en welke overwegingen spelen daarbij een rol?
b. Wat zijn mogelijke privacybeperkingen/risico's binnen sociale netwerksites?

2. ***Hoe beleven gebruikers van sociale netwerksites hun online privacy?***

Om een goed antwoord te kunnen formuleren zijn de volgende subdeelvragen ontwikkeld:

c. Hoe definiëren gebruikers van sociale netwerksites privacy en welke waarden vinden zij belangrijk met betrekking tot hun privacy?
d. In hoeverre houden gebruikers van sociale netwerksites zich bezig met privacyissues in sociale netwerksites?
e. Welke risico's zien zij voor hun privacy in online sociale netwerken?
f. In hoeverre vinden gebruikers dat sociale netwerksites hun privacy waarborgen?
g. Wat willen gebruikers zelf met betrekking tot privacywaarborging op sociale netwerksites?
h. In hoeverre zijn er verschillen te ontdekken tussen leeftijdsgroepen?

1.4 Structuur onderzoeksverslag

In deze paragraaf wordt kort de structuur van dit onderzoeksverslag uiteen gezet. Hoofdstuk twee staat in het teken van verschillende theorieën over sociale netwerksites, waarbij ook ingegaan wordt op enkele voorbeelden van sociale netwerksites. Het volgende hoofdstuk, hoofdstuk drie, richt zich op privacy. In dit hoofdstuk komt het privacybegrip, de verschillende dimensies, privacywaarborging, privacybeleving en bewustwording door gebruikers aan de orde. Zowel kwantitatieve onderzoeken als kwalitatieve onderzoeken naar privacy worden besproken en in relatie tot sociale netwerksites gebracht. Hoofdstuk vier staat geheel in

het teken van de gehanteerde methoden van onderzoek, waarbij aandacht besteed wordt aan de onderzoeksmethodes en de data-analyse. In het daaropvolgende hoofdstuk, hoofdstuk vijf, wordt ingegaan op de privacywaarborging door de aanbieder (deelvraag 1), waarna in hoofdstuk zes de resultaten van het gebruikersonderzoek aan bod komen (deelvraag 2). In de conclusies van beide hoofdstukken wordt antwoord gegeven op de twee deelvragen. Deze zullen vervolgens in de conclusie, in hoofdstuk 7, in samenhang met elkaar worden besproken, waarbij antwoord wordt gegeven op de hoofdvraag van deze thesis. Daarnaast zal in de conclusie van dit onderzoek een aantal aandachtspunten geformuleerd worden voor de waarborging van de privacy van gebruikers op sociale netwerksites vanuit het perspectief van de dienst zelf en vanuit het perspectief van de gebruikers.

2. SOCIALE NETWERKSITES

Zoals in de inleiding is beschreven, staan in deze thesis twee onderwerpen centraal, namelijk sociale netwerksites en privacy. In dit hoofdstuk gaat aandacht uit naar sociale netwerksites. Het begrip kent vele betekenissen. In dit hoofdstuk wordt daarom uitgelegd wat sociale netwerksites zijn, hoe zij te plaatsen zijn binnen web 2.0 diensten en in hoeverre er gebruik wordt gemaakt van sociale netwerksites.

2.1 Web 2.0

Sinds de grootschalige verspreiding en adoptie van Internet heeft ook het gebruik van Internettoepassingen een hoge vlucht genomen. Na de eerste generatie websites, waarbij het mogelijk was om informatie uit te wisselen, ontstaan er nu ook talloze nieuwe diensten. Deze diensten, ook wel Web 2.0 diensten genoemd, onderscheiden zich van andere diensten omdat ze onder andere de gebruiker centraal stellen.

In 2004 introduceerde O'Reilly (2005) het begrip 'Web 2.0' tijdens een conferentie in Silicon Valley en sindsdien wordt het begrip veelvuldig gebruikt. Wat de precieze betekenis is van het begrip is echter niet duidelijk. Zoals O'Reilly zelf opmerkt: 'There's still a huge amount of disagreement about just what Web 2.0 means, with some people decrying it as a meaningless marketing buzzword, and others accepting it as the new conventional wisdom' (O'Reilly, 2005). Heel algemeen gezegd is Web 2.0 een benaming voor een aantal samenhangende ontwikkelingen op het web, waarbij de gebruiker centraal staat (Kol, 2008). De macht ligt hierbij bij de gebruiker, die in staat is om, meestal gratis, informatie, kennis, muziek, films en vrienden te delen (NRC Handelsblad, 2006). Het begrip 'web 2.0' blijkt bij veel mensen niet bekend te zijn, hoewel zij sites als Marktplaats, Wikipedia, Hyves en Youtube vaak wel kennen (Vos & Van Geel, 2007). Dit blijkt uit onderzoek van Ruigrok Netpanel naar bekendheid, gebruik en toegevoegde waarde van Web 2.0 diensten.

2.2 Definitie sociale netwerksites

In de afgelopen paar jaren zijn online sociale netwerken deel uit gaan maken van het dagelijkse leven van mensen (Dwyer et al. 2007). Over wat nu precies een sociale netwerksite is, zijn de meningen verdeeld. Vaak worden de begrippen sociale netwerksites en communities door elkaar heen gebruikt (Broekman, 2007). Soms wordt een sociaal netwerk ook wel als een vorm van een community beschouwd of wordt de term 'virtuele gemeenschap' gehanteerd. Het is moeilijk om een duidelijke definitie te geven van wat een sociale netwerksite nu precies is.

Volgens Gross & Acquisti (2005) richten sociale netwerksites zich op online interactie en communicatie, maar verschillen de sites onderling soms sterk. De meest voorkomende soort is gebaseerd op de presentatie van een profiel en sociaal netwerk van de gebruiker. Dit is bijvoorbeeld bij Hyves, Facebook en LinkedIn het geval. Gross & Acquisti (2005:1) brengen een aantal mogelijkheden in kaart. Volgens hen zijn dat het tonen van een profiel: een representatie van de gebruiker en zijn of haar contacten, met de intentie om in contact te komen met

anderen, nieuwe vrienden te ontmoeten (o.a. Friendster, Orkut), een nieuwe baan te vinden (o.a. LinkedIn) en aanbevelingen te doen of te ontvangen (o.a. Tribe). De definitie van Gross & Acquisti (2005) wordt in dit onderzoeksverslag gehanteerd wanneer over een sociale netwerksite gesproken wordt.

2.3 Criteria sociale netwerksites

Door De Bruin & de Bruin (2001) zijn vier criteria opgesteld waaraan een site tenminste moet voldoen om een sociale netwerksite genoemd te kunnen worden. In de eerste plaats moet er sprake zijn van sociale scheiding tussen leden en niet-leden (De Bruin & de Bruin, 2001). Dit kan al tot stand komen door bijvoorbeeld het invullen van een aanmeldingsformulier. Dit criterium komt echter duidelijker tot uitdrukking doordat er sprake is van regels, plichten en normen die alleen gelden voor de personen die lid zijn van een bepaalde gemeenschap. In de tweede plaats moet er een mogelijkheid bestaan tot sociale interactie en/of communicatie (De Bruin & de Bruin, 2001). Dit kan bijvoorbeeld door middel van het plaatsen van een bericht op een forum, of het chatten met personen. Vaak is deze sociale interactie of communicatie één van de belangrijkste elementen binnen een sociale netwerksite. Ten derde moet er een bepaalde vorm van sociale controle zijn waardoor er toezicht gehouden wordt op de sociale interactie en communicatie (De Bruin & de Bruin, 2001). Deze sociale controle is vaak het grootst binnen de gebruikersgroep zelf, maar soms zorgt een moderator dat de regels worden nageleefd. Als laatste dient er een bepaalde cultuur te bestaan (De Bruin & de Bruin, 2001). Dit houdt vaak niet meer in dan dat een credo (ook wel motto) of een netetiquette geldt binnen de site, waarin opgenomen is aan welke regels gebruikers zich moeten houden. Bovenstaande vier criteria worden in dit onderzoeksverslag gehanteerd bij de bespreking van sociale netwerksites.

2.4 Verschillen tussen sociale netwerksites

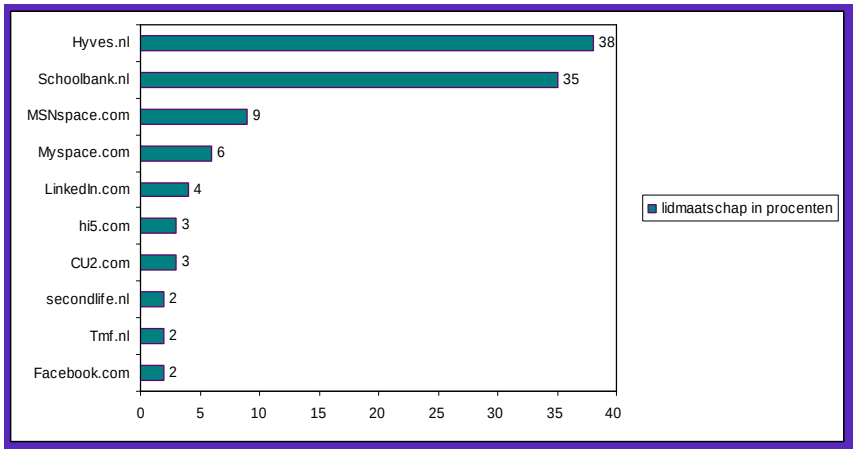
Tussen de verschillende sociale netwerksites bestaan grote verschillen in het tonen van gegevens. Zo is de identificeerbaarheid van personen op de ene site makkelijker dan op een andere. Op sommige sites wordt gebruik gemaakt van een pseudoniem of wordt enkel de voornaam getoond, zoals bij Friendster (Gross & Acquisti, 2005). In de tweede plaats wordt vaak informatie over hobby's en interesses gegeven, maar verschilt het per site hoeveel gegevens verstrekt worden. Ten derde verschilt ook de mate waarin iedereen de gegevens van anderen kan bekijken. Soms hebben alleen vrienden van de gebruiker inzicht in de gegevens, maar vaak is het zo dat iedere gebruiker een profiel van een andere gebruiker kan zien (Gross & Acquisti, 2005). Vooral het laatste is belangrijk bij het leggen van de relatie met privacy. Wanneer gebruikers niet goed op de hoogte zijn van welke informatie voor wie beschikbaar is, kan dit gevolgen hebben voor hoe zij hun privacy beleven.

2.5 Populaire sociale netwerksites

Het gebruik van sociale netwerksites is de afgelopen jaren gestegen. Dit blijkt onder andere uit onderzoek van Comscore (in: Van den Broek, 2007). Het aantal bezoekers van Myspace steeg in juni 2007 met 72 procent ten opzichte van dezelfde maand in 2006. Facebook groeide nog veel sterker, namelijk met 270 procent. In het onderzoek zijn geen Nederlandse sociale netwerksites meegenomen.

Uit het onderzoek van Ruigrok Netpanel blijkt dat 40 procent van de Nederlanders actief is in online netwerken (Vos & Van Geel, 2007). Van deze gebruikers is het merendeel (83 procent) actief op de online sociale netwerksite Hyves. Uit het Mediabarometer-onderzoek van Ernst & Young (2007), uitgevoerd onder 1005 Nederlanders van 15 jaar en ouder, blijkt dat 74 procent van de internetgebruikers één of meer profielen heeft aangemaakt op een sociale netwerksite.

Figuur 1: *Top 10 netwerksites in Nederland*



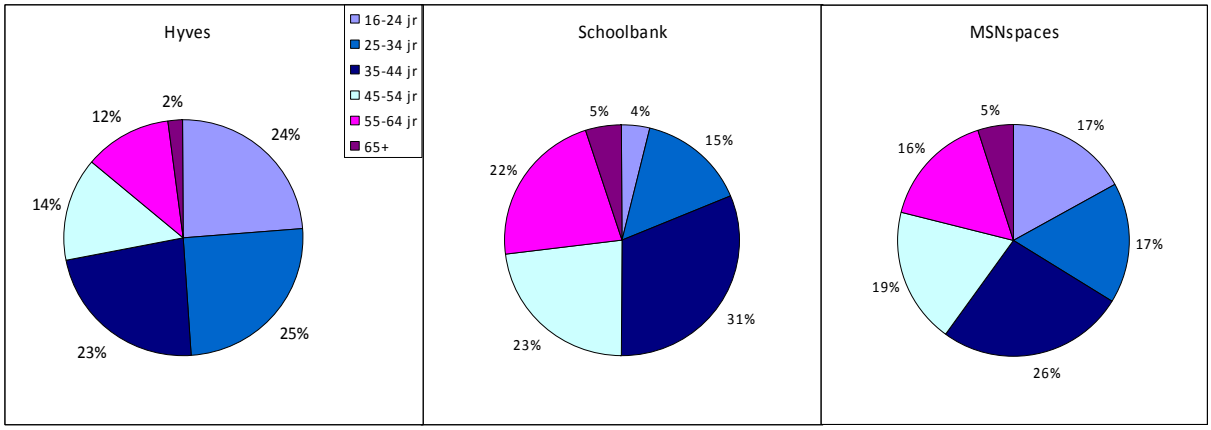
Bron: Ernst & Young. 2007:2. Eyeballs & Communities, Mediabarometer

Zoals uit figuur 1 blijkt, gebruikt 38 procent van de gebruikers van sociale netwerksites Hyves en is 35 procent lid van Schoolbank. Myspace (6 procent) en Facebook (2 procent) blijven daar ver bij achter. Dit terwijl Myspace en Facebook wereldwijd gezien veel groter zijn en volgens internet-onderzoeksbureau Comscore bijna 110 miljoen en 50 miljoen leden hebben (Ernst & Young, 2007). Hyves heeft beduidend minder leden. Het waren er naar verwachting ongeveer vijf miljoen in 2007 (BN-de stem, 2007). Een verklaring voor dit verschil in populariteit van de sites is te vinden in de taal. Zowel Myspace als Facebook zijn Amerikaanse sites, terwijl Hyves voornamelijk Nederlandse leden heeft.

Ook BN-destem (2007) heeft een lijst opgesteld met de meest populaire netwerksites in Nederland. Naast Facebook, LinkedIn, Myspace, Hyves en Cu2 noemen zij ook Superdudes en Sugababes die zich richten op jongens en meisjes in de leeftijd van 13 tot en met 19 jaar. Gezamenlijk hebben deze sites een ledental van ongeveer 1,2 miljoen. Daarnaast nemen zij Xseno op in hun lijst met populaire sociale netwerksites. Ook deze site richt zich op jongeren en had in 2007 ongeveer 140.000 leden.

De leeftijdsopbouw verschilt sterk per sociale netwerksite, zoals in figuur 2 te zien is. Vooral tussen Hyves en Schoolbank bestaan grote verschillen qua leeftijd van de leden. Bij Hyves is 49 procent van de leden tussen de 16 en 34 jaar oud. Bij Schoolbank is dit slechts 19 procent.

Figuur 2: *Leeftijdsopbouw gebruikers van Hyves, Schoolbank en MSNspace*



Bron: Ernst & Young. 2007:3. Eyeballs & Communities, Mediabarometer

Ook worden door respondenten redenen genoemd waarom men geen lid is geworden van een sociale netwerkstite. De meest genoemde redenen zijn het ontbreken van zin en tijd. Daarnaast is één vijfde van de respondenten van mening dat de privacy van gebruikers onvoldoende gegarandeerd wordt en heeft één tiende van de respondenten geen behoefte aan het openbaar maken van hun gegevens. Zij vinden dat de sites geweldige netwerken zijn voor stalkers om informatie uit te halen (Ernst & Young, 2007:4).

2.6 Samenvatting en conclusie

In dit hoofdstuk is aan de orde gesteld wat in deze thesis verstaan wordt onder een sociale netwerksite en waaraan deze moet voldoen. Over wat nu precies een sociale netwerksites is, zijn de meningen namelijk verdeeld. Door Gross & Acquisti (2005:1) zijn een aantal kenmerken van een sociale netwerksite in kaart gebracht. Deze worden meegenomen in de definitie die in deze thesis gehanteerd wordt. Een sociale netwerksite wordt als volgt gedefinieerd: Een site die het mogelijk maakt om een profiel te tonen met de intentie om in contact te komen met anderen, nieuwe vrienden te ontmoeten en/of een nieuwe baan te vinden en/of aanbevelingen te doen of te ontvangen (Gross & Acquisti, 2005:1). Bovendien moet er sprake zijn van sociale scheiding tussen leden en niet-leden en moet er sprake zijn van een bepaalde vorm van sociale controle, waardoor er toezicht gehouden wordt op de sociale interactie en communicatie (De Bruin & de Bruin, 2001). Ten slotte dient er ook een bepaalde cultuur te bestaan (De Bruin & de Bruin, 2001). Bovenstaande definitie en criteria van een sociale netwerksite worden in dit onderzoeksverslag gehanteerd wanneer van een sociale netwerksite sprake is.

Zoals de definitie van Gross en Acquisti (2005) al aantoont, zijn er binnen sociale netwerksites grote verschillen wat betreft de mogelijkheden en kan daarnaast ook de doelgroep sterk verschillen. In Nederland zijn Hyves, Schoolbank en MSNSpaces volgens het onderzoek van Ernst en Young uit 2007 het meest populair. Myspace en Facebook, beide sociale netwerksites die het wereldwijd zeer goed doen, blijven daarbij ver achter.

3. PRIVACY: THEORIE VERSUS PRAKTIJK

'Privacy is dood! Wen er maar aan!' (Scott Mc Nealy, 1999, vertaling uit het Engels)

Deze woorden werden in 1999 door Scott McNealy, topman van het bedrijf Sun, uitgesproken en later veelvuldig geciteerd (Dekker, 2008). Maar wat is privacy precies en wat is er anno 2008 bekend over privacyrisico's en privacybeleving binnen sociale netwerksites? Dit hoofdstuk gaat hier uitgebreid op in. Bovendien worden zowel onderzoeken gericht op internet en internetdiensten als onderzoeken gericht op de gebruiker in dit hoofdstuk meegenomen. Tot slot biedt dit hoofdstuk een overzicht dat als leidraad dient voor de inhoudanalyse en focusgroepsgesprekken. Op de verschillende methoden van onderzoek wordt in hoofdstuk vier uitgebreid ingegaan.

3.1 Definiëring van het privacybegrip

Het begrip 'privacy' is al eeuwen oud, maar blijkt nog altijd een begrip te zijn dat moeilijk te definiëren is. Gutwirth (1998) legt dit als volgt uit: 'Privacy heeft geen éénduidige betekenis. Er is geen tastbaar 'ding' waarnaar de notie verwijst. Er is geen afgebakende ruimte die ermee samenvalt. Er is geen sfeer van menselijke activiteiten die dé privésfeer voorstelt. Privacy is geen natuurlijk gegeven of deel van de werkelijkheid' (Gutwirth, 1998: 25).

Bovendien is privacy een begrip dat erg tijdgebonden is. Wat in de negentiende eeuw nog zo vanzelfsprekend leek, is volgens Weyns (1998) niet langer de realiteit. Toen was privé ook echt privé en publiek ook daadwerkelijk publiek. Van het vermengen of verwarren van deze begrippen was geen enkele sprake. Voor de meeste personen uit de geschiedenis gold dat het privéleven niet openbaar werd gemaakt voor anderen (Boyd, 2007). Alleen edelen en beroemheden hadden hiermee te maken. Alleen het leven van 'the rich and famous' was belangrijk genoeg om te delen.

Een derde component waardoor privacy lastig valt te definiëren, is dat privacy cultureel bepaald is. In veel Afrikaanse landen bijvoorbeeld wijkt het individualisme voor de collectiviteit waardoor de ruimte voor privacy beperkt wordt (Gutwirth,1998:21). Kortom, de tijd en de sociale of culturele groep en daarmee ook de plaats zijn van invloed op de privacy en bemoeilijken daarmee ook de afbakening van het onderwerp. Dit heeft tot gevolg dat wat door een individu onder privacy wordt verstaan, door een ander persoon heel anders omschreven kan worden. Dit kan vervolgens consequenties hebben voor hoe er over privacyissues gedacht wordt en hoe hiermee omgegaan wordt.

3.1.1 Definities van privacy

Eén van de eersten die privacy probeerden te omschrijven waren Warren en Brandeis. Zij omschreven privacy in 1890 als 'a right to be let alone' (in: Buchanan et al. 2007:157). In de decennia die volgden, zijn vervolgens andere begripsbepalingen gedefinieerd. Onder andere Westin omschreef privacy in 1967 als 'the right to prevent the disclosure of personal information to others' (in: Buchanan et al.2007:157). DeCew geeft een definitie die erg op de definitie van Westin lijkt. Hij spreekt over 'privacy (…) as a counterbalance to protect individuals from the social control of others' (in: Woo, 2006:952). Enkele definities richten zich in het bijzonder op de regering en de media en zien hen als het mogelijke kwaad. Zoals Woo vermeldt is 'the modern concept of privacy based on the people's right to be free from intrusion into their live by the government and mass media' (Woo, 2006:952).

3.1.2 Dimensies van privacy

Zoals in de vorige paragraaf werd omschreven, worden doorgaans verschillende definities van privacy door onderzoekers gebruikt. Daarbij is vaak sprake van drie of vier manieren waarop het begrip 'privacy' wordt gehanteerd. In het onderzoek van Paine, Reips, Stieger, Joinson & Buchanan (2007) worden de vier dimensies van Burgoon et al. (1989) aangehaald. Burgoon et al. onderscheiden vier dimensies van privacy en verwoorden dit als 'the ability to control and limit physical, interactional (social), psychological and informational access to the self or one's group' (in: Paine et al. 2007:526). Ook DeCew (1997) onderscheidt verschillende dimensies van privacy en komt tot drie dimensies waaruit privacy bestaat: 'the informational dimension', 'the accessibility dimension' en 'the expressive dimension' (In: Paine et al. 2007:526 en in: Joinson & Paine, 2007:16). Ook Koops en Vedder (2001) onderscheiden drie manieren waarop het begrip privacy wordt gebruikt:

1. In de betekenis van ruimtelijke privacy
2. In de betekenis van intimiteit of individuele zelfbeschikking
3. In de betekenis van informationele privacy

De eerste dimensie komt overeen met de fysieke dimensie van Burgoon et al.(1989) en de tweede dimensie (accessibility) van DeCew (1997). Van ruimtelijke of fysieke privacy is bijvoorbeeld sprake wanneer iemand afzondering en rust opeist (Koops & Vedder, 2001). Voorbeelden van aantasting van de ruimtelijke of fysieke privacy zijn bijvoorbeeld bewaking, toetreding in de persoonlijke levenssfeer en fysiek contact (Joinson & Paine, 2007). De tweede dimensie komt overeen met de interactie- of sociale dimensie van Burgoon et al. (1989) en de expressieve dimensie van DeCew (1997). Hierbij gaat het vooral om het controleren van de sociale contacten en interactie met personen en organisaties. Een voorbeeld is het afschermen van een bepaald deel van het persoonlijke leven tegen al te opdringerige burgers en de overheid. De derde dimensie wordt zowel door Burgoon et al. (1989) als DeCew (1997) genoemd. Bij informationele privacy gaat het om de bescherming van persoonsgegevens. Hierbij moet wel opgemerkt worden dat in sommige gevallen er overlap is binnen de verschillende dimensies die door zowel Burgoon et al.(1989) als DeCew (1997) zijn gedefinieerd.

Hoewel de drie of vier dimensies, zoals deze van oudsher gehanteerd worden, niet geheel verdwenen zijn, gaat de meeste aandacht toch vaak uit naar de informationele privacy. Door Gutwirth (1997) werd dit meer dan tien jaar geleden al opgemerkt. Ook Dubbeld (2000) onderschrijft dit. Volgens haar is het huidige wetenschappelijke en juridische debat over privacy veel te smal, eenzijdig, beperkt en verstard, omdat zij alleen oog heeft voor een informationeel begrip van privacy. Toch is het maar de vraag of online privacy zich uitsluitend richt op informationele aspecten. Zoals Dubbeld zelf aangeeft: 'Met de verspreiding van ICT lijkt privacy echter vrijwel volledig te zijn geïdentificeerd met informatie, en lijkt behoud van privacy geheel samen te vallen met het eigendom van persoonlijke gegevens' (Dubbeld, 2000:7). Natuurlijk is de hoeveelheid en de toegankelijkheid van informatie in het internettijdperk drastisch toegenomen en zijn zaken daardoor veranderd, maar toch is het maar de vraag of het debat zich uitsluitend op informationele privacy moet richten. Het zou heel goed kunnen dat gebruikers de bescherming van de lichamelijke integriteit en de zeggenschap en controle die een gebruiker bezit over zijn persoonlijke sfeer ook in het digitale tijdperk als belangrijke voorwaarde voor de privacy beschouwen (Dubbeld, 2000).

3.1.3 Privacy in de informatiesamenleving

Bovenstaande constatering van Dubbeld komt voort uit één van de huidige ontwikkelingen in de informatiemaatschappij, namelijk de toename en toegankelijkheid van informatie. Deze ontwikkelingen zullen in deze paragraaf uiteengezet worden. Hierbij wordt vooral ingegaan op hoe privacy en het begrip van privacy veranderd is met de komst van ICT, aan de hand van theorieën van Gutwirth en Lessig.

Ver voor de ontwikkeling van het internet, in 1958, schreef Hannah Arendt al over publiek versus privé: 'everything that appears in public can be seen and heard by everybody and has the widest possible publicity' (Hannah Arendt, 1958 In; Boyd, 2007: 22). Deze quote bleek ook voor het internettijdperk een grote waarheid met zich mee te dragen. Privé en publiek zijn niet langer op zich zelf staande begrippen, maar zijn onlosmakelijk met elkaar verbonden en verweven. Ze zijn in het internettijdperk drastisch aan het veranderen en vervagen.

Hoewel privacy zeker niet tot het verleden behoort, zoals Scott McNealy, topman van het bedrijf Sun, dit in 1999 wel meende te signaleren (Dekker, 2008), zijn de begrippen publiek en privé wel minder duidelijk te onderscheiden. Het afgelopen decennium is het delen en openbaar maken van gegevens in een stroomversnelling gekomen door onder andere web 2.0 diensten. Dit kan gevolgen hebben voor hoe de begrippen publiek en privé beleefd worden door gebruikers. Dit komt onder andere tot uiting in een onderzoek naar de sociale netwerksite Hyves (Verschoore de la Houssaije, 2007). Uit dit onderzoek blijkt namelijk dat studenten deze sociale netwerksite als privé beschouwen in plaats van openbaar (zie ook paragraaf 3.3.4) (Verschoore de la Houssaije, 2007) .

Verwerking, convergentie en digitalisering van informatie

Dat er wel degelijk zaken veranderd zijn met de komst van het internet wordt door Gutwirth bevestigd. Volgens hem zijn twee belangrijke dimensies toegevoegd. De eerste richt zich op het technische aspect. Door de technologische ontwikkelingen is de verwerking, convergentie en digitalisering van informatie versterkt en is zoals Gutwirth (1998:48) zelf zegt: 'de bedreiging van de privacy niet alleen groter en omvangrijker, maar ook meer gediversifieerd en veralgemeend'. Een Amerikaanse professor in de rechten, Lessig (1998) sluit zich hierbij aan. Volgens Lessig (1998) leidt de architectuur van de hedendaagse informatietechnologie en informatienetwerken tot een toename van wat kan worden waargenomen en bijgehouden. Dit resulteert vervolgens in een afname van de privacy. Deze bewering legt hij uit aan de hand van twee voorbeelden. Hij maakt daarbij een onderscheidt tussen het gedeelte van iemands leven dat 'is monitored' en het gedeelte dat 'is searched'. Monitored is dat gedeelte wat anderen kunnen zien, waar anderen op kunnen reageren. Searchable is wat achterblijft, zoals de gedachten die worden opgeschreven in een dagboek. Lessig (1998) maakt dit als volgt duidelijk met betrekking tot privacy: 'Life where less is monitored is a life more private; and life where less can (legally perhaps) be searched is also a life more private. Thus understanding the technologies of these two different ideas — understanding, as it were, their architecture — is to understand something of the privacy that any particular context makes possible' (Lessig, 1998:2).

Bovenstaande theorie van Lessig is in die zin van relevantie voor dit onderzoek dat wat 'searchable' is en wat dus beschikbaar blijft voor anderen van groot belang is binnen sociale netwerken. Soms kan dit zelfs zo ver gaan dat bepaalde gegevens voor jaren opgeslagen blijven en dat er bijvoorbeeld een digitaal dossier bijgehouden wordt. Op basis hiervan kunnen allerlei acties ondernomen worden door bijvoorbeeld commerciële partijen. Dit kan consequenties hebben voor de privacybeleving van personen.

Ontwikkeling van ICT in onze samenleving

De tweede dimensie die Gutwirth aandraagt, heeft betrekking op de ontwikkeling van ICT in onze samenleving. Gutwirth (1998:48) legt dit uit aan de hand van begrippen die door verschillende onderzoekers worden genoemd: 'The coming of post-industrial society (Bell, 1976), 'La société digitale (Mercier, Plassard & Scardigli, 1984), 'The third wave (Toffler, 1980) enzovoorts. Deze termen duiden aan dat onze samenleving aan het veranderen is, waarbij informatie een steeds grotere positie inneemt. Het College Bescherming Persoonsgegevens (Kohnstam, & Dubbeld, 2007) gaat nog een stap verder en spreekt over een glazen samenleving. Het college stelt zichzelf de vraag of hightech-gegevensverwerkingen, die ons gedrag als burgers en consumenten transparant maken, een hoofdrol spelen in onze samenleving.

Zoals blijkt uit de twee dimensies die Gutwirth toevoegt, is informatie gemakkelijker toegankelijk en gaat informatie een steeds grotere rol spelen in onze samenleving. De theorie van Lessig sluit hierop aan. De informatie die op internet wordt geplaatst blijkt bijvoorbeeld nog jaren beschikbaar op het net. Maar waarom maken mensen deze informatie eigenlijk beschikbaar? Joinson en Paine (2007) geven in hun onderzoek enkele

verklaringen voor het feit dat publiek en privé steeds meer aan het vervagen zijn, waarbij zij vooral ingaan op hoe gebruikers zelf omgaan met het openbaar maken van hun gegevens. Het begrip disclosure en 'self-disclosure' nemen zij mee in hun betoog. Het gaat hierbij om het openbaar maken van informatie die nog niet bekend is bij een ander of zoals Jourard en Lasakow vermelden: 'the process of making the self known to others' (in: Joinson & Paine, 2007:238). Dit zorgt voor het versterken van de band tussen de personen zoals in het artikel van Joinson & Paine (2007) wordt aangehaald. Ook binnen een groep kan het openbaar maken van gegevens positieve effecten hebben. Zo kan bijvoorbeeld de vertrouwensband binnen een groep versterkt worden, het horen bij een bepaalde groep erkend worden en de groepsidentiteit versterkt worden. Bovenstaande roept de vraag op of dit werkelijk zo belangrijk is dat daar andere zaken, zoals privacy, voor moeten wijken. Vooral voor jongeren zou deze afweging van invloed kunnen zijn op hoe zij omgaan met privacy.

3.1.4 Definitie van privacy binnen sociale netwerksites

De volgende definitie van privacy, die een combinatie is van de definities van Westin (1967), DeCew (1997) en Woo (2006), wordt in dit onderzoeksverslag gebruikt: 'Privacy is the people's right to prevent the disclosure of personal information to others and the right to be free from intrusion and social control by others'.

Deze definitie wordt gehanteerd omdat deze alle dimensies van privacy in zich heeft. Bij privacy gaat het namelijk niet alleen om de bescherming van persoonsgegevens, hoewel dit vaak wel als uitgangspunt wordt genomen. Dit onderzoek zal echter uitgaan van een breder perspectief. Tussen de dimensies die de auteurs hebben opgesteld zijn slechts kleine verschillen op te merken. De theorie van Koops en Vedder (2004) zal in deze thesis als uitgangspunt dienen, omdat deze op een duidelijke manier de verschillen tussen de dimensies verwoord. De tweede dimensie zal wel anders gedefinieerd worden.

De volgende drie dimensies worden meegenomen in dit onderzoek:

1. Ruimtelijke dimensie: rust en afzondering opeisen
2. Relationele dimensie: beschermen van controlemogelijkheden van sociale contacten en relaties door anderen
3. Informationele dimensie: beschermen van (persoons)gegevens

De informationele dimensie is voor dit onderzoek zeker van groot belang, maar het zou zo kunnen zijn dat ook aspecten uit de relationele dimensie en ruimtelijke dimensie tot privacyproblemen leiden binnen sociale netwerksites. Deze dimensies worden in het digitale tijdperk echter vrijwel buiten beschouwing gelaten en in onderzoeken ook nauwelijks meegenomen. Bij de relationele dimensie en ruimtelijke dimensie valt te denken aan het monitoren van de sociale netwerken van personen of aan aantasting van een digitale vorm van de ruimtelijke privacy. De laatste vorm van aantasting van de privacy zou bijvoorbeeld tot uiting kunnen komen in het (ongevraagd) toetreden tot het sociale netwerk van een persoon.

3.2 Privacyrisico's

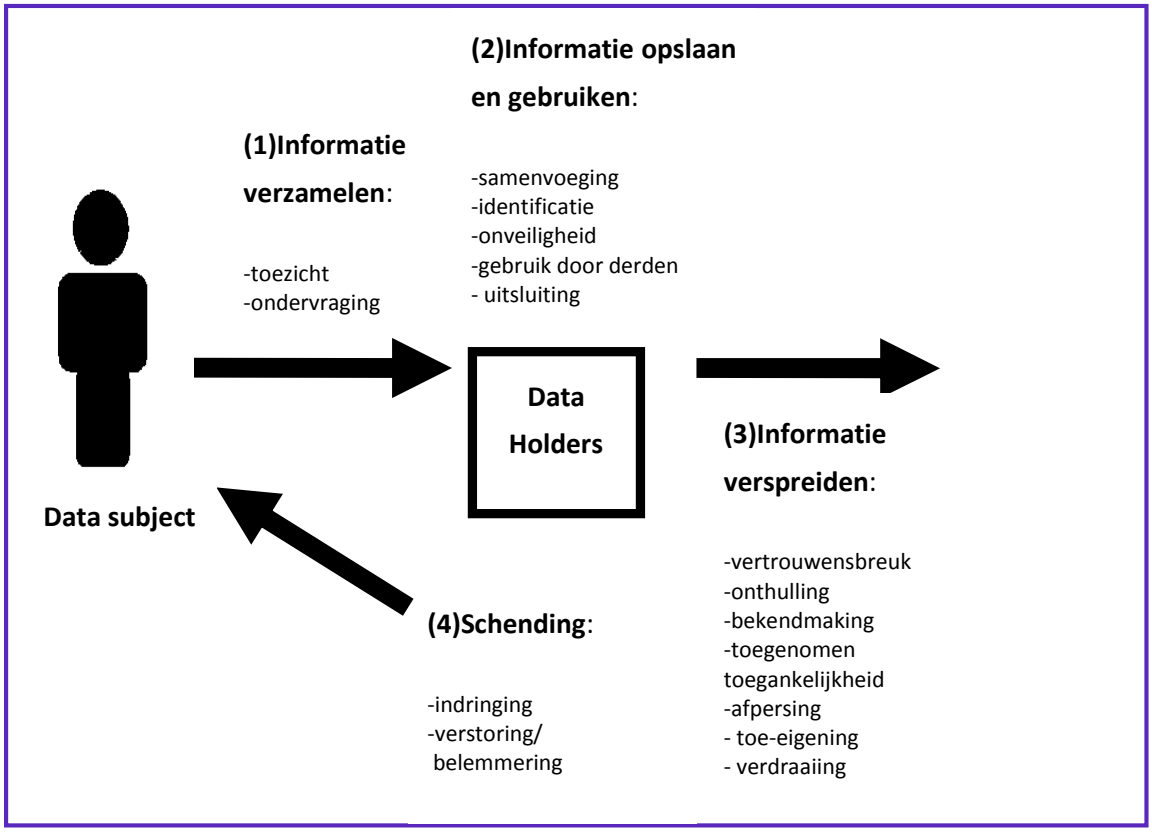
Naar privacyrisico's in het algemeen en bekeken vanuit de diensten zelf is veel onderzoek gedaan. In de komende paragrafen worden de verschillende theorieën en onderzoeken die zich richten op privacyrisico's aan de orde gesteld en waar nodig bekritiseerd. Deze studies zijn relevant, omdat op basis van deze risico's gekeken kan worden hoe het gesteld is met de privacywaarborging op (andere) sociale netwerksites.

3.2.1 Algemene privacyrisico's vanuit de rechtenstudies

Een duidelijke indeling van privacyrisico's bekeken vanuit de rechtenstudies is door Solove uiteengezet. Hij bracht in 2006 mogelijke privacyproblemen (risico's) in kaart. Uitgangspunt van Solove was een onderzoek van William Prosser uit 1960. Volgens Solove (2006) zijn de onderwerpen die William Prosser uitwerkte veel te beperkt en te gedateerd. Prosser richtte zich op vier onderwerpen waarbij zijn aandacht voor de informationele aspecten van privacy achterwege bleef. Aangezien er de afgelopen decennia op technologisch gebied veel veranderd is, gaat Solove in op de problemen over privacy in het nieuwe digitale tijdperk. Hij merkt daarbij op dat het niet gemakkelijk is om een duidelijk beeld te geven van de privacyproblemen, omdat het moeilijk aan te geven is wanneer er daadwerkelijk sprake is van inbreuk op de persoonlijke levenssfeer. Echter, Solove (2006) legt een kader neer waarbinnen het mogelijk is om de privacyproblemen te begrijpen, de overeenkomsten en verschillen te zien, de relaties tussen problemen en de oorzaken van de problemen te overzien. Hij heeft vier groepen van activiteiten bepaald waarbinnen privacyproblemen te vinden zijn: (1) informatie verzamelen, (2) informatie opslaan en gebruiken, (3) informatie verspreiden en (4) schending (Solove, 2006: 490). Deze vier groepen worden getoond in figuur 3.

De eerste groep (1) omvat het verzamelen van informatie door personen, bedrijven en de overheid (door Solove ook wel aangeduid als dataholders). Daarbij zijn het bekijken, luisteren en/of opnemen van iemands activiteiten en de verschillende manieren van ondervragen en het proberen informatie los te krijgen de belangrijkste problemen. De tweede groep (2) omvat activiteiten waarbij het gaat om de manier waarop informatie wordt opgeslagen en gebruikt door verschillende partijen. Privacyproblemen of risico's die hij noemt zijn onder andere identificatie van personen op basis van persoonlijke gegevens, het beschermen van opgeslagen gegevens en het verspreiden van gegevens aan derden. Bij de derde groep van activiteiten (3) gaat het om de verspreiding van informatie. Het verbreken van een belofte om informatie vertrouwelijk te houden, het openbaar maken van specifieke informatie die in het nadeel kan werken van een ander, het tonen van bepaalde beelden en afpersing zijn bij deze groep de mogelijke risico's. Bij de vierde groep (4) gaat het om schending van privézaken. Deze hoeven niet te zijn ontstaan door misbruik van informatie. Hier brengt Solove het lastig gevallen worden door anderen ter sprake. Bij deze groep komen dus ook aspecten van de ruimtelijke en relationele dimensie aan de orde.

Figuur 3: *De taxonomie van privacy*



Bron: Solove. 2006:490. A Taxonomy of Privacy

Kortom, Solove brengt een hiërarchische ordening aan in de privacyproblemen waardoor deze problemen gemakkelijker te begrijpen zijn. Hierbij richt hij zich niet specifiek op privacyproblemen die op het internet kunnen ontstaan, maar zet hij de mogelijke privacyrisico's wel duidelijk uiteen. Met voorbeelden maakt hij duidelijk wat concreet wordt bedoeld met de verschillende risico's, hoewel sommige risico's wel erg veel met elkaar te maken hebben. Solove biedt dus een duidelijk kader en zoals in tabel 5 (zie pagina 33) is te zien, zijn veel van deze risico's in enige mate ook van toepassing binnen sociale netwerksites. Bij deze indeling valt wel op te merken dat het vooral gaat om (persoonlijke) gegevens en hij zich dus ook in sterke mate richt op de informationele privacy.

3.2.2 Privacyrisico's binnen sociale netwerksites

Waar Solove zich richt op de algemene privacyrisico's die in de huidige samenleving mogelijk zijn, richten Dwyer, Hiltz en Passerini (2007) en ENISA (Hogben, 2007) zich specifiek op de privacybedreigingen die in sociale netwerkomgevingen kunnen ontstaan. Dwyer et al. (2007) zijn van mening dat het noodzakelijk is dat sociale netwerksites regels krijgen voor bescherming van data. Pas dan zou eenzelfde niveau van privacy gewaarborgd kunnen worden zoals wij in de offline wereld ervaren (Dwyer, Hiltz & Passerini 2007). Ook ENISA is van mening dat er aandacht moet komen voor privacy in sociale netwerkomgevingen (Hogben, 2007). Daarom heeft zij in oktober 2007 enkele aanbevelingen gedaan aan aanbieders van sociale netwerksites. Het gaat hierbij vooral

om technische aanbevelingen. Deze 19 aanbevelingen komen voort uit de privacyrisico's die door ENISA (Hogben, 2007) in kaart zijn gebracht. De privacyrisico's worden in tabel 1 weergegeven.

Tabel 1: *Privacyrisico's ENISA*

(1) Digital dossier aggregation	het creëren van een digitaal dossier door derde partijen
(2) Secondary data collection	gegevens die verstrekt worden door het gebruik van de site zelf: bijvoorbeeld aantal connecties, bezochte pagina's etc.
(3) Face recognition	het gezicht als 'identifier' en daarmee een link naar andere sites
(4) Content Based Image retrieval	een nieuwe technologie op basis waarvan het mogelijk is om bepaalde zaken op te sporen
(5) Likability from image metadata	ongevraagde verbanden naar persoonlijke gegevens, zoals via het taggen van foto's gebeurt.
(6) Difficulty of complete account Deletion	moeilijk om het totale account te verwijderen met daarbij ook de links van anderen naar de pagina
(7) SNS Spam	ongewenste berichten die worden verspreid via SNS
(8) Cross site scripting, viruses and Worms	bedreigingen van buiten af
(9) SNS aggregators	het aggregeren van profielen
(10)Spear phishing using SNS and SNS-specific phishing	phishing (internetfraude)
(11) Infiltration of networks	het gemak waarmee geïnfiltreerd kan worden in netwerken
(12)Profile-squatting	reputatie schade als gevolg van het overnemen van iemands identiteit
(13) Stalking	cyberstalking via sociale netwerksites
(14) Bullying	intimideren van anderen via sociale netwerksites
(15) Corporate espionage	het gebruiken van sociale netwerksites door bijv. hackers om bedrijfsinformatie in handen te krijgen

Bron: Hogben. 2007. Security issues and recommendations for online social networks (eigen vertaling)

De risico's die door ENISA (Hogben, 2007) worden genoemd geven een aardig compleet beeld van de meest voorkomende risico's binnen sociale netwerksites en daarom worden zij in dit onderzoek meegenomen. Hoe dit precies wordt gedaan, komt in de conclusie van dit hoofdstuk ter sprake.

3.2.3 Privacybedreigingen binnen Facebook

Waar Solove (2006) zich richt op de algemene privacyrisico's en ENISA (Hogben, 2007) zich richt op sociale netwerksites in het algemeen, richten Jones & Soltron (2005) zich specifiek op de privacybedreigingen binnen Facebook. Op basis van onderzoek naar deze sociale netwerksite brachten zij enkele privacybedreigingen in kaart, gebaseerd op drie factoren die bijdragen aan privacyrisico's: (1) gebruikers maken te veel informatie beschikbaar (2) Facebook neemt geen adequate maatregelen om de privacy te beschermen en (3) derde partijen zijn actief op zoek naar informatie van gebruikers. Volgens Jones & Soltron (2005) leidt dit tot de volgende privacyrisico's voor Facebook-gebruikers:

Tabel 2: *Privacyrisico's Jones & Soltron*

(1) Security breach	veiligheidswaarborging. Deze is nooit geheel te waarborgen, maar Facebook zou wel beleid moeten hebben wanneer sprake is van 'veiligheidsbreuk'.
(2) Commercial datamining	de schat aan informatie die via Facebook voorhanden is en die voor commerciële doeleinden zeer interessant is
(3) Database Reverse-Engineering	informatie die slechts voor een beperkt aantal personen beschikbaar zou moeten zijn, maar door middel van bijvoorbeeld 'advanced search' wel boven water te krijgen is.
(4) Password Interception	het onderscheppen van wachtwoorden.
(5) Incomplete Acces Controls	de controle die de gebruiker niet heeft over wie zijn of haar foto's kan zien. Door de URL in te tikken waarbij gezocht wordt op naam is het mogelijk om foto's te bekijken.
(6) University Surveillance	het in de gaten houden van de studenten door de universiteit
(7) Disclosure to advertisers	de profielinformatie die Facebook onder ogen van derde partijen kan brengen.
(8) Lack of User Control of Information	beperkte controle die gebruikers hebben over informatie, doordat bijvoorbeeld foto's getagt worden en zo te herleiden zijn naar personen.

Bron: Jones & Soltron. 2005. Facebook: Threats to privacy (eigen vertaling)

Ook Gross en Acquisti (2005) brengen in hun onderzoek vier privacyrisico's in kaart die specifiek betrekking hebben op de sociale netwerksite Facebook, maar die ook op ander sociale netwerksites van toepassing kunnen zijn. Deze komen allemaal terug in de privacyrisico's die ENISA (Hogben, 2007) en Jones & Soltron (2005) noemen. In de eerste plaats kunnen gebruikers schade ondervinden doordat gebruikers gestalkt kunnen worden (1-Stalking). Ook bestaat er een mogelijkheid dat op basis van bepaalde gegevens een persoon geïdentificeerd wordt zonder dat direct identificerende gegevens zoals naam en adres beschikbaar zijn gesteld (2-Re-identification). Op basis van deze gegevens kan informatie op andere sites naar boven worden gehaald. Ook Gutwirth (1998) staat hierbij stil: 'Feit is eenvoudigweg dat het technisch perfect mogelijk is om alle geautomatiseerde persoonsgegevens over één persoon samen te brengen' (Gutwirth, 1998:15). Een derde risico dat Gross en Acquisti (2005) noemen is de mogelijkheid tot het bijhouden van een digitaal dossier van de profielpagina's van de gebruikers. Informatie kan op deze manier voor lange tijd of zelfs voor altijd beschikbaar blijven. Hier kan misbruik van gemaakt worden (3-Building a digital dossier). Tot slot merken de auteurs op dat er binnen sociale netwerksites sprake kan zijn van een fragiele privacybescherming. Gebruikers kunnen zelf weinig invloed uitoefenen op de totstandkoming van de netwerken van anderen. Op deze manier bestaat de kans dat gegevens ook voor onbekenden beschikbaar worden gemaakt (4-Fragile privacy protection).

Kortom, paragraaf 3.2 toont aan dat er veel onderzoek gedaan is naar mogelijke risico's en gevaren in het algemeen, binnen sociale netwerksites en ook binnen bepaalde sociale netwerksites zoals Facebook. Sommige risico's komen in de onderzoeken in vergelijkbare bewoordingen terug of hebben een direct of indirect verband

met elkaar. Deze risico's zijn belangrijk binnen deze thesis en daarom zal in de conclusie van dit hoofdstuk uitgelegd worden in hoeverre deze risico's mee worden genomen in dit onderzoeksverslag.

3.3 Privacybeleving

De onderzoeken die in paragraaf 3.2 zijn besproken, gaan in op privacyrisico's en bedreigingen voor gebruikers bekeken vanuit een wetenschappelijk oogpunt. De auteurs beschrijven de risico's vanuit de dienst zelf, waarbij geen aandacht is voor de gebruiker. De onderzoeken zijn soms ook technisch georiënteerd en hebben veel te maken met de tools die binnen deze sociale netwerken gebruikt kunnen worden. Daarmee blijven de ervaringen van de gebruikers buiten beeld, terwijl juist die interactie tussen de gebruiker en de dienst zo belangrijk is, zoals in de inleiding werd vermeld. Het is maar de vraag of de risico's die door onderzoeksbureaus en instellingen zijn opgesteld, ook door gebruikers opgemerkt worden.

3.3.1 Waarden en criteria om privacygevoeligheid te meten

Gebruikers staan veelal niet centraal in onderzoeken naar privacy. Als dat wel het geval is, wordt vaak onderzoek verricht op basis van een kwantitatieve methode. Smink, Hamstra en van Dijk (1999) behoren dan ook tot één van de weinigen die aandacht hebben voor de beleving van privacy door burgers. Zij hebben onderzocht welke criteria gelden om de privacygevoeligheid van bepaalde onderwerpen te meten.

Uit de omschrijvingen van de respondenten blijkt dat zij een ruime beschrijving geven van wat zij onder privacy verstaan. Zo zijn 'alles wat van mij is en waarvan ik niet wil dat andere mensen dat weten', 'dat je niet gestoord wordt', geen misbruik van vertrouwen maken' en 'vrij leven zonder inmenging van anderen' veelgehoorde antwoorden wanneer wordt gevraagd naar wat privacy voor de respondenten betekent. De criteria die van belang zijn voor burgers met betrekking tot gegevensverzameling en die voortvloeien uit bovenstaande definities zijn de volgende:

- belang van het doel van gegevensverzameling
- nut van gegevensverzameling
- wijze waarop gegevens worden verzameld
- gebruik van gegevens
- praktische gevolgen van gegevensverzameling
- beveiliging van gegevens
- eigen invloed van burgers op gegevensverzameling
- wenselijkheid van gegevensverzameling
- informatie over gegevensverzameling

Daarnaast hebben zij aan de hand van individuele interviews een aantal waarden kunnen destilleren die belangrijk zijn voor mensen wanneer het gaat over beleving van privacy. De volgende negen waarden zijn voor veel mensen van belang: zelfstandigheid van het individu, bewegingsvrijheid, ongestoord kunnen leven, vrij

blijven van stigmatisering, vrij blijven van manipulatie, eigenwaarde, gelijkheid, integriteit en autonomie. Binnen deze waarden werden onder andere de eerder vermelde criteria genoemd. Hiermee raken deze waarden sterk aan het uitgangspunt van Gutwirth dat privacy onlosmakelijk verbonden is met de individuele vrijheid van de mens. De eerste vier waarden blijken voor vrijwel alle personen van belang te zijn. De overige 5 verschillen sterk van persoon tot persoon, zo blijkt uit het onderzoek (Smink et al. 1999). Deze criteria en waarden kunnen mogelijk ook door gebruikers van sociale netwerksites genoemd worden, waarbij wel gezegd moet worden dat in het onderzoek van Smink et al. (1999) vooral de informationele privacy belicht wordt. Een overzicht van waarden en criteria, die uit het onderzoek van Smink et al. (1999) naar voren kwamen, is te vinden in bijlage vier.

3.3.2 Privacybezorgdheid en privacybewustzijn

In de vorige paragraaf is ingegaan op de waarden en criteria die voor burgers van belang zijn bij het beoordelen van hun privacy. Deze paragraaf gaat hierop door, waarbij verschillende studies behandeld worden die zich richten op de bezorgdheid over en het bewustzijn van privacy door internetgebruikers en gebruikers van sociale netwerksites. Met privacybezorgdheid wordt de mate van ongerustheid bedoeld. Hierbij staat de mening van de gebruiker centraal. Met de mate van privacybewustzijn wordt bedoeld in hoeverre gebruikers nadenken over hun privacy en hoe er vervolgens door hen mee om wordt gegaan. Dus hoe zij omgaan met het beschermen van hun privacy en welke acties zij hiertoe nemen.

De afgelopen jaren hebben verschillende instanties en onderzoekers zich bezig gehouden met onderzoek naar privacy in relatie tot het internet. Conclusie van een onderzoek uitgevoerd door TRUSTe in 1997 was dat 70 procent van de respondenten zich meer druk maken over hun privacy op het internet dan privacy in de traditionele media (O'Neil, 2001). Dat mensen zich met privacy bezig houden en bezorgd zijn over hun privacy wil niet zeggen dat zij ook daadwerkelijk acties ondernemen, zoals blijkt uit een onderzoek wederom uitgevoerd door TRUSTe (O'Neil, 2001). Hoewel internetgebruikers aangeven te weten hoe ze hun privacy moeten beschermen, geeft een meerderheid aan geen privacyverklaringen te lezen. Fran Maier, executive director van TRUSTe zegt daarover het volgende: '(…) the survey results suggest that consumers are not consistently following through in taking actions to protect their personal information' (Auteur onbekend, 2007:19). Ze blijken zich wel bewust te zijn van de mogelijkheid om hun privacy te beschermen maar ondernemen vaak geen stappen in de daadwerkelijke bescherming van hun gegevens. In hoeverre zij dus daadwerkelijk bewust omgaan met hun privacy is maar de vraag. Blijkbaar zijn er verschillen te constateren in wat mensen doen en wat ze zeggen dat ze doen. Dit heeft mogelijk te maken met de vraagstelling. Wanneer vanuit een negatieve invalshoek, dus vanuit privacybezorgdheid gekeken wordt, is het aannemelijk dat internetgebruikers zullen aangeven privacy belangrijk te vinden en zich hier zorgen over te maken.

Onderzoek uitgevoerd door Synovate in opdracht van Ilse Media toont het tegendeel aan. Dit onderzoek wijst uit dat tweederde van de Nederlandse internetgebruikers bewust nadenkt over welke informatie hij of zij op het internet plaatst. Ook gebruikt 45 procent van de internetgebruikers een apart e-mailadres voor online registraties en ligt dit percentage nog hoger bij de zeer actieve internetgebruikers (80 procent) (Nu.nl, 2007).

Internetgebruikers zijn vooral bereid om demografische gegevens en gegevens over lifestyle bekend te maken. Dit berichtten Phelps, Nowak en Ferrell (2000) naar aanleiding van hun onderzoek naar de relatie tussen categorieën van persoonlijke informatie, meningen over direct-marketing, ongerustheid over privacy en het online shoppinggedrag van consumenten. Consumenten blijken het minst bereid te zijn financiële gegevens en informatie over creditcards en telefoonnummers aan marketeers te verstrekken. De reden hiervoor kan mogelijk liggen in het gevaar dat door bedrijven misbruik gemaakt wordt van deze gegevens. Paine, Reips, Stieger, Joinson en Buchanan (2007) hebben onderzoek gedaan naar de privacyissues van internetgebruikers. Tabel 3 toont de privacyissues die door de respondenten zijn genoemd:

Tabel 3: *Online privacyconcerns van gebruikers*

Common concerns	% of respondents	*n*
Viruses	16.1	26
Spam	10.5	17
Spyware	9.9	16
Hackers	8.0	13
Access to personal information	6.8	11
Security	5.6	9
Identity theft	3.7	6
Trojan	3.1	5
Deception/honesty	1.2	2

Bron: Paine et al. 2007:531.Internet users' perceptions of 'privacy concerns' and 'privacy actions'

Verwacht zou mogen worden dat wanneer gebruikers bezorgd zijn over hun privacy, de waarborging van hun privacy belangrijk zal zijn. Gebruikers zullen dan proberen om zo weinig mogelijk informatie bekend te maken aan anderen. Bovendien zouden zij zich kunnen afkeren van de dienst wanneer aanbieders niet op de juiste manier omgaan met de privacy van de gebruikers. Dwyer et al.(2007) hebben hier onderzoek naar gedaan. Aan de hand van een vragenlijst hebben zij onderzocht of een hoge ongerustheid wat betreft internetprivacy bij sociale netwerksites van invloed is op het gebruik van deze sites. In de vragenlijst zijn vragen meegenomen over welke persoonlijke informatie de gebruikers tonen in hun profiel. Opties waren foto's, echte naam van de gebruiker, woonplaats, e-mailadres, telefoonnummers, relatiestatus (relatie of single), seksuele geaardheid en MSN naam. Het onderzoek van Dwyer et al. (2007) toont aan dat online relaties zich kunnen ontwikkelen in sociale netwerksites hoewel vertrouwen en privacywaarborging zwak zijn. Dit heeft mogelijk met de mate van privacybewustzijn te maken.

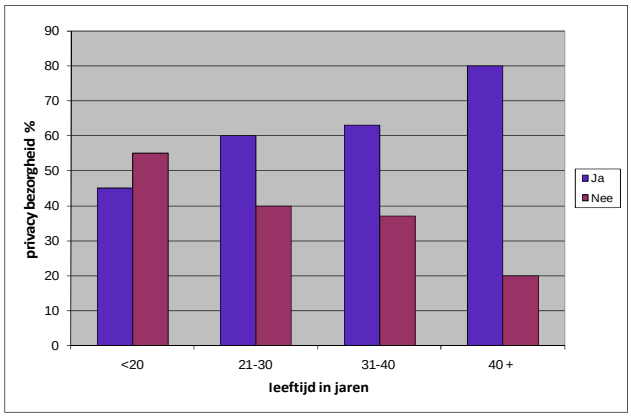
Wanneer het privacybewustzijn hoog is, zullen zij beschermen wat zij belangrijk vinden en wanneer dit niet mogelijk is hier rekening mee houden. Hoe zij vervolgens deze mogelijkheden en beperkingen ervaren binnen het product of de dienst is van invloed op de privacybezorgdheid. Uit onderzoek komt naar voren dat opleidingsniveau en hoogte van inkomen van invloed zijn op het niveau van ongerustheid over privacy (O'Neil, 2001). Ook is er een verschil te constateren tussen mannen en vrouwen zoals onderzoeken uitgevoerd door Louis Harris and Associates in 1996 (In: O'Neill, 2001) en O'Neil (2001) bevestigen. Beide studies kwamen tot de conclusie dat vrouwen ongeruster zijn over privacy dan mannen. Daarnaast blijken er verschillen te zijn tussen verschillende leeftijdsgroepen. De invloed van leeftijd wordt in de volgende paragraaf uitgewerkt.

Kortom, de uitkomsten van bovenstaande onderzoeken, uitgevoerd door TRUSTe (O'Neil, 2001), Synovate (Nu.nl, 2007), Paine et al. (2007) en Dwyer et al. (2007), tonen allesbehalve een eenduidig beeld over hoe over privacyissues gedacht wordt en of er al dan niet bewust met privacy wordt omgegaan.

3.3.3 Verschillen in mate van privacybezorgdheid en privacybewustzijn tussen leeftijdsgroepen

Onderzoek van Paine, Reips, Stieger, Joinson en Buchanan (2007) toont aan dat er een verschil is in de bezorgdheid over privacyissues tussen verschillende leeftijdsgroepen. Figuur 4 laat zien dat deze bezorgdheid toeneemt naarmate mensen ouder zijn. Van de personen onder de 20 jaar die meewerkten aan het onderzoek is slechts 45 procent bezorgd over zijn of haar privacy tegen 80 procent van de 40-plussers.

Figuur 4: *Privacybezorgdheid per leeftijdsgroep (in %)*



Bron: Paine et al. 2007:531. Internet users' perceptions of 'privacy concerns' and 'privacy actions'

Hierbij moet wel een kanttekening geplaatst worden. Privacybezorgdheid is namelijk een normatief begrip en is erg persoonsgebonden. Of jongeren inderdaad minder bezorgd zijn over hun privacy dan ouderen wordt door andere onderzoeken niet bevestigd. In dit onderzoek wordt dit verschil in privacybezorgdheid tussen leeftijds-groepen meegenomen aangezien verwacht wordt dat jongeren ook binnen sociale netwerksites minder bezorgd zullen zijn over hun privacy dan ouderen.

Gebruikers (12-18 jaar) van sociale netwerksites

Diverse onderzoeken wekken de suggestie dat jongeren minder bezorgd zijn over hun privacy dan ouderen. In deze onderzoeken wordt vooral ingegaan op hoe jongeren met hun privacy omgaan. Uit enkele onderzoeken, waaronder onderzoeken van PEW Internet (Lenhart & Madden, 2007) en Digibewust (2007), komt naar voren dat jongeren veel informatie prijsgeven op het internet en in sociale netwerken zoals onder ander blijkt uit onderzoeken van PEW Internet en het American Life Project en Digibewust. Zij hebben beide in 2007 onderzoek gedaan naar tieners en privacy in online sociale netwerken (Lenhart & Madden, 2007, Digibewust, 2007). Digibewust (2007) heeft onderzoek uitgevoerd onder jongeren van 12 tot 18 jaar en hen gevraagd hoe zij omgaan met hun persoonsgegevens op het internet. Jongeren blijken veel gegevens openbaar te maken. De meeste jongeren zetten hun voornaam online (92 procent) en meer dan de helft ook hun achternaam (62 procent). Daarnaast plaatst 64 procent van de jongeren foto's van henzelf op hun profiel. Ook e-mailadres (44 procent) en woonplaats (40 procent) komen vaak voor op hun profielpagina. Telefoonnummer en huisadres worden minder vaak openbaar gemaakt, respectievelijk 5 procent en 4 procent. Van de jongeren geeft 53 procent aan er geen problemen mee te hebben dat iedereen zijn of haar gegevens kan zien en wil 33 procent van alle jongeren niet dat vreemden hun gegevens kunnen zien. Verder blijkt dat één op de vijf tieners nog nooit heeft nagedacht over het afschermen van zijn of haar gegevens en dat 18 procent van de jongeren van 12 en 13 denkt anoniem te zijn op het internet. Het overgrote deel van de jongeren is zich wel bewust van het feit dat zij te identificeren zijn door de gegevens die zij openbaar maken op het internet. In vergelijking tot de Amerikaanse gebruikers maken Nederlandse gebruikers hun achternaam vaker bekend en wordt ook het e-mailadres door Nederlandse jongeren vaker openbaar gemaakt.

Gebruikers (studenten) van Hyves

Ook studenten blijken veel gegevens openbaar te maken en zijn tevens niet altijd op de hoogte voor wie zij deze informatie beschikbaar maken. Daarnaast zien zij de mogelijke consequenties van het openbaar maken van bepaalde persoonlijke gegevens vaak niet. Er blijkt sprake te zijn van een discrepantie tussen wat studenten openbaar maken in hun Hyves profiel en wat ze zeggen dat ze openbaar maken (Verschoore de la Houssaije, 2007). Dit komt vooral tot uiting bij contactgegevens zoals e-mailadres en telefoonnummer. Ook is er sprake van een discrepantie tussen wat studenten openbaar maken in hun 'krabbels' en hoe zij zeggen daarmee om te gaan: ze zijn zich niet altijd bewust van de hoeveelheid informatie die ze hiermee vrijgeven. 'Krabbels' van anderen lezen gebeurt vaak en wordt door de studenten ook als een leuke bezigheid gezien. De helft van de respondenten vindt het echter niet leuk dat werkgevers de profielen lezen, om daarmee een indruk te krijgen van een persoon. Ook is de helft van de studenten van mening dat er niets met de gegevens gedaan wordt die zij openbaar maken. Kortom, uit dit onderzoek kan geconcludeerd worden dat studenten Hyves als privé beschouwen in plaats van openbaar (Verschoore de la Houssaije, 2007).

Gebruikers van Facebook

Naast Hyves is ook de Amerikaanse sociale netwerksite Facebook door verschillende sociale wetenschappers onderzocht. Onderzoeken van Gross & Acquisti (2005), Lampe, Ellison, and Steinfield (2007) en Stutzman (2006) tonen aan dat gebruikers veel informatie over hen zelf op de pagina's plaatsen (in Dwyer et al, 2007). Bovendien zijn zij zich niet erg bewust van de mogelijkheden om bepaalde gegevens af te schermen (Dwyer et al. 2007). Gross & Acquisti (2005) gaan hierop in waarbij zij opmerken dat gegevens voor heel veel mensen beschikbaar gemaakt kunnen worden: 'Many individuals in a person's online extended network would hardly be defined as actual friends by that person; in fact many may be complete strangers. And yet, personal and often sensitive information is freely and publicly provided' (Gross & Acquisti 2005:9).

Beheerder van de jongerensite CU2.nl, Filip Leendertz, is wel van mening dat de gebruikers van deze site erg bewust met hun privacy bezig zijn. Volgens Leendertz registreert 90 procent van de gebruikers zich niet met zijn of haar volledige naam (Nu.nl, 2007). Kortom, in hoeverre jongeren zich bewust zijn van de gegevens die zij openbaar maken en de mogelijkheid om bepaalde informatie af te schermen is maar de vraag. In dit onderzoek wordt hierop ingegaan door te onderzoeken hoe jongeren hun privacy beleven en in hoeverre dit verschilt van anderen leeftijdsgroepen.

3.3.4 Privacy fundamentalists, pragmatists en unconcerned

Privacy, privacyissues en privacybezorgdheid blijken niet eenvoudig te achterhalen. Uit paragraaf 3.3.1 bleek al dat burgers privacy verschillend definiëren en ook andere waarden noemen. Uit het onderzoek van Smink et al. (1999) naar privacybeleving van burgers kwam daarnaast naar voren dat burgers op basis van hun privacybeleving in drie groepen kunnen worden ingedeeld. Ook in het artikel van Buchanan et al. (2007) en Joinson & Paine (2007) wordt gesproken over het indelen van personen op basis van mate van bezorgdheid. Dit gebeurt op basis van de Westin privacy segmentation.

De eerste groep die op basis van het onderzoek van Smink et al.(1999) is beschreven, blijkt nauwelijks privacyproblemen te ondervinden door de informatietechnologie, wat blijkt uit het relatief kleine aantal waarden wat deze mensen noemen. Door Westin (1967) wordt deze groep de 'privacy unconcerned' genoemd (in: Buchanan et al.2007, Joinson & Paine, 2007). De tweede groep hanteert iets meer waarden en geeft daarnaast aan dat er sprake is van privacyproblemen. Westin (1967) noemt deze groep de 'privacy pragmatists' (in: Buchanan et al.2007, Joinson & Paine, 2007). Voor de tweede groep zijn per waarde de genoemde meest relevante criteria weergegeven in bijlage vier. Hieruit zijn criteria af te leiden die van toepassing kunnen zijn op sociale netwerksites. De derde groep brengt de meeste waarden ter sprake. Deze groep is van mening dat informatietechnologie privacyproblemen met zich meebrengt, maar dat deze te voorkomen zijn. Zij zijn van mening dat gebruik van informatietechnologie vaak niet nodig is. Door Westin (1967) wordt deze groep de 'privacy fundamentalists' genoemd (in: Buchanan et al.2007, Joinson & Paine, 2007). Ook hebben Smink et al. (1999) de respondenten enkele stellingen voorgelegd. Hieruit blijken nogmaals de verschillen tussen de drie

groepen, waarbij de sterke privacybezorgdheid van groep drie duidelijk tot uiting komt. De resultaten zijn in tabel 4 opgenomen.

Tabel 4: *Algemeen privacyoordeel in relatie tot informatietechnologie*
(schaal van 1-7; helemaal mee oneens – helemaal mee eens)

Groep	*1*	*2*	*3*	*Totaal*
Ik vind dat door het toenemende gebruik van de informatietechnologie (computers en andere manieren om gegevens elektronisch op te slaan en uit te wisselen) mijn privacy steeds meer in het geding komt.	2.8	5.4	6.3	5.3
Ik denk dat de huidige maatschappij alleen goed kan functioneren als persoonlijke gegevens via computers worden vastgelegd en uitgewisseld.	4.8	4.2	2.7	3.7

Bron: Smink et al.1999. Privacybeleving van burgers in de informatiemaatschappij

Wanneer aan gebruikers gevraagd zou worden in hoeverre zij zich zorgen maken over privacy en privacyissues binnen sociale netwerksites, is het wellicht mogelijk deze personen in te delen door middel van de indeling van Smink et al. (1999) en de Westin privacy segmentation: 'privacy fundamentalists', 'privacy pragmatists' en 'privacy unconcerned'. Dit zou kunnen gebeuren aan de hand van de waarden en criteria die zij noemen. Daarbij moet wel in ogenschouw worden genomen dat de mate van privacybewustzijn door Smink et al. (1999) niet duidelijk wordt onderscheiden. Voor hen zijn het noemen van waarden, de hoeveelheid waarden en het ter sprake brengen van eventuele problemen de criteria om personen in te delen in categorie één, twee of drie. Welke factoren van invloed zijn op het privacybewustzijn van personen, blijft echter achterwege in de onderzoeken. Wanneer privacybewustzijn laag is, is het aannemelijk dat weinig waarden genoemd worden en dat daarnaast weinig gevaren gezien worden.

3.4 Samenvatting en conclusie

Dit hoofdstuk heeft zichtbaar gemaakt wat er binnen het onderwerp privacy en sociale netwerksites onderzocht is. De relevantie van de theorieën en onderzoeken die in dit hoofdstuk aan de orde zijn gesteld, wordt in deze conclusie beschreven.

Betekenis van de theorie voor onderzoek naar beleving van gebruikers

In de eerste plaats is een definitie geformuleerd die naar verwachting zal aansluiten bij privacy zoals deze binnen sociale netwerksites ervaren wordt. Binnen deze definitie komen alle dimensies aan de orde die in privacytheorieën worden behandeld. Vaak gaat de aandacht uit naar informationele privacy. Of de definitie en de dimensies ook door gebruikers zo ervaren worden, zal moeten blijken uit het gebruikersonderzoek. Op deze

manier kan een antwoord gegeven worden op de vraag of traditionele privacytheorieën op dit moment (nog) overeenkomen met hoe door gebruikers gedacht wordt over en omgegaan wordt met privacy.

Voor het gebruikersonderzoek zijn verder de waarden en criteria die door Smink et al. (1999) zijn ontwikkeld op basis van belevingsonderzoek zeer interessant. Deze criteria en waarden kunnen mogelijk ook door gebruikers van sociale netwerksites genoemd worden, waarbij wel gezegd moet worden dat daarbij vooral de informationele privacy belicht wordt. De beleving van de gebruikers zal in het resultatenhoofdstuk dan ook naast de waarden en criteria van Smink et al. (1999) worden geplaatst en worden vergeleken met de traditionele theorieën over privacy. In hoeverre er overeenkomsten en verschillen zijn te vinden tussen de waarden en criteria die worden aangedragen, zal in het resultatenhoofdstuk worden beschreven. Daarnaast zal gekeken worden naar de mate van privacybezorgdheid van de gebruikers door middel van de indeling van Smink et al. (1999) en de Westin privacy segmentation: 'privacy fundamentalists', 'privacy pragmatists' en 'privacy unconcerned'.

Ook zal in het gebruikersonderzoek ingegaan worden op de privacyrisico's en mogelijke privacyschendingen en hoe gebruikers hiermee omgaan. Tabel 5 geeft een overzicht van alle privacyrisico's die in de voorgaande paragrafen aan de orde zijn gekomen:

Tabel 5: *Samenvatting privacyrisico's*

Hogben (o.a SNS)	**Gross & Acquisti (SNS)**	**Jones (SNS-->Facebook)**	**Solove (taxonomy)**
Digital dossier aggregation	Buiding digital dossier	Commercial datamining	disclosure (information dissemination)
Secondary data collection	Re-identification	Disclosure to advertisers	secondary use (information processing)
Face recognition	Stalking	Database Reverse-Engineering	identification (information processing)
CBIR (Content-Based Image Retrieval)	Fragile privacy protection	Incomplete Acces Controls	Surveillance (information collection)
Linkability from image metadata		Surveillance	exposure (information dissemination)
Difficulty of complete account deletion		Lack of User Control of Information	distortion (information dissemination)
SNS Spam		Security breach	blackmail (information dissemination)
Cross site scripting, viruses and worms		Password Interception	intrusion (invasion)
SN aggregators			decisional interference (invasion)
Spear phishing using SNS			insecurity (information processing)
Infiltration of networks			interrogation (information collection)
Profile-squatting			aggregation (information processing)
Stalking			breach of confidentiality (information dissemination)
Bullying			exclusion (information processing)
Corporate espionage			

Bron: Hogben (2007), Gross & Acquisti (2005), Jones & Soltron (2005) Solove (2006)

Zoals is gebleken, zijn niet alle onderzoeken gericht op sociale netwerksites. Solove bijvoorbeeld, richt zich op privacy in het algemeen. Daarnaast valt op dat enkele risico's overeenkomen of elkaar overlappen. Daarom is gekozen om deze risico's uitvoerig te bestuderen en in verband met elkaar te brengen. Op deze manier is een lijst met privacyrisico's ontstaan die een overzicht biedt van de mogelijke privacyrisico's die door gebruikers genoemd kunnen worden (zie tabel 6). Om de risico's te kunnen categoriseren is gekozen voor de indeling van Solove, omdat blijkt dat veel van de risico's binnen deze vier groepen te plaatsen zijn.

Tabel 6: *Overzicht van mogelijke privacyrisico's (die door gebruikers genoemd zouden kunnen worden)*

	inbreuk op de privacy, risico	risico's genoemd in eerdere onderzoeken
(1)Informatie verzamelen	toezicht/bewaking	surveillance
	ondervraging/uithoring	interrogation
	verliezen van controle	incomplete access controls/lack of user control of information
(2)Informatie opslaan en gebruiken	aggregeren van gegevens	aggregation
	herkenning	identification, face- recognition, CBIR -->interrogation, distortion
	wachtwoord onderscheppen	password interception
	data gebruiken voor andere doeleinden	secondary use-->breach of confidentiality
	uitsluiting, niet informeren van personen	exclusion
	digitaal dossier	buiding digital dossier, digital dossier aggregation
(3)Informatie verspreiden	openbaring	disclosure, disclosure tot advertisers,database reverse-enigineering
	direct marketing	secondary data collection, commercial datamining
	bekendmaken	exposure, breach of confidentiality
	vervorming, verdraaiing	distortion
	afpersing	blackmail
(4)Schending	binnendringen	intrusion, infiltration in networks
	spam	spam
	stalken	stalking
	intimideren	bullying
	identiteit overnemen	identity theft, profile squatting

In de eerste kolom staan de 4 categorieën van Solove. De mogelijke privacyrisico's staan in de kolom daarnaast. In de derde kolom zijn de privacyrisico's, die in dit hoofdstuk aan de orde zijn gekomen, ondergebracht waarbij risico's die veel overeenkomsten hebben met elkaar, zijn samengebracht.

Een laatste punt dat meegenomen wordt in dit onderzoek betreft de invloed van leeftijd op mogelijke verschillen tussen gebruikers. Gekeken zal worden of privacybewustzijn en privacybezorgdheid tussen leeftijdsgroepen duidelijk van elkaar verschillen en hoe dit dan tot uiting komt. Uit eerdere onderzoeken bleek namelijk dat gebruikers, en dan vooral jongeren, veel informatie prijs geven op de sociale netwerksites en zich niet altijd bewust zijn van de mogelijkheden om bepaalde gegevens af te schermen. Wanneer gevraagd zou worden naar hun privacybezorgdheid zou echter wel naar voren kunnen komen dat ze inderdaad bezorgd zijn. In hun gedrag komt dit echter niet tot uiting. In dit onderzoek zal dan ook gekeken worden naar de mate van privacybezorgdheid, de risico's die de gebruikers noemen en de manier waarop zij willen dat hun privacy gewaarborgd wordt of zou moeten worden.

<u>Betekenis van de theorie voor onderzoek naar de privacywaarborging door de aanbieder</u>

Ook biedt de theorie aanknopingspunten voor de bestudering van de internetdienst zelf. Naar aanleiding van de risico's die uit eerdere onderzoeken naar voren zijn gekomen, zijn enkele vragen opgesteld. Op deze manier wordt onderzocht welke mogelijke risico's er kunnen zijn binnen een sociale netwerksite. Voorbeelden zijn: Hoe waarborgen aanbieders de privacy van gebruikers? Door het afschermen van bepaalde informatie voor groepen mensen? Op welke manieren? Hoe en waarom? Deze vragen die in tabel 7 zijn beschreven, gelden als richtlijn voor de inhoudsanalyse en zouden mogelijk de risico's die in tabel 6 zijn beschreven tot gevolg kunnen hebben.

Tabel 7: *Template voor bestudering van sociale netwerksites*

	mogelijke privacy bedreigingen, risico (oorzaak)
(1)Informatie verzamelen	Welke gegevens kunnen worden getoond? Mogelijkheden om persoonlijke gegevens af te schermen voor anderen? Mogelijkheid om onderscheid te maken tussen type gebruikers binnen de eigen vriendengroep? Mogelijkheid om mensen te weigeren? Mogelijkheid om profiel te deleten? Standaard instellingen?
(2)Informatie opslaan en gebruiken	Identificeerbaar, identiteit te herleiden, traceerbaarheid van gegevens naar persoon? Links met andere sites mogelijk? uitwisselen en koppelen van gegevens? Opbouwen van een digitaal dossier? bewaartermijn gegevens ? Zorgvuldig omgaan met gegevens. Hoe wordt er omgegaan met privacy bescherming ?
(3)Informatie verspreiden	Gegevens beschikbaar voor derden? Gegevens beschikbaar voor commerciële doeleinden?
(4)Schending	Veiligheid binnen de site en de dienst zelf? Privacy verklaring duidelijk? Inzage in wat met gegevens gebeurt ? Herleiden van sociale netwerken?

4. DE CASESTUDY ALS ONDERZOEKSMETHODE

Dit hoofdstuk behandelt de opzet van het onderzoek. Daarbij wordt ingegaan op de methode van onderzoek, het onderzoeksobject en de methode van dataverzameling en data-analyse.

4.1 Casestudy

Zoals al gebleken is bij de definiëring van de hoofdvraag en deelvragen, worden in dit onderzoek twee kanten van privacy belicht. Zowel de aanbieders van sociale netwerksites als de gebruikers staan centraal. Gekozen is om deze twee kanten van privacy door middel van een casestudy te onderzoeken. Een casestudy wordt ook wel gevalstudie genoemd en wordt door Peters (2001), die Goode en Hatt citeert (1992), als volgt uitgelegd: 'bij een gevalsstudie gaat het om de intensieve bestudering van een verschijnsel binnen zijn natuurlijke situatie, zodanig dat de verwevenheid van relevante factoren blijft behouden' (Peters, 2001:15).

Voor het doen van een casestudy is gekozen, omdat deze methode van onderzoek één geval of object uitvoerig bestudeerd. De hoofdvraag, deelvragen en subdeelvragen lenen zich goed voor deze methode van onderzoek, omdat vooral de subdeelvragen, een uitgebreid antwoord wensen. Zonder deze diepgang is het moeilijk om een goed onderbouwd antwoord te formuleren op de hoofdvraag.

Bovendien is voor deze methode van onderzoek gekozen, omdat binnen de casestudymethode verschillende onderzoeksmethoden gehanteerd kunnen worden. In dit onderzoek is hier ook voor gekozen. In tabel 8 is te zien welke methoden van dataverzameling zijn gebruikt voor beantwoording van de deelvragen. Hierbij gaat het om kwalitatieve methoden van onderzoek. Hiervoor is gekozen, omdat het gaat om een minder concreet onderwerp (privacy) en het onderzoek daarnaast gericht is op de beleving van privacy door gebruikers. De diverse methoden van onderzoek worden in paragraaf 4.4 uitgebreid besproken.

Tabel 8: *Methoden van dataverzameling per deelvraag*

Deelvragen	Methode van dataverzameling
Deelonderzoek 1: Waarborging door aanbieder **In hoeverre spelen aanbieders van sociale netwerksites in op de privacywaarborging van gebruikers van deze sites?** Hierbij horen de subdeelvragen a en b	inhoudsanalyse, interview, literatuuronderzoek
Deelonderzoek 2: Gebruikersonderzoek **Hoe beleven gebruikers van sociale netwerksites hun online privacy?** Hierbij horen de subdeelvragen c t/m h	Focusgroepgesprekken literatuuronderzoek

4.2 Selectie en verantwoording case

Voordat een keuze is gemaakt voor de case, is deskresearch uitgevoerd. Dit onderzoek is uitgevoerd door middel van literatuuronderzoek van drie sociale netwerksites, namelijk Myspace, Hyves en Facebook. Voor deze drie sociale netwerken is gekozen, omdat zij voorkomen in de top 10 van meest gebruikte sociale netwerksites in Nederland en een redelijk brede doelgroep hebben. Criteria die zijn meegenomen en een rol hebben gespeeld in de uiteindelijke keuze voor de sociale netwerksite, zijn de volgende: (1) functionaliteiten binnen de dienst, (2) de populariteit van de dienst in Nederland en (3) de doelgroep.

Hoewel uit onderzoek van Gross en Acquisti (2005) blijkt dat er grote verschillen zijn in het tonen van gegevens tussen verschillende sociale netwerksites, verschillen Facebook, Myspace en Hyves qua type dienst en het tonen van gegevens niet heel erg sterk van elkaar. Het zijn alle drie algemene sociale netwerksites die ongeveer dezelfde functionaliteiten bieden. Gross & Acquisti (2005) geven een aantal mogelijkheden van het doel van sociale netwerksites. Bij Hyves, Myspace en Facebook gaat het vooral om de eerste, namelijk het tonen van een profiel: een representatie van de gebruiker en zijn of haar contacten, met de intentie om in contact te komen met anderen. Wel hebben ze elk een eigen doelgroep, waar zij zich bij de oprichting vooral op gefocust hebben. In het kort zal daarom per site worden ingegaan op de doelgroep, het aantal leden en de populariteit van de sociale netwerksite in Nederland.

Facebook is, zoals op de website zelf kenbaar wordt gemaakt, een (…)'social utility that connects you with the people around you' (Facebook, 2008). De sociale netwerksite is ontwikkeld door Mark Zuckerberg en is sinds 4 februari 2004 online. Microsoft heeft een belang van 1,6 procent in de sociale netwerksite.

Afbeelding 1: *Logo Facebook*

Bron: facebook.com

De Amerikaanse site heeft op dit moment ongeveer 70 miljoen actieve leden (Facebook Factsheet, 2008). Dit aantal is gebaseerd op de leden die binnen één maand meerdere keren actief waren op de site. Volgens de statistieken van Facebook zelf keert 45 procent van de Facebook-gebruikers iedere dag terug naar de site (Facebook Statistics, 2008). Wie deze gebruikers precies zijn is niet duidelijk. Aanvankelijk bestond de groep gebruikers uit studenten en was het netwerk ook alleen beschikbaar voor studenten. Echter, statistieken wijzen nu uit dat de helft van de Facebook-gebruikers niet meer aan het studeren is en dat de groep die het meest groeit de groep met personen van 25 jaar en ouder is. Ook wereldwijd groeit Facebook nog steeds. De landen met het grootste aantal actieve gebruikers zijn Amerika, Engeland en Canada. Nederland komt niet voor in de top tien van landen met de meeste gebruikers. Met 236.000 bezoekers per maand staat Facebook in Nederland

op plaats acht wat betreft de meest gebruikte sociale netwerksites in februari 2008, zoals in tabel 9 te zien is (Ymerce Social Networking, 2008).

Tabel 9: *Meest populaire sociale netwerksites in Nederland (X 1000, februari 2008)*

		Unieke bezoekers		**Dagelijkse bezoekers**		**Bekeken pagina's**	
		jan-08	feb-08	jan-08	feb-08	jan-08	feb-08
	Total audience	*10,99*	*10,86*	*6,946*	*6,937*	*38,014*	*35,175*
1	Hyves	4,981	5,187	1,658	1,7	2,89	2,832
2	Live Spaces	2,356	1,991	184	153	27	18
3	Schoolbank	1,023	919	77	69	36	31
4	Partyflock	995	915	181	190	553	488
5	MySpace	621	508	55	37	28	19
6	Netlog	428	400	82	74	201	111
7	HI5	387	393	49	54	64	60
8	Facebook	304	236	45	28	53	15
9	Linkedin	267	236	18	12	3	3
10	Superdudes	292	229	50	40	42	30

Bron: Comscore, 2008 in Ymerce-Social Networking. 2008. Social networking diensten in Nederland.

Ook Myspace, één van de grootste sociale netwerksites, is in Nederland niet te vinden in de top drie van meeste bezoekers in de maanden januari en februari van dit jaar. Met 508.000 unieke bezoekers is Myspace te vinden op plaats vijf in Nederland (Ymerce-Social Networking, 2007). Wereldwijd had Myspace in mei 2007 meer dan 67 miljoen bezoekers (Derksen, 2007). MySpace is een online community waar je in contact kunt komen met vrienden en vrienden van jouw vrienden. De sociale netwerksite is door Tom Anderson in augustus 2003 opgezet en is vooral bekend geworden als bron van nieuw muzikaal talent. Het bekendste voorbeeld is de doorbraak van de Arctic Monkeys.

Afbeelding 2: *Logo Myspace (Nederland)*

Bron: www.myspace.nl

Facebook en Myspace zijn dus vooral internationaal gezien erg populair, maar kunnen in Nederland op dit moment nog niet echt partij bieden aan Hyves. Hoewel Myspace met een Nederlandse versie van de site het waarschijnlijk in Nederland wel beter zal gaan doen, staat Hyves in Nederland op ruime voorsprong wat betreft aantal leden. Hyves is een gratis online profielennetwerk, gericht op het onderhouden van sociale contacten. De dienst is ontwikkeld door Raymond Spanjar, Koen Kam en Floris Rost van Tonningen en is online sinds 2004.

Afbeelding 3: *Logo Hyves*

Bron: www.hyves.nl

Joop van den Ende heeft sinds 4 april 2008 een belang in het sociale netwerk. De omvang van het belang is niet bekend gemaakt. Wel is duidelijk dat het gaat om een flinke investering. Volgens RTL Nieuws zou het gaan om een belang van tussen de 20 en 30 procent (RTL Nieuws, 2008). Van den Ende & Deitmers gebruiken hun Crossmedia Fund om te investeren in Hyves. Dat fonds heeft een omvang van 100 miljoen euro (Starkenburg, 2008). De site is, net zoals Facebook, gestart als sociaal netwerk voor studenten, maar was wel voor iedereen vanaf het eerste begin toegankelijk. Tegenwoordig zijn het niet alleen de studenten die actief zijn op Hyves. Van alle Nederlanders die actief zijn op sociale netwerken, geeft 83 procent aan het meest actief te zijn op Hyves, zoals in hoofdstuk twee ook al aan de orde is gesteld. Het meest actief binnen deze site zijn personen van 13 tot en met 34 jaar. In Nederland maakt 70 procent van de tieners (13-19 jaar) gebruik van Hyves en in de leeftijdsgroep 20-34 jaar is dit 74 procent (Ymerce Hyves, 2008).

Tabel 10: *Gebruik van Hyves per leeftijdsgroep (februari 2008)*

Leeftijd	Bereik	Absoluut bereik	Aantal bezoeken	Bezoeken per maand
13-19	70,3%	978.000	18.608.000	19,03
20-34	73,6%	2.260.000	47.925.000	21,21
35-49	53,1%	2.035.000	35.769.000	17,58
50-ouder	21,8%	1.157.000	11.397.000	9,85

Bron: Ymerce-Hyves. 2008. Leuke Hyves-cijfertjes voor het weekend.

Onderzoek van Ernst & Young (2007) wees uit dat 49 procent van de leden van Hyves tussen de 16 en 34 jaar oud is. In totaal heeft Hyves nu zo'n 6 miljoen leden en zo'n 1700.000 bezoekers per dag (Ymerce Hyves, 2008). Van alle gebruikers van Hyves is maar liefst 91,5% afkomstig uit Nederland. Verder is Hyves redelijk populair in China (4.3%) en in Duitsland (1.0%) (Alexa, 2008).

Kortom, Hyves is in Nederland verreweg de meest populaire sociale netwerksite en heeft een groot draagvlak onder internetgebruikers van verschillende leeftijden. Daarnaast verschillen de type diensten en tools die Hyves aanbiedt niet wezenlijk van die van Facebook of Myspace. Volgens de algemeen directeur van Hyves, Raymond Spanjar, is Hyves zelfs een combinatie van Facebook en Myspace: 'We proberen de beste dingen van beide netwerken te combineren, en proberen ze te optimaliseren' (Bertrams, 2008). Om bovenstaande redenen is Hyves in dit onderzoek bestudeerd door middel van de casestudymethode.

4.3 Onderzoeksobject

Om personen naar hun privacybeleving te kunnen vragen, moet helder zijn hoe dit begrip, maar ook andere begrippen uit de vraagstelling, deelvragen en subdeelvragen geoperationaliseerd worden. Beleving is een lastig begrip en een definitie is dan ook niet gemakkelijk te geven. Het begrip is vooral contextgebonden en vaak is het zo dat verschillende indicatoren samen de beleving van mensen over een bepaald onderwerp weergeven. Beleving kan het best omschreven worden als de waardering van en ervaringen met een bepaald onderwerp of object. In dit geval dus privacy op sociale netwerksites.

In vorige hoofdstukken is uitgelegd wat in dit onderzoek wordt verstaan onder een sociale netwerksite en onder het begrip 'privacy'. Met online privacy wordt privacy op het internet bedoeld. Privacyissues zijn privacyonderwerpen of privacykwesties. Wanneer over privacywaarborging wordt gesproken, wordt de bescherming van privacy door zowel aanbieders als gebruikers bedoeld. Bovendien komen de begrippen privacybezorgdheid en privacybewustzijn aan de orde in dit onderzoek. Onder privacybewustzijn wordt het nadenken over privacy en de actie die wordt ondernomen om privacy te beschermen bedoeld. Privacybezorgdheid gaat over de ongerustheid over privacy en privacyissues.

4.4. Diverse methoden van onderzoek

Zoals in paragraaf 4.1 kort is aangegeven, is gebruik gemaakt van diverse methoden van onderzoek binnen de casestudy. De onderzoeksmethoden zullen in de volgende paragrafen uitgebreid aan bod komen.

4.4.1 Focusgroeponderzoek

Voor focusgroeponderzoek is gekozen, omdat het in dit onderzoek vooral gaat om het achterhalen van wat speelt binnen bepaalde groepen. In dit onderzoek draait het om de gebruikers van online sociale netwerken en dan vooral de effecten van de verschillen in leeftijd (zie paragraaf 3.4). De verwachting bij focusgroepen is dat door middel van interactie de gedeelde en/of beter geëxpliciteerde opvattingen achterhaald kunnen worden. Precies om deze reden is ervoor gekozen om focusgroepgesprekken te voeren in plaats van interviews te houden. Zoals Van Selm en Wester stellen: 'Doordat de groepsinteractie als middel gebruikt wordt, kunnen deelnemers elkaar aanvullen in het blootleggen van wat belangrijke subculturele kenmerken en perspectieven zijn en kunnen deelnemers elkaar corrigeren en bijsturen in het definiëren van normatieve grenzen' (in: Wester, Renckstorf & Scheepers, 2006: 544).

Uitvoering

De focusgroepmethode is in dit onderzoek als onderdeel van de casestudy gehanteerd. Twee focusgroep sessies van ongeveer twee uur vonden op 17 en 31 mei 2008 plaats op de Erasmus Universiteit. De groepsgesprekken zijn gevoerd aan de hand van een topiclijst. De topiclijsten zijn te vinden in bijlagen 1 en 2.
Deze lijsten zijn nagenoeg hetzelfde, maar zijn wat betreft taalgebruik zoveel mogelijk aangepast aan de leeftijd van de respondenten. De topiclijsten zijn tot stand gekomen naar aanleiding van de begrippen uit het

theoretisch kader, waarna 'sensitizing concepts' zijn gecreëerd; richtinggevende of attenderende concepten waar vanuit de situatie geanalyseerd kan worden (Wester & Peters, 2004:24). Voorbeelden van 'sensitizing concepts' zijn privacy, privacywaarden, privacyrisico's en privacywaarborging. Deze begrippen zijn vervolgens omgezet in de topiclijst: de onderwerpen die tijdens het gesprek aan bod moesten komen. De volgorde van de topics stond hierbij vast, hoewel er ruimte was om gaande het gesprek al in te gaan op onderwerpen die pas later op de agenda stonden. In dit onderzoek is dus gebruik gemaakt van een semi-gestructureerde vragenlijst, waarbij wel voornamelijk open vragen werden gesteld. De groepsgesprekken zijn opgenomen op een recorder en daarnaast zijn aantekeningen gemaakt.

Verantwoording respondenten

Uit het onderzoek van Paine et al. (2007) naar de privacybezorgdheid bleek dat naarmate mensen ouder zijn zij bezorgder zijn over hun privacy. In dit onderzoek is daarom ook onderscheid gemaakt tussen verschillende leeftijdsgroepen. In eerste instantie is uitgegaan van de groep 12 tot en met 18 jaar, aangezien dit een groep is die op de middelbare school zit en naar verwachting niet zo erg bezorgd is over privacy. Personen in de leeftijd van 24 tot en met 30 jaar zijn uitgekozen omdat zij niet (helemaal) met het internet zijn opgegroeid en nu zij op de arbeidsmarkt actief zijn wellicht anders over hun privacy in de sociale netwerken denken. Verwacht werd dat de tweede groep een hogere privacybezorgdheid kent en meer waarden en risico's zou noemen. Voor deze groepen is bovendien gekozen omdat uit onderzoeken blijkt dat zij actief zijn op sociale netwerksites (Ernst & Young, 2007).

De respondentenwerving is volgens de sneeuwbalmethode verlopen. In deze methode vormt het netwerk van de onderzoeker de basis. Via dit netwerk zijn respondenten geworven door de onderzoeker. Om dit te bereiken is Hyves ingezet. Aan de geïnteresseerden is gevraagd het verzoek om mee te werken aan het onderzoek ook in hun netwerk te verspreiden. Uiteindelijk zijn 12 personen bereid gevonden om deel te nemen aan een groepsgesprek. Zes personen in de leeftijd van 13 tot en met 18 jaar deden mee aan het onderzoek. Het bleek niet mogelijk om nog iemand van 12 jaar te vinden, maar de respondent van 13 was net een paar weken daarvoor jarig geweest en zat zelfs nog op de basisschool. Daarnaast is aan mensen in de leeftijd van 24 tot en met 30 jaar gevraagd aan het onderzoek mee te doen. Vooral het vinden van personen in de leeftijd van 27 tot en met 30 jaar bleek moeilijk te zijn. Daarom is besloten om één persoon van 31 jaar te betrekken in het onderzoek.

Het onderzoek maakt tevens gebruik van een doelgerichte steekproefstrategie. Dit betekent dat de respondenten niet op basis van gemak of zelfselectie uitgekozen worden, maar op basis van een zo goed mogelijke representatie van het veld waarover onderzoek wordt gedaan. Daarom is geprobeerd om mensen van verschillende leeftijden en opleidingsniveaus te selecteren, waarbij is gekozen voor personen met een hogere opleiding (HAVO, VWO, HBO en WO). Uit cijfers blijkt namelijk dat het grootste gedeelte van de Hyvers hoog opgeleid is (Kol, 2008). Bovendien was de verwachting dat zij zich gemakkelijker konden uitdrukken. Dit is

vooral belangrijk bij de jongere groep. Tevens is getracht evenveel mannelijke als vrouwelijke deelnemers te benaderen, waardoor de groepen alleen wat betreft leeftijd van elkaar verschilden. In tabel 11 en tabel 12 worden de fictieve namen en bijbehorende gegevens van de respondenten getoond.

Tabel 11: *Respondenten van focusgroep A (17 mei 2008)*

Naam	**leeftijd**	***opleidingsniveau***
Brenda	24	HBO
Karlijn	24	HBO
Peter	25	HBO
Sander	26	WO
Claudia	30	HBO
Tom	31	WO

Tabel 12*: Respondenten van focusgroep B (31 mei 2008)*

Naam	**leeftijd**	***opleidingsniveau***
Sjoerd	13	Havo/Vwo
Liza	13	Havo/Vwo
Simone	16	Havo
Marcel	16	Vwo
Kim	17	Havo
Jacqueline	18	Vwo

4.4.2 Inhoudsanalyse

Naast focusgroeponderzoek is inhoudsanalyse als methode gehanteerd. Hierbij ging het om een inhoudsanalyse van wat mogelijk is binnen Hyves en hoe de privacy door de aanbieder wordt gewaarborgd. Volgens Wester (2006) is 'inhoudsanalyse een systematische vorm van lezen om waarnemingen te doen' (Wester, 2006 in Wester et al. 2006:16). Voor het lezen wordt daarbij uitgegaan van een vraagstelling, die richting geeft aan de te lezen inhoud. Daarnaast bepaalt het interpretatiekader hoe naar deze inhoud gekeken zal worden (Wester, 2006 in Wester et al. 2006). Uiteindelijk bepaalt het waarnemingsinstrument hoe het materiaal precies bestudeerd zal worden. Voor deze methode van onderzoek is gekozen omdat op deze manier te achterhalen is wat aanbieders op dit moment doen aan privacywaarborging zonder dat sprake is van een inbreuk op de gewone gang van zaken (Wester, 2006 in Wester et al. 2006). De website is namelijk in zijn natuurlijke situatie bestudeerd zonder dat iets of iemand in de weg staat.

4.4.3 Interview

Tevens is gekozen om een diepte-interview te houden. Op deze manier kon achterhaald worden waarom er door de internetdienst op een bepaalde manier met privacy wordt omgegaan en welke overwegingen daarbij een rol spelen. Om dus een duidelijker beeld te krijgen van Hyves is getracht experts of werknemers van Hyves te interviewen. Hyves was echter niet bereid om mee te werken aan het onderzoek. Eva Kol, auteur van het

boek ‘Hyves’ was wel bereid om bij te dragen. Zij liep stage bij Hyves, kwam er vervolgens in dienst en studeerde vorig jaar af aan de masteropleiding Communicatie- en Informatiewetenschappen en Nieuwe Media aan de Universiteit van Amsterdam. In het interview met haar is onder andere aandacht uitgegaan naar het succes van Hyves, de keuzes die Hyves maakt ten aanzien van de privacywaarborging en in hoeverre er verantwoordelijkheid ligt bij Hyves om gebruikers op de hoogte te stellen van mogelijke risico’s. De topiclijst die bij het interview is gebruikt, is in bijlage 3 te vinden.

4.4.4 Literatuuronderzoek

Bestaande bronnen zijn ook meegenomen als aanvulling op de data die door middel van de inhoudsanalyse van Hyves en het interview zijn verkregen. Deze drie methoden van gegevensverzameling zorgen samen voor de data op basis waarvan, na analyse, antwoord gegeven kan worden op deelvraag 1 en de subdeelvragen a en b (zie paragraaf 1.3).

4.5 Analyse methodes

De analyse van de focusgroepgesprekken en het diepte-interview is gebaseerd op de audiotapes die gemaakt zijn en de notities van de onderzoeker. In de eerste plaats zijn de groepsgesprekken aan de hand van de audio-tapes getranscribeerd. De verkregen data, afkomstig uit de groepsgesprekken, is vervolgens met behulp van de gefundeerde theoriebenadering geanalyseerd. De vier stappen (exploratie, specificatie, reductie en integratie) die de gefundeerde theoriebenadering kent (Wester & Peters, 2004) zijn in dit onderzoek dan ook doorlopen. De *exploratiefase* bestaat uit de eerste ordening van het materiaal: het *open coderen* (Glaser & Strauss, 1967). Op een verkennende manier zijn codes gegeven aan bepaalde passages, zinnen en stukken uit de transcripties door trefwoorden te noteren in de kantlijnen. Nadat de belangrijkste stukken waren voorzien van codes, zijn in de *specificatiefase* de transcripties bij elkaar gelegd en voorzien van overkoepelende thema’s. Naar aanleiding van de verschillende thema’s is daarna in de *reductiefase* op zoek gegaan naar de belangrijkste onderdelen binnen de thema’s. In de *integratiefase* is tenslotte de relatie gelegd tussen de verschillende focusgroepen en zijn overeenkomsten en verschillen geconstrueerd.

De analyse van de sociale netwerksite Hyves bestond uit analyse van de privacywaarborging van deze website. Vaak wordt onderscheid gemaakt tussen twee typen inhoudsanalyse: de kwalitatief-interpreterende inhoudsanalyse en het kwantitatief-beschrijvende type. In dit onderzoek is vooral gebruik gemaakt van de kwalitatief-interpreterende inhoudsanalyse, hoewel van te voren wel een aantal vragen zijn opgesteld op basis waarvan de site is geanalyseerd. De mogelijkheid om van de vragen af te wijken was dus aanwezig. Bovendien sluit het doel van dit soort onderzoek: ‘exploratie of beschrijving in de vorm van een illustratie aan de hand van een centraal begrip of nieuw geformuleerde typen’ (Wester, 2006 in Wester et al. 2006:27) goed aan bij dit type inhoudsanalyse. Daarnaast zijn overige bronnen meegenomen in de analyse, waardoor het één en ander verduidelijkt of bevestigd kon worden. De analyse van het interview is niet aan de hand van de gefundeerde theoriebenadering gebeurd. De verkregen data is als nieuwe bron gebruikt, die de data verkregen door middel

van de inhoudsanalyse hier en daar kan versterken en verduidelijken.

4.6 Principes van dit onderzoek

In dit onderzoek is het analyseren sterk verbonden met het theoretische gedeelte en is het analyseren daarnaast ook gezien als een steeds terugkomende fase in het onderzoek. Er wordt daarom ook wel gesproken over een cyclisch proces. De cyclus van dit onderzoek bestaat namelijk uit dataverzameling, analyse, reflectie en toetsing (Wester & Peters, 2004). Door de verschillende methoden van onderzoek, die gehanteerd zijn, zijn tijdens de uitvoering van het onderzoek nog wijzigingen opgetreden. De twee deelvragen staan namelijk sterk in verbinding met elkaar. Resultaten van de inhoudsanalyse bleken gevolgen te hebben voor de topiclijst.

Bovendien is de rol van de onderzoeker, vooral bij de focusgroepgesprekken, van groot belang. Gespreksleiders kunnen namelijk verschillende rollen op zich nemen. In dit onderzoek heeft de gespreksleider de rol van 'de goed geïnformeerde 'speurder naar wijsheid' gehanteerd, die door Krueger als één van de mogelijke rolopvattingen wordt gezien (Wester et al. 2006: 551). Daarnaast is getracht om groepsconformiteit en groepspolarisatie te voorkomen. Dit kan het gesprek in de weg staan en de sfeer kan hierdoor verslechteren. Om ervaring op te doen, is in april een proeffocusgroepgesprek van ongeveer 20 minuten gehouden met studiegenoten van de opleiding Media en Journalistiek. Een tweede punt dat belangrijk is, omdat het kan bijdrage aan de geldigheid van het onderzoek, is dat van te voren vooronderstellingen duidelijk worden en deze daardoor juist niet mee worden genomen in het onderzoek zelf. Deze zijn dan ook vooraf op papier gezet.

4.7 Samenvatting en conclusie

In dit hoofdstuk is ingegaan op de methoden van onderzoek die binnen de casestudy gehanteerd zijn: inhoudsanalyse, focusgroeponderzoek, interviews en literatuuronderzoek. Tabel 13 geeft per subdeelvraag weer welke methoden van onderzoek en analyse gebruikt zijn.

Tabel 13: *Overzicht methoden van dataverzameling en data-analyse per subdeelvraag*

subdeelvragen	Methode van dataverzameling	Methode van data-analyse
a. Hoe waarborgen aanbieders de privacy van gebruikers op dit moment en welke overwegingen spelen daarbij een rol?	inhoudsanalyse, interviews, literatuuronderzoek	kwalitatieve analyse
b. Wat zijn mogelijke privacybeperkingen/risico's binnen sociale netwerksites?	inhoudsanalyse, interviews, literatuuronderzoek	kwalitatieve analyse
c. Hoe definiëren gebruikers van sociale netwerksites hun privacy en welke waarden vinden zij belangrijk met betrekking tot hun privacy?	Focus group	gefundeerde theorie benadering
d. In hoeverre houden gebruikers van sociale netwerksites zich bezig met privacyissues op sociale netwerksites?	Focus group	gefundeerde theorie benadering
e. Welke risico's zien zij voor hun privacy in online sociale netwerken?	Focus group	gefundeerde theorie benadering
f. In hoeverre vinden gebruikers dat sociale netwerksites hun privacy waarborgen?	Focus group	gefundeerde theorie benadering
g. Wat willen gebruikers zelf met betrekking tot hun privacy?	Focus group	gefundeerde theorie benadering
h. In hoeverre zijn er verschillen te ontdekken tussen leeftijdsgroepen?	Focus group	gefundeerde theorie benadering/analyse na beantwoording van deelvragen a t/m e

In de hoofdstukken vijf en zes zal antwoord gegeven worden op bovenstaande vragen. De subdeelvragen a en b zullen in hoofdstuk vijf beantwoord worden. De overige vragen komen in hoofdstuk zes aan de orde.

Tabel 14 geeft weer welke onderwerpen in de volgende twee hoofdstukken besproken worden. Deze komen voort uit de overzichten die in hoofdstuk drie zijn gegeven in tabel 6 en 7 (vooral hoofdstuk zes) en de topiclijsten (vooral hoofdstuk zeven) die te vinden zijn in bijlagen 1 en 2.

Tabel 14: *Overzicht van onderwerpen die in de resultatenhoofdstukken worden besproken*

Hoofdstuk 6	Hoofdstuk 7
Diensten	Algemene mening over Hyves
Verdienmodel	Definitie
Informatie opslaan	Waarden
Informatie gebruiken	Houding ten opzichte van Hyves
Informatie verspreiden	Mogelijke risico's binnen Hyves
Privacyschendingen	Privacywaarborging binnen en door Hyves

5. PRIVACYWAARBORGING EN PRIVACYBEPERKINGEN BINNEN HYVES

'Ik denk dat er misschien wel een verantwoordelijkheid ligt bij Hyves. Ja, eigenlijk om vooral jonge gebruikers bewust te maken van de risico's' (Eva Kol).

In dit hoofdstuk wordt verslag gedaan van de resultaten van de inhoudsanalyse, het interview en het literatuuronderzoek, bekeken vanuit het perspectief van de sociale netwerksite Hyves. De volgende vraag wordt in de conclusie van dit hoofdstuk beantwoord: ***In hoeverre waarborgen aanbieders van sociale netwerksites de privacy van gebruikers binnen deze sites?*** Om deze vraag te kunnen beantwoorden gaat in dit hoofdstuk aandacht uit naar subdeelvragen a en b.

5.1 Hyves in het algemeen

In de volgende paragrafen worden de belangrijkste diensten en tools die Hyves aanbiedt besproken. Daarnaast gaat aandacht uit naar het verdienmodel dat Hyves hanteert.

5.1.1 De diensten

Eén van de onderdelen van een sociale netwerksite is het profiel. Via het profiel wordt de gebruiker in staat gesteld om zichzelf te presenteren. De gebruiker bepaalt welke gegevens daarbij getoond worden. Het Hyves profiel maakt onderdeel uit van de profielpagina van de gebruiker. Op deze pagina zijn nog veel meer toepassingen te vinden, zoals vrienden, WieWatWaar, Hyves (groepen) enzovoorts.

Op de profielpagina kan de gebruiker zien welke negen *vrienden* als laatsten zijn ingelogd. Deze vrienden worden op de pagina weergegeven door middel van de naam van deze persoon en de profielfoto. Daarnaast toont de profielpagina de *video's* en *foto's* van de gebruiker afgebeeld en ook eventuele *tips* of *polls*. Bovendien kunnen leden zich aanmelden bij thematische groepen, *Hyves (groepen)*, waarmee zij zich graag associëren. Voorbeelden van Hyves (groepen) zijn scholen, tv-series en verenigingen. Tot slot kunnen er bij *gadgets* nog tal van filmpjes, slideshows en muziekfragmenten toegevoegd worden.

Sinds 24 april 2008 is het ook mogelijk om als gebruiker alle activiteiten op Hyves uit jouw vriendennetwerk te zien. Door Hyves wordt deze tool *Buzz* genoemd. Zowel op de homepage als op de profielpagina is het mogelijk om te zien wat andere gebruikers doen zoals het plaatsen van reacties, foto's, blogs, nieuwe WieWatWaar berichten en het accepteren van vrienden (Hyves, 2008).

Naast bovenstaande tools, is de 'krabbelfunctie' een belangrijk onderdeel van de profielpagina. *Krabbels* zijn korte berichtjes die gebruikers naar elkaar kunnen sturen. De berichten kunnen leuker gemaakt worden door de vele emoticons die toe te voegen zijn. Een andere mogelijkheid om te communiceren is via de zogenaamde *tik-tool*, waarmee de gebruiker zijn of haar vrienden een tik kan geven. Dit is een heel kort berichtje waarbij uit

een aantal zinnen te kiezen is; eventueel kan zelf een korte zin opgesteld worden. Zo kun je bijvoorbeeld iemand een drankje aanbieden of een knipoog geven. Verder wordt op de profielpagina de laatste *WieWatWaar* met datum weergegeven. Hier kan de persoon die de pagina bezoekt zien waar zijn of haar vriend(in) mee bezig is of was. Naast de krabbels, tikken en de WieWatwaar kan er bovendien via een *blog* gecommuniceerd worden. Over welk onderwerp dan ook kan de gebruiker een blog plaatsen op zijn of haar eigen profielpagina.

Afbeelding 4: *Homepage van Hyves*

Bron: www.hyves.nl

Hyves biedt een aantal applicaties die sterk web 2.0 georiënteerd zijn, zoals bijvoorbeeld de integratie van Google Maps, waardoor te zien is waar je vrienden wonen. Hierbij is het mogelijk om foto's toe te voegen op de kaart en zelf aan te geven waar je woont. Een dienst die hieraan verwant is en eveneens geïntegreerd kan worden in Hyves is Trackr. Trackr is een mobiele dienst waarmee je via GPS kan zien waar je vrienden zich bevinden.

Verder maakt de chatfunctie binnen Hyves het mogelijk om live met vrienden te praten. Deze functie lijkt op MSN Messenger en wordt door Hyves Kwekker genoemd. Binnen Hyves is het ook mogelijk om tags te plaatsen bij foto's, video's en blogs en kan de gebruiker een waarderingscijfer geven aan een foto. Ook bij het plaatsen van een tip is het mogelijk om een waardering aan te geven door middel van sterren (1-5).

5.1.2 Verdienmodel

Hyves is een gratis dienst. De gebruikers kunnen kosteloos gebruik maken van de diensten die de site aanbiedt. Om de site interessant te houden voor de gebruikers wordt door Hyves constant naar nieuwe applicaties gezocht die de site nog leuker maken (Kol, 2008). Hyves biedt gebruikers de mogelijkheid om Goldmember te worden tegen betaling, waardoor extra informatie te verkrijgen is. Wanneer een gebruiker Goldmember wordt, krijgt hij of zij inzicht in wie zijn of haar profiel bezoekt en waar dan naar gekeken wordt. Goldmembers zien dit alleen wanneer gebruikers toestemming hebben gegeven dat anderen dit kunnen zien. Ook krijgen zij bepaalde privileges waardoor zij hun pagina kunnen 'pimpen'. Bovendien hebben Goldmembers toegang tot meer smileys en kunnen zij meer vrienden toevoegen dan een gemiddelde gebruiker. Voor een gewone gebruiker is het maximum aantal vrienden vastgesteld op 750. Goldmembers kunnen bij het afsluiten van een halfjaar abonnement maar liefst 1000 vrienden toevoegen. De prijs voor het Goldmembership is vastgesteld op basis van het aantal maanden van het lidmaatschap en kost voor een jaar ongeveer € 25,00. Daarnaast heeft Hyves een fotodrukdienst, waaruit zij eveneens inkomsten genereert. De foto's uit de albums kunnen worden geprint en het is zelfs mogelijk om de afbeeldingen op posters en mokken te printen (Kol, 2008). Het Goldmembership en de fotodrukdienst zijn echter niet de belangrijkste inkomstenbronnen. De belangrijkste bron van inkomsten voor Hyves zijn namelijk advertenties. In eerste instantie vond het management een advertentiemodel niet bij Hyves passen, maar later werd dit model toch werkelijkheid, mede dankzij de enthousiaste reacties van leden (Kol, 2008). Via een forum was aan leden namelijk gevraagd naar hun mening over dit onderwerp.

Of Hyves in 2007 winst heeft gemaakt is niet zeker, maar wordt wel verwacht. Omzet- en winstcijfers maakt Hyves niet bekend. Wel bracht Raymond Spanjar in maart 2007 naar buiten dat Hyves in 2006 een bescheiden winst had gemaakt (Tomesen, 2007). Het is niet aannemelijk dat Hyves geen winst maakt.

5.2 Informatie verzamelen

Nu duidelijk is wat Hyves precies is en wat de mogelijkheden zijn binnen de dienst, wordt in de komende paragrafen ingegaan op hoe Hyves probeert de privacy van haar leden te waarborgen. Verder passeren de consequenties die dit mogelijk voor de gebruiker kan hebben de revue. De belangrijkste risico's en beperkingen, die gebruikers kunnen noemen, worden daarbij besproken. De risico's zijn gecategoriseerd aan de hand van de vier categorieën van Solove. Deze paragraaf start met de eerste categorie, namelijk informatie verzamelen. Daarbij gaat de aandacht uit naar welke gegevens personen moeten verstrekken, welke gegevens zij kunnen verstrekken en wat de mogelijke gevolgen hiervan zouden kunnen zijn.

5.2.1 Openbaar maken

Om je te registreren als Hyves-gebruiker, is het nodig om een aantal gegevens te verstrekken. Alleen naam, e-mailadres, gebruikersnaam en wachtwoord zijn verplicht. De overige gegevens zoals land, woonplaats, postcode, mobiele telefoonnummer, geslacht en geboortedatum zijn optioneel. Het inloggen op Hyves gebeurt door het invoeren van gebruikersnaam en wachtwoord.

Na registratie wordt de mogelijkheid geboden om je profiel uit te breiden. In het profiel kan de volgende informatie worden weergegeven:

Algemeen	Over mij, what's on my mind, relatie, verjaardag, leeftijd, religie, woonsituatie, woonplaats, scholen, mbo/hbo/universiteit, bedrijven, talen, mogelijkheid om zelf drie onderwerpen in te vullen, Contact: e-mail (zie instellingen, staat ingevuld) MSN en website
Foto	Mogelijkheid om een foto te uploaden
Interesses en Merken	Boeken, eten, films, gadgets, games, helden, media, muziek, overig, reizen, sport, tv-programma's, mijn merken
Spots	Mijn eigen privé spots (Spots zijn de nieuwe netwerken voor restaurants, bars en clubs! Nieuwe locaties toevoegen aan je profiel, spots van je vrienden
Gadgets	gadgets sorteren
Playlist	volgorde van de muziek wijzigen en opslaan

Bovenstaande lijst met gegevens die in het profiel getoond kunnen worden, komt aardig overeen met de gegevens die gebruikers op andere sociale netwerksites, zoals Orkut, Friendster, Friendzy, Tribe en Tickle, kunnen vermelden. Gevoel voor humor, seksuele geaardheid en aantal kinderen, die bij één of meer van deze sites ingevuld kunnen worden, komen bij Hyves niet voor. Bij Hyves is het wel mogelijk om drie onderwerpen naar keuze te bepalen en in te vullen.

Veel van de bovenstaande onderwerpen zijn niet verplicht in te vullen zoals al vermeld: alleen de naam van de gebruiker wordt standaard getoond en het e-mailadres van de gebruiker is te zien voor zijn of haar vrienden. De overige informatie kan ingevuld worden als de gebruiker dat wil. Hyves-gebruikers kunnen dus goed in de gaten houden welke informatie zij verstrekken.

5.2.2 Afschermen

De afgelopen jaren heeft Hyves steeds aanvullende mogelijkheden gecreëerd voor gebruikers waardoor zij zelf kunnen bepalen welke gegevens openbaar worden gemaakt en voor wie. Bovendien heeft Hyves toegezegd zich nog meer bezig te willen houden met bescherming van de privacy. Dit gaan zij onder andere doen met behulp van organisaties zoals Digibewust en Mijn Kind Online (Spits, 2007).

Dat Hyves het belang van privacy inziet, wordt duidelijk door de plek die privacy inneemt in de functies en applicaties die aangeboden worden op de site. Bij Hyves is via de interface Home en vervolgens My-account, alles te regelen wat met het account van de gebruiker te maken heeft. Deze pagina bevat de volgende onderwerpen: instellingen, privacy, profielinformatie, profielopmaak, toevoegen en tegoed. Onder privacy vallen de volgende onderwerpen: algemeen, WieWatWaar, chat, statistieken, blocklist en API & partner sites (beta).

Bij 'Algemeen' is het mogelijk om te kiezen uit vier categorieën. Gebruikers hebben de keuze om bepaalde gegevens beschikbaar te maken voor (1)Niemand, (2) Alleen vrienden, (3) Vrienden van Vrienden of (4) Hyvers. De meeste gegevens staan standaard ingesteld op "te zien voor Hyvers". E-mail is alleen te zien voor vrienden en de rest van de contactgegevens staan standaard ingesteld op "te zien voor niemand". Verder is het mogelijk om aan te geven voor wie de hele Hyvespagina te zien is. Hierbij kan de gebruiker een keuze maken uit vijf categorieën. Naast bovenstaande vier categorieën is het mogelijk om de Hyvespagina openbaar te maken voor iedereen. Wanneer de pagina opengezet wordt voor vrienden van vrienden is het wel mogelijk om andere onderdelen, zoals krabbels of foto's af te sluiten voor deze personen. Door Hyves is echter een beperking ingesteld voor het aantal keer dat de gebruiker zijn instellingen kan wijzigen voor de profielpagina in zijn geheel (vijf keer). De mogelijkheid om het profiel en de krabbels af te schermen is in de zomer van 2007 in het leven geroepen door Hyves (Van Soest, 2007). Veel Hyvers bleken deze mogelijkheid te willen gebruiken. Binnen een paar maanden hadden 70.000 leden hun profiel geblokkeerd. Toch blijkt dit nog steeds vrij weinig te zijn. Volgens de directeur van Hyves, Raymond Spanjar, ging het om minder dan 4procent in de eerste maanden (Van Soest, 2007).

Bij 'WieWatWaar' kan de gebruiker aangeven voor wie de oude WieWatWaar's (korte berichtjes waarin de gebruiker aangeeft waar hij of zij mee bezig is) te zien zijn. Daarnaast bestaat de mogelijkheid om te bepalen of de gebruiker de WieWatWaar geschiedenis vanaf nu wil tonen of vanaf het moment dat het lidmaatschap werd aangegaan. 'Chat' biedt de mogelijkheid om in te stellen wat je online status is: online, bezig, ben zo terug, away, aan de telefoon, lunchen, toon offline, en voor wie deze online status te zien is. Hierbij zijn er weer vier keuzemogelijkheden. De online status staat standaard op online en is zichtbaar voor Hyvers. Standaard staat aangevinkt dat alleen vrienden met de gebruiker mogen chatten. Daarnaast is het mogelijk om bepaalde vrienden uit te sluiten van de mogelijkheid om te chatten met de gebruiker. Bij 'Statistieken' kan de gebruiker aangeven of zijn of haar bezoeken aan andere profielen ook te zien zijn voor die personen. Het bekijken van de personen die het profiel van een gebruiker hebben bezocht is alleen mogelijk voor Goldmembers. Standaard staat ingesteld dat niemand te zien krijgt of je de pagina van een gebruiker bezocht hebt. Daarnaast is er een zwarte lijst. Hier kan toegevoegd worden wie niet te zien krijgen dat je op hun pagina bent geweest.

Bij 'Blocklist' kan de gebruiker zien wie hij of zij geblokkeerd heeft. Bij RSS kan de gebruiker instellen op welke content hij of zij de RSS feeds wil hebben. Op de website Marketingfacts wordt de volgende omschrijving gegeven van RSS: "RSS (of Really Simple Synication) is een toepassing van de metataal XML en wordt gebruikt om informatie op een website gelijktijdig beschikbaar te stellen aan derden. Internetgebruikers of websites die zijn geabonneerd op de RSS-feeds van een website krijgen automatisch een bericht als er nieuwe informatie op de betreffende website is geplaatst" (Marketingfacts, 2008). Bij Buzz instellingen kan de gebruiker bepalen voor wie Buzz te zien is, waarbij keuze is uit (1) niemand, (2) vrienden of (3) Hyvers. Tot slot kan de gebruiker bij 'API en partner sites' zien welke bedrijven de gebruiker toestemming heeft verleend voor het gebruik van zijn of haar gegevens. De lijst met bedrijven ontbreekt op dit moment alleen nog (17-7-2008). Niet opgenomen bij de

privacyinstellingen, maar wel mogelijk is het om bij Google Maps aan te geven wie mag zien waar je woont. Hier kan gekozen worden uit vijf categorieën, namelijk: (1)Niemand, (2) Alleen vrienden, (3) Vrienden van Vrienden (4) Hyvers of (5) iedereen. Dit geldt ook voor de foto's en video's die geplaatst kunnen worden. Wanneer er een tag geplaatst wordt bij een foto of video krijgt alleen de eigenaar van de foto of video te zien wie de tag geplaatst heeft. Overigens kunnen alleen vrienden een tag plaatsen.

Hoewel het dus mogelijk is voor gebruikers om zelf te bepalen welke gegevens voor wie openbaar worden, worden op Hyves bepaalde tools vanaf het begin openbaar gemaakt aan bepaalde groepen. De Buzz is standaard ingesteld op "te zien voor vrienden". Dit kan mogelijk door gebruikers als een privacyschending worden bestempeld, aangezien op deze manier precies bij te houden is wat iemand allemaal doet op Hyves; onder andere waar hij of zij reacties op plaats en wie hij of zij toevoegt aan de vriendenlijst. Door Eva Kol wordt dit bevestigd. Wel is het mogelijk om de gegevens te veranderen. Hier is geen limiet aan verbonden.

Het blijkt mogelijk te zijn om informatie te achterhalen over mensen via Hyves ook wanneer je geen lid bent van de sociale netwerksite. Soms is het wel zo dat personen hun profielen afschermen en dat daarom alleen de profielfoto en naam te zien zijn. Zoals eerder is gemeld, blijken relatief weinig gebruikers dit daadwerkelijk te doen. Doordat veel profielen dus openbaar zijn, zijn deze ook toegankelijk voor werkgevers. Kol gaat zowel in haar boek als in het interview in op het gebruik van Hyves door werkgevers. Volgens haar houdt niet iedereen er rekening mee dat ook (potentiële) werkgevers een kijkje nemen op het profiel van een gebruiker (Kol, 2008). Daarnaast merkt zij op dat ook de politie en de Belastingdienst Hyves gebruiken. Dat werkgevers inderdaad profielen van sollicitanten screenen, wordt door Dorien Smit, eigenaar van een wervingsbureau bevestigd. Ze zoekt standaard op Hyves om te kijken of een persoon past in een bedrijf (Vermeulen, 2006). Ook in Amerika wordt veel gebruik gemaakt van het internet door wervings- en selectiebureaus. Uit onderzoek onder honderd bureaus van de Amerikaanse carrièresite Execunet bleek dat 77 procent gebruik maakt van het internet voor het screenen van mensen (Vermeulen, 2006).

Verder is het tot op heden niet mogelijk om te bepalen welke gegevens voor vrienden, familie of collega's te zien zijn. In het soort vriend is dus geen hiërarchie aan te brengen, terwijl het aannemelijk is dat sommige mensen bepaalde informatie wel aan een vriend kenbaar willen maken, maar niet aan een collega. Ook Kol (2008) gaat hier in haar boek op in en spreekt van botsende werelden. Mensen uit een bepaald netwerk (bijvoorbeeld collega's) komen normaal gesproken in de offline wereld niet zo snel in aanraking met een ander netwerk (bijvoorbeeld familie) van een gebruiker. In de online wereld en zeker via online sociale netwerksites is dit wel het geval (Kol, 2008). Hyves zou hier mogelijk op in kunnen spelen door verder onderscheid aan te brengen in het soort vriend (subgroep) en welke gegevens deze persoon ziet, hoewel dit voor gebruikers wel veel extra werk zal opleveren. Door Kol wordt dit onderschreven. Hoewel het dus niet mogelijk is om binnen de vriendengroep aan te geven wat voor wie te zien is, is het uiteraard wel mogelijk om de hele pagina alleen voor vrienden beschikbaar te stellen.

5.2.3 Weigeren, blokkeren en deleten

Hyves biedt de gebruiker de mogelijkheid om mensen te weigeren, zodat zij geen vriend worden van de gebruiker. Daarnaast is het mogelijk om bepaalde mensen te blokkeren. Ook als de gebruiker zijn Hyves account in het geheel wil deleten is dit mogelijk. Deze optie is echter moeilijk te vinden. Bij Help is 'hoe verwijder ik mijn account?' wel één van de veelgestelde vragen. In de gebruiksvoorwaarden staat ook aangegeven dat bij de help-sectie wordt uitgelegd hoe het account beëindigd kan worden. De gebruiker moet aangeven waarom hij of zij het account wil verwijderen en tevens wordt het wachtwoord gevraagd. Onduidelijk blijft wat er precies verwijderd wordt. Het is niet zeker of bijvoorbeeld krabbels, die de gebruiker heeft geplaatst bij anderen, verwijderd worden wanneer het complete account vervalt.

Hyves biedt de gebruiker dus de mogelijkheden om informatie te deleten en personen te weigeren of te blokkeren, maar ook Hyves zelf mag content verwijderen. Dit staat op de volgende wijze beschreven in de gebruiksvoorwaarden: "b) het recht om enige door jou ter beschikking gestelde bestanden, gegevens en/of materialen te verwijderen van de servers van Hyves en van de dienst van Hyves, bedoeld of onbedoeld, en voor welke reden dan ook en ook zonder reden, zonder dat Hyves op welke wijze dan ook aansprakelijk wordt jegens jou of een derde" (Hyves gebruiksvoorwaarden, 2008).

5.3 Informatie opslaan en gebruiken

De privacypolicy van Hyves gaat onder andere in op de informatie die Hyves opslaat en verwerkt. Hierbij wordt een onderscheid gemaakt tussen de gegevens die de gebruikers in hun Hyves-account moeten en kunnen verstrekken en automatisch gegenereerde informatie. Bij het eerste onderwerp wordt beschreven welke informatie verplicht te vertrekken is en welke informatie verder nog in het Hyves account te plaatsen is.

Ook wat Hyves doet met de automatisch gegenereerde gegevens is zeer interessant in relatie tot de privacy van gebruikers. In de privacypolicy wordt vermeld dat Hyves automatisch gegenereerde informatie over het surfgedrag van de gebruiker verzamelt tijdens het gebruik van Hyves. Deze informatie omvat onder ander het IP-adres (nummer van je computer dat het mogelijk maakt jouw computer te herkennen), het type browser (computerprogramma om internetpagina's mee te kunnen bekijken), de pagina's die de gebruiker bezoekt en 'cookies' (Hyves-Privacypolicy 2008).

Daarnaast wordt in de privacypolicy ingegaan op wat Hyves met de informatie doet uit het Hyves account en de automatisch gegenereerde informatie. Hyves (Privacypolicy 2008) geeft aan de informatie te gebruiken voor de volgende doeleinden:

- om met de gebruiker te communiceren over Hyves en informatie toe te zenden omtrent de eigen diensten, zoals updates van Hyves
- om Hyves aan te passen aan de wensen en behoeften van de gebruiker
- ter beveiliging en om geanonimiseerde statistische gegevens op te stellen

Hyves verzamelt dus gegevens ten behoeve van de eigen dienstverlening. Deze gegevens worden bijvoorbeeld gebruikt om te zorgen dat een gebruiker advertenties te zien krijgt die goed bij die persoon passen (Hyves-Privacypolicy, 2008). Daarnaast gebruikt Hyves de automatisch gegenereerde gegevens voor beveiliging en worden de IP-adressen bijvoorbeeld benut om stalkers te achterhalen. Ook gebruikt Hyves de automatisch gegenereerde informatie voor het opstellen van geanonimiseerde gebruikersstatistieken. De informatie die Hyves hiermee verzamelt, kan tevens in een digitaal dossier bijgehouden worden. Of Hyves dit doet, wat zij precies verzamelt en ten behoeve waarvan dit precies is, wordt niet duidelijk. Bovendien wordt niet duidelijk hoe lang deze gegevens bewaard blijven. Het blijkt vrij gemakkelijk te zijn om data te aggregeren en vervolgens bij te houden in een dossier. Mogelijke websites die op de profielpagina staan vermeld, zoals een persoonlijke website of link naar de profielpagina van een anders sociale netwerksite, worden namelijk getoond wanneer, zonder in te loggen, gezocht wordt op een persoon. Deze gegevens kunnen gecombineerd worden en bijgehouden worden in een digitaal dossier.

5.4 Informatie verspreiden

Onder andere in de gebruiksvoorwaarden en privacypolicy wordt door Hyves ingegaan op het verspreiden van gegevens. De gebruiksvoorwaarden en het privacypolicy zijn duidelijk te vinden. Ze staan rechts onderin en zijn altijd te raadplegen. Ook wanneer een gebruiker niet is ingelogd. Bij Hyves behoudt de gebruiker het auteursrecht over de content die hij of zij plaatst: ‘Onder de voorwaarden die in deze gebruiksvoorwaarden zijn gesteld, behoud je in beginsel de auteursrechten en andere intellectuele eigendomsrechten die aan jou toebehoren met betrekking tot de bestanden die door jou via Hyves ter beschikking worden gesteld’ (Hyves-Gebruiksvoorwaarden, 2008). Toch kan Hyves wel van alles doen met de gegevens die openbaar worden gemaakt. Hierbij gaat het om gegevens die ten behoeve van de brede dienstverlening van Hyves gebruikt en verspreid worden: ‘Je erkent en stemt er mee in dat je door het beschikbaar stellen van bestanden, gegevens en/of materialen aan Hyves je automatisch aan Hyves: (a) een kosteloze, onbezwaarde, wereldwijde, niet-exclusieve licentie verleent om (i) de bestanden, gegevens en/of materialen te gebruiken, verveelvoudigen, verspreiden en openbaar te maken in verband met de dienst van Hyves en (ii) de bestanden, gegevens en/of materialen te gebruiken en verveelvoudigen (en aan derden toe te staan om te gebruiken en verveelvoudigen) in welke media dan ook voor marketing en/of promotie doeleinden in verband met de dienstverlening van Hyves’ (Hyves-Gebruiksvoorwaarden, 2008). Ook Kol gaat hierop in, waarbij zij stelt dat Hyves min of meer eigenaar is van content die door een gebruiker is gemaakt, omdat zij van alles kan doen met de gegevens die door gebruikers openbaar worden gemaakt. Door deze verwarring over auteursrecht en het gebruik van gegevens van gebruikers door Hyves is het voor gebruikers waarschijnlijk niet duidelijk wat nu precies hun rechten zijn.

De privacypolicy van Hyves wijst uitdrukkelijk op het feit dat zaken die een gebruiker plaatst op het profiel ook publiek worden. Wanneer gebruikers zich registeren, moet zij aangegeven worden dat de gebruiksvoorwaarden en privacypolicy zijn gelezen en dat zij ermee akkoord gaan. Zoals uit eerder onderzoek

bleek, is het maar de vraag of gebruikers deze documenten raadplegen.

Omdat jongeren waarschijnlijk de gebruiksvoorwaarden en privacypolicy niet lezen, kan het heel goed mogelijk zijn dat zij zelf een profiel aanmaken, óók als zij jonger dan 16 jaar zijn. Volgens de privacywet mogen aanbieders van sociale netwerksites geen persoonlijke informatie van kinderen jonger dan zestien jaar publiceren zonder toestemming van hun ouders (Spits, 2007). Volgens Kol ligt er een verantwoordelijkheid bij Hyves om vooral jonge gebruikers bewust te maken van de risico's. Hierbij vermeldt zij het volgende: (…)'Er is in ieder geval nu totaal geen voorlichting. Als je een profiel aanmaakt, krijg je geen waarschuwende teksten. Natuurlijk logisch, want ze willen dat je lid wordt en ze willen open profielen zien natuurlijk, maar ik denk dat het wel verantwoord zou zijn als ze…ja in ieder geval de jonge gebruikers wel een berichtje sturen van goh zo werkt Hyves, dit kun je ermee en dit zijn de risico's'. Hierbij denkt zij aan kinderen en jongeren tussen de 7 en 17 jaar. Zij kunnen, via de e-mail die iedereen standaard krijgt na aanmelding, op de hoogte worden gesteld van mogelijke risico's. Ook het CBP vindt dat sites zoals Hyves te weinig doen om de privacy van hun gebruikers te beschermen (Spits, 2007). Daarnaast geven dergelijke sites volgens het CBP te weinig voorlichting over de risico's van het online publiceren van persoonlijke informatie. Overigens hebben aanbieders van sites, waaronder ook Hyves, toegezegd zich meer bezig te gaan houden met de bescherming van de privacy. Dit gaan zij onder andere doen met behulp van organisaties zoals Digibewust en Mijn Kind Online (Spits, 2007).

Informatie in het profiel, relaties, berichten, zoekwoorden enz. worden door Hyves verzameld om zo goede service te kunnen bieden en gepersonaliseerde features aan te kunnen bieden. Hyves mag de informatie uit het profiel van gebruikers gebruiken, maar mag geen informatie verstrekken aan derden over de gebruiker als individu. Pas wanneer de gebruiker toestemming geeft voor API's is het voor derde partijen mogelijk om iets met de gegevens van de gebruiker te doen. Daarbij is het dan wel gelijk mogelijk voor derde partijen om een digitaal dossier te creëren en op deze manier iets te doen met de schat aan informatie die voorhanden is en die voor commerciële doeleinden zeer interessant is. Op individueel niveau wordt dus geen informatie door Hyves openbaar gemaakt aan adverteerders. Dit gebeurt dus alleen op geaggregeerd niveau. Kol licht dit toe, waarbij zij opmerkt dat de persoonlijke gegevens van de gebruikers niet worden verkocht, maar de gegevens alleen worden gebruikt om de advertenties op de juiste profielen te kunnen plaatsen.

5.5 Privacyschendingen

Enkele privacyschendingen van de laatste tijd worden hierna uiteengezet. Daarnaast wordt ingegaan op risico's die binnen Hyves mogelijk zijn en die door Solove (2006) onder de vierde groep, namelijk 'schending' geplaatst worden.

Eva Kol (2008) gaat in haar boek over Hyves in op een incident waarmee Hyves te maken kreeg en waarmee de privacy van gebruikers in gevaar kwam. Dit incident beschouwen de oprichters als dieptepunt van Hyves en is de boeken ingegaan als de Goldmember-affaire. De lancering van het Goldmembership, waarbij gebruikers

inzicht konden krijgen in statistieken en wie hun pagina bezoekt, bleek nogal wat voeten in de aarde te hebben. Het bleek namelijk dat de bezoekersgeschiedenis van de afgelopen weken niet was gewist en dat statistieken voor iedereen open stonden (Kol, 2008: 67). Op deze manier was het dus niet mogelijk om anoniem te surfen en de profielen van anderen te bekijken. Binnen korte tijd kwamen er dan ook veel boze telefoontjes binnen van gebruikers. Vervolgens ging de site uit de lucht en is de fout hersteld. Hier was dus duidelijk sprake van een vertrouwensbreuk.

Ook op 24 april 2008 zorgde een aanpassing op Hyves voor opschudding. Hyves bracht toen naar buiten regels te willen stellen aan het afschermen van de profielen. Sinds die datum is het niet meer mogelijk voor de gebruiker om bij andere mensen dan zijn of haar eigen vrienden te kijken wanneer het eigen profiel alleen te zien is voor vrienden. Hyves had hiervoor de volgende redenen:

1. Er wordt het meest gehyved tussen vrienden en vrienden van vrienden.
2. Veel mensen die hun profiel afschermen vinden het prima als vrienden van vrienden hun pagina ook mogen zien.
3. In een kleiner deel van de gevallen moeten mensen wel hun pagina afschermen, bijvoorbeeld omdat ze in een TBS kliniek werken.
4. Hyvers die hun profiel niet afschermen vonden het storend en niet fair dat afgeschermde hyvers wel bij hen konden kijken (Spanjar, 2008).

Het gluren bij anderen wordt daarmee ingeperkt, maar de vraag is of mensen dat willen. Een meer realistisch scenario is dat meer mensen hun profiel open zullen zetten. In plaats van de surveillance te beperken zal hierdoor alleen maar méér informatie openbaar gemaakt worden. Kol bevestigt dit: ‘Ja, ik denk dat de medewerkers van Hyves net zo als ik denken in de zin van Hyven was vooral leuk omdat je kon kijken bij iedereen, omdat het zo open is en als je dat wegneemt gaat een deel van de lol ervan af. Dus ze hopen natuurlijk gewoon, dat meer mensen het toch open laten, omdat het anders een stukje minder leuk wordt’.

Bovendien blijkt het vrij gemakkelijk te zijn om je voor te doen als iemand anders en combinaties van correcte en valse gegevens van deze persoon openbaar te maken. Hierbij kan gedacht worden aan persoonsgegevens en contactgegevens, maar ook aan foto’s en blogs. Op deze manier kan dus vrij gemakkelijk iemands identiteit overgenomen worden, wat bijvoorbeeld reputatieschade als consequentie kan hebben. Verder blijken er nog steeds veel doorstuurmailtjes en kettingbrieven doorgestuurd te worden via de Hyves inbox. De communitymanagers van Hyves houden zich hier wel mee bezig en proberen dit zoveel mogelijk te achterhalen en een halt toe te roepen.

Daarnaast is het mogelijk om gestalkt en lastig gevallen te worden via Hyves. Hiervoor is de blokkeerfunctie erg handig. Ook kan Hyves ingrijpen wanneer hier om gevraagd wordt. Dat Hyves hier meer en meer aandacht voor heeft wordt door Eva Kol bevestigd: ‘(…)In het begin was het van: Ja daar is geen tijd voor en ja dat komt wel …

en alleen maar bezig zijn met het bouwen van nieuwe applicaties. Dus steeds meer en meer en groter werd het. En nu zijn ze toch wel wat meer aan het kijken van: wat zeggen de gebruikers, wat vinden zij, en daar luisteren ze over het algemeen ook wel naar. Ze proberen zoveel mogelijk om er iets aan te doen op het moment dat er meldingen binnen komen van pesten en stalken en dat soort zaken, maar ja je kan niet alles controleren. Gebruikers moeten het wel zelf aangeven. Gebruikers moeten daarvoor zelf op de DitisnietOK-knop drukken. Hyves kan het anders gewoon niet vinden. Het netwerk is te groot om daar allemaal mensen op te zetten die actief moeten zoeken naar dat soort dingen'. Bovenstaand voorbeeld van Kol is een voorbeeld van één van de criteria waar sociale netwerksites volgens De Bruin & de Bruin (2001) aan moeten voldoen. Volgens hen moet er namelijk een bepaalde vorm van sociale controle zijn waardoor toezicht kan worden gehouden op de sociale interactie en communicatie. Deze controle wordt binnen Hyves vooral door de gebruikers zelf uitgevoerd, door bijvoorbeeld op de DitisnietOK-knop te drukken.

Hyves geeft niet aan wanneer er wijzigingen zijn opgetreden in de gebruiksvoorwaarden en van welke datum de gebruiksvoorwaarden zijn. Zo blijkt in de periode tussen april 2008 en juni 2008 een aantal zinnen toegevoegd te zijn bij punt 2 over het account en profiel waaronder de volgende:
'2.3 Als je jonger bent dan zestien (16) jaar, moet je van je ouders of voogd toestemming hebben voor het aanmaken van een account. Door deze gebruiksvoorwaarden te accepteren, garandeer je dat je zestien (16) jaar of ouder bent of toestemming hebt van je ouders of voogd voor het aanmaken van een account. 2.4 Je mag geen accounts aanmaken op naam van een andere persoon, tenzij die andere persoon je daarvoor toestemming heeft gegeven' (Gebruiksvoorwaarden Hyves, 18 juni 2008).

Zeer waarschijnlijk zijn bovenstaande wijzigingen tot stand gekomen naar aanleiding van eerder onderzoek van het College Bescherming Persoonsgegevens. Volgens het CBP schenden sociale netwerksites, waaronder ook Hyves, de Nederlandse privacywetgeving. Zij mogen namelijk formeel gezien geen persoonlijke informatie van kinderen jonger dan zestien jaar publiceren zonder toestemming van hun ouders. Volgens het CBP publiceren sociale netwerksites deze gegevens wel en worden jongeren daarnaast niet op de hoogte gebracht van deze regels (Spits, 2007) Toch heeft het CBP niet gelijk actie ondernomen, maar werd een oproep gedaan aan vooral de beheerders van de websites om zelf hun verantwoordelijkheid te nemen (Spits, 2007). Zoals bovenstaand voorbeeld aangeeft, heeft Hyves dit gedaan.

5.6 Samenvatting en conclusie

In deze conclusie wordt antwoord worden gegeven op deelvraag 2: ***In hoeverre waarborgen aanbieders van sociale netwerksites de privacy van gebruikers binnen deze sites?*** Deze vraag is bestudeerd vanuit de sociale netwerksite Hyves aan de hand van twee subdeelvragen.

Hoe waarborgen aanbieders de privacy van gebruikers op dit moment en welke overwegingen spelen daarbij een rol?

Hyves is zich bewust van het feit dat er verantwoordelijkheid rust bij haar om de privacy van gebruikers te beschermen. De afgelopen jaren heeft Hyves steeds meer mogelijkheden gecreëerd voor gebruikers waardoor zij zelf kunnen bepalen welke gegevens openbaar worden gemaakt en voor wie: (1)Niemand, (2) Alleen vrienden, (3) Vrienden van Vrienden of (4) Hyvers. Alleen de naam van de gebruiker wordt standaard getoond en het e-mailadres van de gebruiker is te zien voor zijn of haar vrienden. De overige informatie kan ingevuld worden als de gebruiker dat wil. Daarnaast is het mogelijk om gegevens te verwijderen, aan te passen, personen te weigeren en te blokkeren. Bovendien heeft Hyves toegezegd zich meer bezig te gaan houden met de bescherming van de privacy (Spits, 2007). Hieruit kan geconcludeerd worden dat Hyves het belang van privacy inziet en weet dat dit belangrijk is voor gebruikers.

Toch worden de keuzemogelijkheden voor gebruikers soms beperkt. Een voorbeeld daarvan is de beslissing die Hyves op 24 april 2008 nam over de afscherming van de profielen van gebruikers. Sinds die datum is het namelijk niet meer mogelijk voor de gebruiker om bij andere mensen dan zijn of haar eigen vrienden te kijken wanneer het eigen profiel alleen te zien is voor vrienden. Het gluren bij anderen wordt daarmee ingeperkt, maar de vraag is of mensen dat willen. Een meer realistisch scenario is dat meer mensen daardoor hun profiel open zetten, zodat nog meer gegevens openbaar worden. Voor Hyves zelf zou dit in algemene zin gunstig kunnen zijn: hoe meer gegevens van gebruikers, des te interessanter voor Hyves en derde partijen. Hyves mag alle gegevens namelijk gebruiken voor haar eigen dienstverlening. De gegevens mogen ook gebruikt worden om te zorgen dat een gebruiker advertenties te zien krijgt die goed bij die persoon passen (Hyves-Privacypolicy, 2008). Daarnaast worden de automatisch gegenereerde gegevens gebruikt voor beveiliging en worden de IP-adressen bijvoorbeeld gebruikt om stalkers te achterhalen. Ook gebruikt Hyves de automatisch gegenereerde informatie voor het opstellen van geanonimiseerde gebruikersstatistieken. De informatie die Hyves hiermee verzamelt kan tevens in een digitaal dossier bijgehouden worden. Of Hyves dit doet, wat er precies verzameld wordt en ten behoeve waarvan dit precies is, is niet duidelijk. Persoonlijke informatie wordt niet doorverkocht aan derden zonder toestemming van de gebruikers. Hyves mag weliswaar de informatie uit het profiel van gebruikers gebruiken, maar mag geen informatie verstrekken aan derden over de gebruiker als individu. Pas wanneer de gebruiker toestemming geeft voor API's is het voor derde partijen mogelijk om iets met de individuele gegevens van de gebruiker te doen. Daarbij is het dan wel gelijk mogelijk voor derde partijen om een digitaal dossier te creëren en op deze manier iets te doen met de schat aan informatie die voorhanden is en die voor commerciële doeleinden zeer interessant is.

Wat zijn mogelijke privacybeperkingen/risico's binnen sociale netwerksites?

De paragrafen in dit hoofdstuk geven een goed inzicht in hoe Hyves de privacy van haar gebruikers tracht te waarborgen. Daarbij zijn een aantal risico's en beperkingen ter sprake gekomen. Hierna worden deze samengevat aan de hand van de categorieën van Solove (2006) die in dit hoofdstuk zijn gebruikt.

Informatie verzamelen

In de eerste plaats blijkt dat, ook wanneer je geen lid bent van Hyves, het mogelijk is om via Hyves informatie te achterhalen over gebruikers. Soms is het alleen wel zo dat personen hun profielen afschermen en dat daardoor alleen de profielfoto en naam te zien zijn. Toch is het op deze manier altijd mogelijk om iets te weten te komen over een persoon door bijvoorbeeld werkgevers, de politie of de Belastingdienst. Ten tweede staat de Buzz standaard ingesteld op “te zien voor vrienden”. Dit zou mogelijk door gebruikers als een privacyschending kunnen worden bestempeld, aangezien op deze manier precies bijgehouden kan worden wat iemand allemaal doet op Hyves. Door Eva Kol wordt dit bevestigd. Verder is het tot op heden niet mogelijk om te bepalen welke gegevens voor de subgroepen vrienden, familie of collega’s te zien zijn. In het soort vriend is dus geen hiërarchie aan te brengen, terwijl het aannemelijk is dat sommige mensen bepaalde informatie wel aan een vriend kenbaar willen maken, maar niet aan een collega. Ten slotte blijft onduidelijk wat er nu precies verwijderd wordt bij het deleten van het account. Het is niet zeker of bijvoorbeeld krabbels, die de gebruiker heeft geplaatst bij anderen, verwijderd worden wanneer het complete account vervalt.

Info opslaan en gebruiken

Hyves gebruikt de automatisch gegenereerde informatie voor het opstellen van geanonimiseerde gebruikersstatistieken. De informatie die Hyves hiermee verzamelt kan tevens in een digitaal dossier bijgehouden worden. Of Hyves dit doet, wat er precies verzameld wordt en ten behoeve waarvan dit precies is, wordt niet duidelijk. Bovendien wordt niet duidelijk hoe lang deze gegevens bewaard zullen blijven. Het blijkt vrij gemakkelijk te zijn om data te aggregeren en vervolgens bij te houden in een dossier. Mogelijke websites die op het profiel staan vermeld, worden namelijk getoond, wanneer zonder in te loggen gezocht wordt op een persoon.

Informatie verspreiden

Pas wanneer de gebruiker toestemming geeft voor API’s is het voor derde partijen mogelijk om iets met de individuele gegevens van de gebruiker te doen. Daarbij is het dan ook mogelijk voor derde partijen om een digitaal dossier te creëren en op deze manier iets te doen met de schat aan informatie die voorhanden is en die voor commerciële doeleinden zeer interessant is.

Privacyschendingen

Er blijken nog steeds veel doorstuurmailtjes en kettingbrieven doorgestuurd te worden via de Hyves inbox. Daarnaast is het mogelijk om gestalkt en lastig gevallen te worden via Hyves. Ook blijkt het vrij gemakkelijk te zijn om een profiel voor iemand anders aan te maken.

De risico’s en beperkingen, die in tabel 15 zijn beschreven, zijn in dit hoofdstuk aan de orde gekomen en kunnen binnen Hyves voorkomen en eventueel door gebruikers worden genoemd. In hoeverre hier ook aandacht aan wordt gegeven door gebruikers komt in het volgende hoofdstuk ter sprake.

Tabel 15: *Overzicht risico's en beperkingen naar aanleiding van inhoudsanalyse*

	Risico's/beperkingen
Informatie verzamelen	Surveillance (onbekenden, werkgevers, politie, belastingdienst) Gebrek aan controle door gebruikers (subgroepen) Standaard instellingen Deleten account
Informatie opslaan en gebruiken	Bijhouden van digitaal dossier Aggregatie van gegevens
Informatie verspreiden	Commerciële doeleinden Bijhouden van digitaal dossier door derden
Privacyschendingen	Spam Stalking Identiteitsovername Afschermen profiel

6. DE PRIVACYBELEVING VAN HYVES-GEBRUIKERS

(…)'Het is één van de veiligste manieren om via internet met elkaar te communiceren op MSN na' (Sjoerd, 13 jaar)
'Het is het gevoel van controle, maar eigenlijk is het niet meer dan een vinkje zetten. Technisch gezien heb je er eigenlijk geen controle over. De enige controle die je hebt is een vinkje' (Tom, 31 jaar).

In dit hoofdstuk staat de beleving van de gebruikers over hun privacy binnen de sociale netwerksite Hyves centraal. Zoals in het methodehoofdstuk al is beschreven, zijn deze resultaten tot stand gekomen door het houden van focusgroepgesprekken met twee verschillende groepen variërend in leeftijd. In dit hoofdstuk wordt de oudere groep, de 24- tot en met 31-jarigen, groep A genoemd. De groep respondenten in de leeftijd van 13 tot en met 18 jaar wordt groep B genoemd. Aan de hand van de subdeelvragen c tot en met h zal de online privacybeleving van Hyves-gebruikers worden beschreven. Samen geven deze vragen antwoord op de volgende vraag: ***Hoe beleven gebruikers van sociale netwerksites hun online privacy?*** De belangrijkste uitkomsten komen in dit hoofdstuk aan de orde waarbij vooral aandacht uitgaat naar de verschillen en overeenkomsten tussen beide groepen.

6.1 Meningen over Hyves

Algemeen

Aan de respondenten van beide groepen is gevraagd wanneer zij voor het laatst zijn ingelogd op Hyves en wat zij toen gedaan hebben. De antwoorden verschilden, maar waren niet erg verrassend. Iedereen was in de afgelopen twee dagen minimaal één keer ingelogd. De meest gebruikte toepassingen binnen Hyves werden genoemd zoals het downloaden van foto's, het sturen van een krabbel, het bijwerken van de status in de WieWatWaar, toevoegen van vrienden en het rondkijken op Hyvespagina's van anderen.

De respondenten zien Hyves vooral als een leuke manier om met mensen in contact te komen. Dit kunnen oude bekenden zijn van bijvoorbeeld de basisschool, maar ook personen die de gebruikers binnenkort gaan ontmoeten. Daarnaast wordt veel gebruikt gemaakt van Hyves wanneer mensen zich vervelen: *(…)* 'Nou ja, misschien ook uit verveling dat je foto's gaat kijken van anderen en krabbels gaat lezen en weer door gaat linken naar iemand anders die daar dan vervolgens weer op heeft gereageerd' (Karlijn, 24 jaar). Dat dit inderdaad vaker voorkomt werd door twee andere respondenten bevestigd.

Groep A

De 24- tot en met 31-jarigen zien Hyves als een leuke en handige manier om oude bekenden en vrienden van vroeger op te zoeken en met hen in contact te komen. Overigens wordt de communicatie als veel oppervlakkiger beschouwd dan in het echte leven. Door sommige respondenten uit deze groep wordt de sociale netwerksites ook wel als hulpmiddel gezien om bijvoorbeeld verjaardagen te onthouden of wordt de site als adresboek gebruikt om mensen terug te zoeken. Bovendien bleek uit de antwoorden dat zij vooral

actief bezig zijn binnen de site en bijvoorbeeld foto's downloaden of krabbels sturen.

Groep B

Hoewel een enkeling het ook leuk vindt om bekenden van vroeger, zoals van de basisschool, op te zoeken, vinden de 13- tot en met 18-jarigen het ontmoeten van nieuwe contacten erg leuk. Sjoerd merkte dit op: 'Ik heb pas de lijst binnen gehad met wie ik allemaal in de klas zit en dan komen er echt een heleboel mensen naar je Hyves toe van: Ik zit volgend jaar bij jou in de klas en dan denk ik van: 'ok leuk!' en dan ga je ze krabbelen en daardoor ken ik nu iemand al heel erg goed (Sjoerd, 13 jaar). Bovendien zijn het sturen van berichten, het bekijken en plaatsen van filmpjes en het plaatsen van foto's veel voorkomende bezigheden binnen Hyves. De 13- tot en met 18-jarigen loggen redelijk vaak in op Hyves. Zij waren allemaal een dag voor het focusgroepgesprek of dezelfde dag ingelogd op de site. Opvallend is dat de jongere groep vooral inlogt op Hyves om 'rond te neuzen' en te 'kijken of er nog krabbels of berichten zijn'.

Samenvattend

Grote verschillen tussen beide groepen zijn er niet wat betreft de mening over Hyves en de tools die zij binnen de dienst gebruiken. Wel blijkt uit de antwoorden dat de oudere respondenten over het algemeen bewuste activiteiten ontplooien binnen Hyves. De jongeren sturen ook berichten en plaatsen filmpjes en foto's, maar vinden het daarnaast leuk om zomaar rond te kijken binnen Hyves.

6.2 Definitie

Algemeen

Aan de respondenten is gevraagd aan welke woorden zij denken bij het woord privacy. In eerste instantie werden de volgende woorden door de groepen genoteerd:

Tabel 16: *Woorden waaraan gedacht wordt bij privacy*

24- tot en met 31-jarigen	13- tot en met 18-jarigen
Privé (3 x)	Geheim (4 x) iets wat je met iemand deelt waarvan alleen jullie afweten, Privé(dingen)
Onderscheid	Zichtbaar voor
Dicht	Zelf bepalen wie wat mag zien, zichtbaar voor, zelf bepalen wat jij wilt
Afgeschermd	Niet voor iedereen, niet openbaar, eigen
Binnen/buiten	Bescherming (3 x)
NAW-gegevens (2 x)	Krabbels
Adres	Naam
Telefoon/e-mailgegevens	E-mail
Foto's	Hyves
Vrienden/familie, vrienden, partner	Wachtwoord
Imago	

Hoewel sommigen woorden op het eerste gezicht niet veel met privacy te maken lijken te hebben, werd door de respondenten wel duidelijk uitgelegd wat er mee bedoeld wat ze bedoelen. Zo gingen Claudia en Brenda in op adres en telefoon/e-mailgegevens en zei Kim ongeveer hetzelfde waarbij ze inging op bescherming:

'(…)Ze hoeven niet voor mijn stoep te komen staan' (Claudia, 30 jaar).
'Dat ineens mensen je beginnen te mailen terwijl je zelf zoiets hebt van: 'Ik heb helemaal geen zin in jou' (Brenda, 24 jaar).
'Ja met privacy en dat soort dingen kun je toch, ook wat ik net zei, beschermen. Dingen van buitenaf die je eigenlijk gewoon niet wil. Contact met mensen dat je zegt: Mwa…alsjeblieft zeg' (Kim, 17 jaar).

Uit bovenstaande zinnen blijkt heel duidelijk de ruimtelijke dimensie zoals die in hoofdstuk drie is gedefinieerd, namelijk rust en afzondering opeisen. Ook de relationele dimensie komt erin terug. Deze dimensie komt vooral in de zinnen twee en drie aan de orde. In de genoteerde woorden van beide groepen (zie tabel 16) wordt ook de derde dimensie meegenomen, namelijk de bescherming van persoonsgegevens. Deze dimensie komt tot uiting in wat de respondenten 'het beschermen van wie jij bent en waar je voor staat' en het 'zelf bepalen welke gegevens jij vrijgeeft' noemen. De respondenten zijn het er allemaal over eens dat privacy over twintig jaar nog steeds zal bestaan. De 24- tot en met 31-jarigen verwoorden dit als volgt: 'Je hebt altijd dingen voor jezelf' en 'je hebt altijd controle over bepaalde gegevens'. Dat het anders zal worden was wel de conclusie van beide groepsgesprekken.

<u>Groep A</u>
Door in te gaan op de opgeschreven woorden en de vraag te stellen: Privacy is….? werden de volgende woorden en zinnen genoemd door de 24- tot en met 31-jarigen: regiefunctie, controle, filtering, persoonlijk, beschermen van jezelf: wie je bent, waar je voor staat, je omgeving, je bezittingen, beschermen van wat jij wilt beschermen, beperkte openheid, onvindbaarheid, imago.

Hoewel de ruimtelijke dimensie niet terugkomt in de woorden die genoemd worden, is er wel aandacht voor de relationele dimensie in die zin dat beperkte openheid en onvindbaarheid als belangrijke woorden worden meegenomen door de 24- tot en met 31-jarigen. Op deze manier wordt gestreefd naar het afschermen van een bepaald deel van het persoonlijk leven. Hierbij gaat het om het beschermen van wie je bent, waar je voor staat, je omgeving zoals vrienden en familie en je bezittingen. Deze woorden komen als volgt terug in de definitie van privacy die door de respondenten is opgesteld:

> De regie nemen over de bescherming van wat jij belangrijk vindt om te beschermen, zoals wie je bent, wat je doet, je omgeving (vrienden en familie) en bezittingen om zo te zorgen dat bepaalde zaken niet openbaar worden gemaakt en tegen je gebruikt kunnen worden.

Deze definitie komt nagenoeg overeen met de definitie zoals geformuleerd in het theoretische hoofdstuk over privacy: 'Privacy is the people's right to prevent the disclosure of personal information to others and the right to be free from intrusion and social control by others'. Wat opvalt, is dat de respondenten persoonlijke informatie verder uitsplitsen en bovendien ingaan op het doel van de bescherming, namelijk te zorgen dat bepaalde zaken niet openbaar gemaakt kunnen worden en tegen een persoon gebruikt kunnen worden. Voor de respondenten blijken reputatie en imago dus belangrijk te zijn. Op het binnendringen in iemands leven en de sociale controle door anderen wordt in de definitie niet ingegaan. Wel blijkt uit de waarden (zie paragraaf 6.3) en uit de uitleg van de gebruikers (zie tekst na tabel 16) dat de gebruikers deze aspecten van de ruimtelijke en relationele dimensie als belangrijk ervaren.

Op de stelling: 'Door internet is het begrip privacy aan het veranderen' werd wisselend gereageerd. De helft van de 24- tot en met 31-jarigen is het met de stelling eens, de andere helft niet. Daarbij werd vooral ingegaan op een mogelijke verandering van het privacybegrip of dat privacy zelf verandert. Het eerste is volgens de respondenten niet het geval. Het kader zal volgens hen hetzelfde blijven, maar de inhoud zal wel veranderen. Daarnaast werd opgemerkt dat privacy misschien ook het internet verandert, waarbij OpenID als voorbeeld werd gegeven. Door ECP.nl (2007) wordt OpenID als volgt definieert: ' (…)een gedecentraliseerd identiteitsmanagement systeem dat het mogelijk maakt dat een gebruiker met één gebruikersnaam en wachtwoord kan inloggen bij verschillende websites' (ECP.nl, 2007:7).

De respondenten zijn het er wel over eens dat privacy over twintig jaar nog steeds zal bestaan. Wel zullen andere middelen gebruikt gaan worden en bovendien is de verwachting dat de overheid zich er ook steeds meer mee bezig zal gaan houden, zoals Brenda verwoordde: '(…) dat het nog meer wordt dat er bijvoorbeeld boetes komen te staan als een bedrijf bijvoorbeeld ongevraagd je gegevens opslaat om het zo maar te zeggen' (Brenda, 24 jaar).

<u>Groep B</u>
De 13- tot en met 18-jarigen noemden onder andere: 'Een vorm van zelfbescherming', 'niet voor iedereen bestemd', 'zelf bepalen welke gegevens jij vrijgeeft voor iedereen uit zelfbescherming' en 'wat je geheim wilt houden' op de vraag: 'Wat is privacy voor jullie?' In tegenstelling tot de oudere groep, wordt door de 13- tot en met 18-jarigen niet ingegaan op de relationele dimensie. Wel werd door Kim het volgende gezegd, op de vraag: 'Gegevens, wat zijn dat dan precies voor jou? Heb je het dan over persoonsgegevens?': 'Nee ook andere dingen. Niet heel de wereld hoeft te weten dat dat je vriendje is' (Kim, 17 jaar).

Door de 13- tot en met 18-jarigen werd de volgende definitie geformuleerd:

> Privacy is een vorm van zelfbescherming waarbij je zelf bepaalt welke gegevens en geheimen voor wie bestemd zijn. Gegevens zijn onder andere N.A.W. gegevens, wat je doet, waar je te vinden bent en interesses. Onder geheimen wordt de info verstaan die je binnen een bepaalde groep wilt houden.

Deze definitie komt gedeeltelijk overeen met de definitie zoals geformuleerd in het theoretisch hoofdstuk over privacy. Door de respondenten wordt alleen ingegaan op het beschermen van persoonlijke informatie, waarbij wel duidelijk wordt omschreven wat hier precies mee bedoeld wordt.

De 13- tot en met 18-jarigen zijn het er, op één respondent na, over eens dat door internet het begrip privacy aan het veranderen is. Daarbij werd niet ingegaan op het begrip zoals dit eerder al geformuleerd was, maar meer op het internet als medium en de mogelijkheden daarvan. Ook Marcel is het hiermee eens, al gaf hij wel aan dat daardoor het begrip op zich niet veranderd is*:* 'Op zich blijft privacy wel hetzelfde, alleen je krijgt nu door het internet meer toegang tot iemand anders zijn privacy, zeg maar, maar het begrip op zich, dat je dingen geheim wilt houden dat verandert niet. Er wordt alleen anders mee omgegaan'. Bovendien zijn de respondenten in de leeftijd van 13 tot en met 18 jaar het er over eens dat privacy over twintig jaar nog steeds zal bestaan. Volgens hen wordt er steeds meer waarde aan privacy gehecht en zal privacy daarom alleen maar belangrijker worden. Redenen die zij hiervoor aanvoeren zijn onder andere dat mensen steeds voorzichtiger worden omdat ze zelf dingen meemaken of door de media op de hoogte worden gesteld.

Samenvattend

Beide groepen geven een duidelijke definitie waarin de informationele dimensie duidelijk naar voren komt, maar waar de ruimtelijke dimensie niet in mee wordt genomen. De respondenten in de leeftijd van 24 tot en met 31 jaar nemen daarnaast de relationele dimensie mee in hun definitie en gaan bovendien in op het doel van het beschermen van de privacy, namelijk imagobescherming.

6.3 Waarden

Algemeen

Tabel 17 geeft weer welke waarden werden genoemd door beide groepen. Hierbij gaat het om idealen en motieven die de gebruikers belangrijk vinden bij privacy. Voor beide groepen blijkt de bescherming van jezelf en persoonlijke gegevens heel belangrijk te zijn.

Tabel 17: *Waarden bij privacy*

24- tot en met 31-jarigen	13- tot en met 18-jarigen
Vrijheid (3 x), soeverein	Vertrouwen
Doen en laten wat je wilt	Vertrouwelijke informatie kunnen beschermen
Sociaal contact	Geheimhouding, geheimhouden
Bescherming van anderen	Niet doorvertellen aan anderen
Persoonlijke gegevens	Eerlijkheid, eerlijk zijn tegenover elkaar
Niet bloot geven, beperkte openheid	Bescherming, bescherming van jezelf
Persoonlijk blijven	Zorgen dat mensen niet achter je aankomen die je niet kent
Mijn/Dijn	Anderen in hun waarde laten
Persoonlijke bezittingen	Anderen moeten accepteren dat jij behoefte hebt aan privacy
Doem/Karma	Respect
Geen negatief imago/gevolgen	

Groep A

Een groot aandeel in de antwoorden van de 24- tot en met 31-jarigen heeft de waarde vrijheid en daaraan gekoppelde woorden, zoals soeverein (zelfbeschikking), doen en laten wat je wilt en vrij zijn in het onderhouden van sociale contacten. Claudia ging hier op in: 'Mensen worden heel vaak uitgenodigd voor feestjes of verjaardagen. Hallo, als ik je toegevoegd heb, wil dat nog niet zeggen dat ik daar behoefte aan heb. Of ja, ze leggen je iets op. Ik moet daar wel vrij in zijn om die sociale contacten te willen onderhouden of niet' (Claudia, 30 jaar). Ook beperkte openheid en eigen baas blijven werden vervolgens door de respondenten genoemd. Verder gingen zij in op de bescherming van anderen, van bezittingen, van wat van jou is en de gevolgen die het voor jou zou kunnen hebben zoals een negatief imago, of misbruik. Daarnaast werd nog gesproken over karma, waarmee de geschiedschrijving van je leven werd bedoeld.

Bovenstaande waarden en criteria die de groep oudere respondenten noemde, komen aardig overeen met de waarden en criteria die door Smink et al. (1999) zijn beschreven. Het zelf keuzes kunnen maken, ongestoord kunnen leven, bewegingsvrijheid hebben en het vrij blijven van stigmatisering worden door de respondenten allemaal genoemd. Ook in de bovenstaande woorden komt duidelijk naar voren dat het uitgangspunt van Gutwirth, dat privacy onlosmakelijk verbonden is met de individuele vrijheid van de mens, nog steeds heel belangrijk is.

Groep B

De jongere groep respondenten bracht de waarde vrijheid niet ter sprake. Zij vinden eerlijkheid en vertrouwen heel erg belangrijk, waarmee zij het vertrouwen van hun vrienden en de eerlijkheid die daar onlosmakelijk mee verbonden is, bedoelen. Het nakomen van beloftes is daarbij heel belangrijk. Kim verwoordde dit als volgt: 'dan

kan jouw privacy aangetast worden, omdat…bijvoorbeeld goede mensen weten dingen over jou die de rest van de wereld niet hoeft te weten en dat kan dan in een keer naar buiten komen' (Kim, 17 jaar). Ook respect werd door hen genoemd. Hiermee wordt het 'accepteren dat dingen alleen voor jezelf zijn en niet voor anderen of maar voor sommigen' bedoeld.

De waarden en criteria die de 13- tot en met 18-jarigen noemden (zie tabel 17), komen iets minder duidelijk overeen met de waarden en criteria die door Smink et al. (1999) zijn beschreven. Toch zou gezegd kunnen worden dat onderdelen van de vier belangrijkste waarden wel naar voren werden gebracht. Zo worden vertrouwen en zelf kunnen bepalen wie wat van je weet door de respondenten genoemd en door Smink et al. (1999) onder de waarde zelfstandigheid geplaatst.

Samenvattend

De respondenten geven allemaal een ruime beschrijving van de waarden die voor hen belangrijk zijn bij privacy. De antwoorden uit het onderzoek van Smink et al. (1999): 'alles wat van mij is en waarvan ik niet wil dat andere mensen dat weten'; 'dat je niet gestoord wordt'; geen misbruik van vertrouwen maken' en 'vrij leven zonder inmenging van anderen' worden ook in dit onderzoek (met iets andere bewoordingen) genoemd. Daarnaast blijkt de verwachting van Dubbeld (2000) gedeeltelijk te kloppen. Gebruikers van Hyves blijken inderdaad de zeggenschap en controle die een gebruiker bezit over zijn persoonlijke sfeer ook in het digitale tijdperk als een belangrijke voorwaarde voor privacy te beschouwen.

6.4 Houding ten op zichte van privacy

Algemeen

De respondenten zijn van mening dat zij steeds meer aandacht hebben voor privacy en vooral door de oudere groep wordt daarbij de vergelijking getrokken met de beginperiode waarin zij actief waren op Hyves:

Claudia, 30 jaar: 'Is het niet zo dat in het begin van Hyves, dan gooi je alles erop….'

Karlijn, 24 jaar: 'Ja dan wil je dat iedereen alles over je weet'.

Claudia, 30 jaar: 'en daarna denk je van….'

Sander, 26 jaar: 'Al doende leert men hè'!

Claudia, 30 jaar: 'Ja en dan denk je: schluss! en dan zet je foto's onzichtbaar en scherm je ook je profiel af'.

Bovendien werd aangegeven dat er soms niet goed wordt omgegaan met privacy door de gebruikers zelf. Wel zijn ze van mening dat gebruikers zich steeds meer bewust te worden van de gevaren. Door Sjoerd wordt hier op ingegaan: 'Nou, het is tegenwoordig steeds meer van: ja, even een wachtwoordje. En je hebt ook voor steeds meer dingen wachtwoorden nodig en mensen gaan er steeds soepeler over denken, van ja het is alleen maar voor dat….en achteraf stel dat er iets bij jou is gebeurd, dat je dan pas realiseert ja eigenlijk is een wachtwoord toch wel iets wat niet zomaar iedereen hoeft te weten. Dat het dan toch wel privé is' (Sjoerd, 13 jaar). Niet alleen de gebruikers beginnen zich steeds meer bewust te worden van hun online privacy. Ook Hyves is zich bezig gaan houden met privacy en manieren aan het ontwikkelen om de privacy van haar gebruikers te

beschermen, volgens de respondenten.

De bezorgdheid over hun privacy is volgens de respondenten dus toegenomen. Dit is versterkt door de nieuws-items die op televisie worden uitgezonden en de politiek die zich ook steeds meer bezig gaat houden met privacyissues. Door Brenda wordt dit als volgt uitgelegd: 'Ja, je denkt alleen maar aan de leuke mensen die op internet zijn, maar je vergeet soms dat er ook minder leuke mensen zijn' (Brenda, 24 jaar). Ook door de 13- tot en met 18-jarigen is het effect van de media op de bezorgdheid en bewustwording aan de orde gesteld: 'een poosje geleden….was er een man geloof ik en die kon zomaar aan gegevens komen van mensen, van 1000 ofzo, om te hacken en zo en dan komt het in de krant en dan hebben de mensen zo iets van oh dat is wel gevaarlijk, dus ik ga maar een beetje voorzichtiger worden enzo' (Marcel, 16 jaar).

Dat mensen zich met privacy bezig houden en bezorgd zijn over hun privacy wil niet zeggen dat zij ook daadwerkelijk acties ondernemen, zoals blijkt uit een onderzoek uitgevoerd door TRUSTe (O'Neill, 2001). Hoewel internetgebruikers aangeven te weten hoe ze hun privacy moeten beschermen, blijkt uit onderzoek dat een meerderheid geen privacyverklaringen leest (O-Neill, 2001). Ook de respondenten antwoorden niet met een volmondige ja wanneer gevraagd werd naar de privacypolicy en of ze die gelezen hebben. Sommige hadden hem wel eens gezien, anderen hadden hem wel eens globaal doorgelezen en een enkeling wist zelfs niet dat er een privacypolicy was. De 13- tot en met 18-jarigen zijn er nog duidelijker in. Zij accepteren de gebruiksvoorwaarden en privacypolicies/statements eigenlijk altijd, zonder deze te lezen.

Toch nemen respondenten zelf wel extra maatregelen om hun privacy te beschermen. Ieder heeft hier zo zijn eigen manier voor, zoals: 'zo extreem veel erop zetten, dat je niks meer terug kan vinden wat eventueel belastend zou kunnen zijn', 'jezelf Googlen', 'niet teveel vertellen aan mensen die je niet goed kent' en 'krabbels oppervlakkig houden'. Dat betekent dat ze in ieder geval wel weten wat er kan gebeuren en dit zo goed mogelijk proberen te voorkomen. Ook de jongere gebruikers hebben hier oplossingen voor bedacht, zoals het volgende fragment aantoont. Sjoerd: 'Ja dan krabbel ik meestal naar iemand van: "hoe zit dat nou?" en ook heel vaak dan…bijvoorbeeld dat iemand iets aan mij vertelt en dan zeggen we ja we praten op Hyves wel verder en dan stuurt ze dat en als het geheim is dan hebben we wel een foefje dat je het niet kan lezen'. 'Interviewer: en wat dan precies'? Sjoerd: 'Nou, kijken welke kleur de achtergrond heeft en dan die kleur letter kiezen en dan kan je het alleen zien als je het selecteert. Alleen dan kan je het lezen' (Sjoerd, 13 jaar).

<u>Groep A</u>

Het blijkt dat de respondenten in de leeftijd van 24 tot en met 31 jaar spanning ervaren tussen exposure (het openbaar willen maken van zaken) en het beschermen van wat er echt toe doet. Eén van de respondenten ging hierop in. Tom: (…) 'Dus aan de ene kant is denk ik de drang om dingen over jezelf te laten zien belangrijk voor mensen en…daar ben ik zelf heel erg tegen aangelopen' (Tom, 31 jaar). Dat deze drang om informatie openbaar te maken vrij logisch is, wordt door Joinson & Paine (2007) opgemerkt. Dit zorgt namelijk voor het

versterken van de band tussen personen zoals Jourard &Lasakow (1958) stellen (In: Joinson & Paine, 2007). Ook binnen een groep kan het openbaar maken van gegevens positieve effecten hebben. Zo kan bijvoorbeeld de vertrouwensband binnen een groep versterkt worden, het horen bij een bepaalde groep erkend worden en de groepsidentiteit versterkt worden (Joinson &Paine, 2007). Aan de andere kant wil je niet dat er misbruik gemaakt wordt van wat jij als persoon op Hyves plaatst. Deze tegenstrijdigheid is kenmerkend voor hoe respondenten denken over privacy.

Niet alleen de bezorgdheid over privacy op het internet en op sociale netwerksites kwam ter sprake. Door de 24- tot en met 31-jarigen werd ook ingegaan op de privacygevaren in de offline wereld, zoals gegevens die de overheid van je weet, wat er gebeurt als gegevens van verzekeringsmaatschappijen op straat belanden, het volgen van GSM-gesprekken en misbruik van creditcards. Daarnaast brachten zij ter sprake dat werkgevers Hyves gebruiken voor het screenen van potentiële werknemers. Dat dit soms heel ver gaat, blijkt uit het voorbeeld van Brenda: '(…) en dan kunnen ze ook al zien aan de manier waarop jij je profiel hebt ingevuld, dus wat voor kleuren jij hebt gebruikt, wat voor achtergrond je gebruikt of dat het er netjes uit ziet. Als het er netjes uitziet en geordend is, dan ben je een net persoon, maar als je tienduizend kleuren hebt gebruikt ofzo dan zouden ze het idee hebben dat je heel erg rommelig bent' (Brenda, 24 jaar).

Het privacybewustzijn van personen blijkt binnen de groepen zelf sterk te verschillen. Zo zijn Tom en Claudia zich aardig bewust van de mogelijke gevaren binnen Hyves, terwijl Karlijn zich eigenlijk niet zoveel zorgen maakt over Hyves en de mogelijke gevaren: 'Ja ik weet niet. Ik vind dat we dan allemaal iets te achterdochtig worden. Kijken jullie iets teveel films ofzo??? Ik neem het allemaal niet zo nauw hiermee. Je hebt het allemaal zelf in de hand. En dit soort verhalen…'(Karlijn, 24 jaar).

<u>Groep B</u>

De jongere groep blijkt zich nog niet echt bewust bezig te houden met privacy. Zij zetten hun profiel voornamelijk voor iedereen open, waarbij ze soms wel de profielinformatie en krabbels uitschakelen. Sommigen weten niet precies wat ze voor wie beschikbaar maken: 'Volgens mij is bij mij alles voor iedereen. Heb er eigenlijk nog nooit echt goed naar gekeken eerlijk gezegd' (Marcel, 16 jaar). Daarnaast geven zij aan zich geen zorgen te maken over de mogelijke privacyrisico's. Ze hebben tenslotte toch niks te verbergen. Eva Kol bevestigt bovenstaande. Volgens haar zijn jongeren die opgegroeid zijn met het internet, een stuk minder 'paranoia' dan volwassen: ' (…)die volwassenen kijken vaak wat kritischer naar issues zoals privacy en ja heel veel jongeren besluiten gewoon …ik heb niks te verbergen…ik gooi mijn leven op het internet, ik schrijf blogs, ik laat overal mijn voetdruk achter en ja mensen zien maar wat ze ermee doen, ik heb geen geheimen.

Verder blijken zij niet op de hoogte te zijn van het gebruik van sociale netwerksites door werkgevers. Op de vraag: 'Denk je dat werkgevers iets zullen doen met de informatie die jij vermeldt op je profiel?' werd als volgt gereageerd: 'Volgens mij niet hoor, als ze iets willen weten dan vragen ze het wel gewoon' (Simone, 16 jaar).

Ook Marcel ging hierop in: ‘Het is wel heel nieuwsgierig als ze achter je rug om allemaal gegevens gaan opzoeken’ (Marcel, 16 jaar).

Samenvattend

De respondenten zijn van mening dat zij steeds meer aandacht hebben voor privacy en dat de bezorgdheid over hun privacy is toegenomen. Toch heeft bijna niemand de gebruiksvoorwaarden en privacypolicy gelezen. Wel nemen zij maatregelen ten behoeve van hun privacy, zoals ‘zo extreem veel erop zetten, dat je niks meer terug kan vinden wat eventueel belastend zou kunnen zijn, ‘ jezelf Googlen’, en ‘communiceren in geheimschrift’. Beide groepen zijn wel met privacy bezig, maar vooral de 24- tot en met 31-jarigen gaan daarbij in op mogelijke gevaren. De jongere groep zegt niets te verbergen te hebben en blijkt bovendien vaak hun gegevens openbaar te maken. Onderzoeken van Digibewust (2007) en Pew Internet (Lenhart & Madden, 2007), waarin wordt gesteld dat jongeren in de leeftijd van 12 tot 18 jaar veel gegevens openbaar maken, worden daarmee bevestigd. Tussen beide groepen blijkt dus een verschil te zijn in hun privacybewustzijn en privacybezorgdheid. Het onderzoek van Paine et al. (2007) wordt daarmee bevestigd.

6.5 Mogelijke risico’s binnen Hyves

Algemeen

Aan beide groepen respondenten is gevraagd of zij wel eens iets vervelends meegemaakt hebben en of zij mogelijke gevaren zien binnen Hyves. De risico’s, die in tabel 18 zijn beschreven, zijn ook afgeleid uit andere delen van het groepsgesprek. Tussendoor kwamen namelijk ook geregeld zaken aan bod, die de respondenten liever wilden voorkomen zoals het ongevraagd opslaan van gegevens door bedrijven. Onderstaande woorden werden door de respondenten niet letterlijk gebruikt, maar de uitspraken kunnen het beste op deze manier worden samengevat.

Tabel 18: *Mogelijke risico’s genoemd door respondenten*

24- tot en met 31-jarigen	**13- tot en met 18-jarigen**
1. Indringen in iemands leven	1. Indringen in iemands leven
2. Openbaarmaking (voor adverteerders)	2. Openbaarmaking
3. Data-aggregatie	3. Data -aggregatie
4. Direct marketing/targeting	4. Identiteit overnemen → Vervorming, verdraaiing
5. Stalking	5. Hacken/ wachtwoorden kraken/onderscheppen
6. Spam	
7. Bekijken/verzamelen van gegevens door werkgevers	

Door beide groepen respondenten werden indringen, het openbaar maken van gegevens en data-aggregatie als mogelijke risico's aangedragen. Deze zullen nu één voor één besproken worden.

Het ongewenst benaderen van personen door onbekenden wordt door de respondenten als hinderlijk ervaren. Door Solove (2006) wordt dit als 'invasion' aangemerkt. De respondenten geven bijvoorbeeld aan niet te zitten wachten op mails of krabbels van personen met dezelfde achternaam. Daarnaast werd ook de relatie tussen Hyves en de offline wereld aan de orde gesteld, waarbij aangegeven werd waarom bepaalde gegevens vaak privé wordt gehouden. Claudia en Brenda zeiden hierover het volgende: 'Ja adres vaak. Ik bedoel ze hoeven niet voor mijn stoep te komen staan. Het is leuk voor een krabbel, maar privé hoef ik ze niet' (Claudia, 30 jaar). 'Het is net als telefoonnummers ook en e-mailgegevens. Dat ineens mensen je beginnen te mailen of je gelijk beginnen te smsen terwijl je zelf zoiets hebt van: 'Eigenlijk heb ik helemaal geen zin in jou' (Brenda, 24 jaar).

Het openbaar maken van gegevens (door anderen) wordt ook als een mogelijk gevaar gezien. Door Solove (2006) wordt dit geplaatst onder 'information dissemination'. Door één van de respondenten werd onder andere het voorbeeld gegeven dat een willekeurig persoon een artikel plaatst met NAW gegevens van een ander. Ook gebruikers kunnen gegevens openbaar maken die nadelige gevolgen kunnen hebben zoals onderstaand voorbeeld van Kim illustreert: 'Toen was het nog niet zo dat je je profiel en je krabbels apart op 'niet zichtbaar' of 'zichtbaar' kon zetten en toen waren die krabbels dus nog zichtbaar en daar waren hele nare dingen over gegaan tussen twee vriendinnen zeg maar. Het ging over een meisje en dat meisje kon het dus lezen, omdat die krabbels niet op onzichtbaar stonden en dat is niet zo goed uitgepakt' (Kim, 17 jaar). Door een andere respondent werd ingegaan op welke informatie voor wie openbaar wordt gemaakt, waarbij hij meldde dat de verjaardag van een gebruiker via Hyves naar de gehele vriendenlijst wordt gestuurd. Volgens hem is het niet nodig dat oud-klasgenoten van de basisschool hiervan op de hoogte worden gesteld.

Het derde risico dat door beide groepen in het groepsgesprek ter sprake kwam is data-aggregatie en de gevolgen hiervan. Hierbij kwam aan de orde wat andere bedrijven met Hyves kunnen als aanvullende bron, zoals het BKR. Tom: 'Dat BKR die registratie, (…)dat is heus niet om te zien of …dat is heus wel zo…. je iemand geen krediet meer mag geven, maar je kan ook bekijken..op het moment dat je een creditcard hebt dan zie je dat iemand blijkbaar goed is voor krediet. Als hij drie creditcards heeft en een goldcard en je hebt nog wat informatie uit Hyves of weet ik veel wat' (Tom, 31 jaar). Hiermee wordt gesuggereerd dat er een heleboel informatie op internet staat die door combinatie nieuwe interessante data op kan leveren. Ook door de 13- tot en met 18-jarigen werd ingegaan op wat anderen allemaal kunnen opzoeken van je en ook in relatie tot elkaar kunnen brengen. 'Op je achternaam kunnen ze nog zoveel van je te weten komen. Omdat je al zoveel op internet heb aan KPN en dat soort dingen om adressen te zoeken, sportuitslagen en dat soort dingen. Ze kunnen toch dingen opzoeken die jij eigenlijk niet wil dat ze die weten' (Kim, 17 jaar). Bovenstaand fragment geeft weer wat door Solove (2006) 'aggregation' wordt genoemd en door ENISA (Hogben, 2007) met 'Digital Dossier aggregation' wordt bedoeld.

Groep A

De 24- tot en met 31-jarigen spraken indirect over het verdienmodel van Hyves en de privacypolicy. Bij stelling drie: Hyves neemt het niet zo nauw met de privacy, werd dit ter sprake gebracht. De respondenten gingen in op wat Hyves met de informatie, die de gebruikers verstrekken, doet en of Hyves geïnteresseerd is in die gegevens die de gebruikers openbaar maken. Volgens Tom is het verdienmodel van Hyves hier juist op gebaseerd. Het is niet zo dat ze individuele informatie verzamelen, maar ze kunnen wel informatie van bepaalde gebruikers samen pakken en op deze manier iets over een bepaalde groep zeggen. Tom gaf hier een voorbeeld van: 'Hyves kijkt naar al die profielen en denkt dan wie luisteren er naar Iron Maiden en dan zeggen ze 10 % luistert naar Iron Maiden en allemaal hebben ze de I-Phone. Dan weet I-phone of Apple dat ze daar iets mee kunnen' (Tom, 31 jaar). Op deze manier biedt Hyves bedrijven data waarmee zij een direct marketingcampagne kunnen opzetten. Door Jones & Soltron (2005) wordt dit als één van de risico's genoemd binnen Facebook.

De respondenten in de leeftijd van 24 tot en met 31 jaar gingen tijdens het focusgroepgesprek verder in op dit onderwerp, waarbij bleek dat de mate van agressiviteit bepaalt of de mailing gewenst of ongewenst is. Wanneer een mailing ongewenst is, zou dit ook ervaren kunnen worden als spam en dit is volgens de respondenten dan ook het geval. Ook kettingbrieven worden als een vorm van spam beschouwd. Ook brengen de 24- tot en met 31-jarigen het risico van stalken ter sprake, zoals Claudia aangeeft. 'Maar wat ik ook vind is stalking. Dan krijg je ineens rozen en dan kijkt je vriendje en dan denkt hij ineens van: waar ben jij geweest? En dan is het hoezo? Nou er staat een liefdesbericht. Zo heb ik me ook eens toegevoegd bij een Kamasutra Hyve. En toen dacht iedereen dat ik een paaldanseres was ofzo..weet ik veel. Dus ik kreeg steeds uitnodigingen van : 'zoooo jij bent leuk'. Dus mijn vriend denkt van: 'Zo wie zijn dat? Waar haal je ze vandaan'? (Claudia, 30 jaar). Zoals blijkt uit bovenstaand voorbeeld wordt het éénmalig, ongewenst benaderen van een persoon door Claudia gezien als stalking. Spam en stalking worden beide genoemd door ENISA (Hogben, 2007) als mogelijker risico's binnen sociale netwerksites.

Ten slotte werd er ook, zoals eerder al aan de orde is gesteld in paragraaf 6.4, ingegaan op het onderwerp werkgevers. Wanneer mensen zich niet bewust zijn van wat zij openbaar maken op hun profiel en voor wie zij dat doen, kan dat vervelend uitpakken. Brenda ging hierop in: '(…) Dus ik had echt zoiets van: hoe weten zij dat? Toen zeiden ze: 'ja, want we hebben je even op Hyves opgezocht en toen zagen we in je profiel staan dat je Feyenoord als hobby hebt'. Toen dacht ik van: 'ik ben blij dat ik mijn foto's niet openbaar heb gemaakt, zodat ze daar niet zomaar op kunnen kijken. Niet dat ik er rare foto's op heb staan dat ik met een hamer in mijn handen staan, maar toch zoiets van ze hoeven niet te zien hoe ik privé op Hyves sta' (Brenda, 24 jaar). Hoewel het soms verkeerd uit kan pakken, kan een Hyvesprofiel ook positieve effecten hebben. Zo geeft Tom aan heel bewust bezig te zijn met wat hij aan gegevens op zijn profiel zet. Zelf ziet hij dit als marketing van zichzelf. Door Kol wordt dit bevestigd.

Het schenden van de privacy wordt door de respondenten in de leeftijd van 24 tot en met 31 jaar in de online wereld niet anders ervaren als in de fysieke wereld. Volgens hen gaat het zowel in de offline wereld als online wereld om het beschermen van je bezit en wie je bent en wordt internet als een medium gezien om de privacy van personen te kunnen schenden. Verder wordt daarbij opgemerkt dat het makkelijker is om via het internet te zoeken en op deze manier gegevens te achterhalen.

Groep B

Deze laatste opmerking over 'het gemak van internet' wordt ook door de jongere groep gemaakt. Zij vinden dat het schenden van de privacy toch wel anders is, maar gaan daarbij alleen in op het feit dat door het internet op een eenvoudige manier aan gegevens gekomen kan worden.

De risico's die zij verder nog noemen hebben hier onder andere mee te maken. Zo gingen zij in op het overnemen van iemands identiteit. Volgens de 13- tot en met 18-jarigen blijkt het erg gemakkelijk te zijn om uit naam van iemand anders een account aan te maken. Dit gebeurt bijvoorbeeld vaak voor BN'ers (Beroemde Nederlanders) maar ook voor eigen vrienden is het redelijk eenvoudig om een account op te stellen met daarin gegevens van die persoon. Sjoerd ging hier als volgt op in: 'Ja, want hoe weet je nou of iemand het echt is? Hoe weet je dat nou? Ik kan zo een profiel maken van iemand anders. Ik kan heus wel een foto ergens vinden en wat gegevens invullen. En ja alleen het e-mailadres is dan anders. Maar ja dan kan ik een e-mailadres maken wat er erg op lijkt ofzo van nienke_91, maak ik dan nienke_92 ofzo. Dat kan gewoon (Sjoerd, 13 jaar). Bovenstaand fragment is een voorbeeld van 'profile squatting' zoals door ENISA (Hogben, 2007) wordt aangemerkt als één van de vijftien risico's binnen sociale netwerksites.

Bovendien is volgens de respondenten het hacken van accounts bijzonder gevaarlijk. Hierbij wordt vooral ingegaan op het kraken van wachtwoorden. Maar wachtwoorden hoeven niet altijd gekraakt te worden om in handen te komen van een ander. Uit het gesprek met de 13- tot en met 18-jarigen bleek dat het voorkomt dat gebruikers wachtwoorden verstrekken aan vriendjes en vriendinnetjes. Dat hier gevaren aan kleven, wordt door de respondenten niet onderschat zoals Marcel onder andere aangaf: 'Ja die andere persoon kan er van alles mee doen. Die kan natuurlijk heel erg aardig zijn maar ondertussen kan ze allerlei rare dingen gaan doen met je account (Marcel, 16 jaar). Dat dit vervolgens gevolgen kan hebben voor hoe mensen met je omgaan, is voor de respondenten duidelijk. Ze blijken zich er van bewust te zijn dat dit ten koste kan gaan van de vriendenkring en dat het moeilijk is om uit te leggen dat jij het niet was die bepaalde dingen gezegd of gedaan hebt binnen Hyves. Ook Hyves zelf is zich hiervan bewust en heeft in haar privacypolicy daarover het volgende opgenomen: 'Houd ook je wachtwoord geheim om te voorkomen dat anderen, zonder jouw toestemming, gebruik maken van jouw Hyves account' (Hyves-Privacypolicy, 2008).

Samenvattend

De respondenten van beide groepen geven in totaliteit een aardig compleet beeld van de mogelijke risico's binnen , waarbij er wel een duidelijk verschil is tussen de twee groepen. Hoewel er ook overeenkomsten te vinden zijn: beide groepen noemen namelijk (1) binnendringen in iemands leven, (2) openbaarmaking en (3) data-aggregatie, blijkt de oudere groep toch veel meer bezig te zijn met wat andere partijen met hun gegevens kunnen doen en noemen zij ook meer risico's. De jongere groep respondenten in de leeftijd van 13 tot en met 18 jaar is hier niet mee bezig en de risico's die genoemd worden blijven dan ook vooral beperkt tot risico's die zich binnen hun vriendennetwerk kunnen voordoen.

6.6 Privacywaarborging binnen en door Hyves

Algemeen

Op de stelling 'Hyves neemt het niet zo nauw met privacy' werd door de respondenten wisselend gereageerd. Van de groep met personen in de leeftijd van 24 tot en met 31 jaar waren twee personen het eens met de stelling. Alle respondenten in de leeftijd van 13 tot en met 18 jaar waren het oneens met de stelling, hoewel in de discussie ook het andere standpunt werd ingenomen. Hoewel er dus verschillen waren tussen beide groepen bleek aan het einde van beide discussies dat de respondenten het er over eens zijn dat het aan de gebruiker zelf is om de privacy te beschermen en dit in de hand te houden, maar dat Hyves er daarnaast alles aan doet om de functies aan te bieden waarmee dit ook mogelijk is. Dit wordt bevestigd door de volgende quote van Jacqueline: 'Je kan zelf beslissen wie jouw foto's mogen zien en wie jouw krabbels kunnen lezen. Je hebt het allemaal zelf in de hand. En er kunnen alsnog wel dingen gebeuren, maar dat ligt denk ik niet aan het systeem van Hyves zelf' (Jacqueline, 18 jaar). Ook volgens de oudere groep houdt Hyves tegenwoordig meer rekening met de privacy van haar gebruikers. Hyves biedt namelijk steeds meer mogelijkheden om bepaalde informatie alleen zichtbaar te maken voor bijvoorbeeld vrienden. Dat de verantwoordelijkheid om daar vervolgens iets mee te doen bij de gebruiker ligt, kwam als volgt tot uiting: 'Zij bieden jou de mogelijkheden maar uiteindelijk beslis je zelf. Het is niet zo dat Hyves ervoor zorgt dat mijn gegevens niet gepubliceerd worden. Dat doe ik zelf' (Sander, 26 jaar). Wel opgemerkt werd dat Hyves als commerciële organisatie belang heeft bij het verzamelen van gegevens en waarschijnlijk tot het uiterste zal gaan van wat wettelijk mag in relatie tot het verzamelen, gebruiken en verspreiden van gegevens van gebruikers.

Zoals naar voren komt in de quotes van Sander en Jacqueline, blijken zowel de functies die Hyves biedt als de manier waarop gebruikers hier mee omgaan van invloed te zijn op hoe zij de privacywaarborging ervaren. Blijkbaar zijn dus privacybewustzijn en de controlemogelijkheden die door de aanbieder worden aangeboden aan de gebruiker van invloed op hoe gebruikers hun privacy beleven en het gevoel hebben dan hun privacy gewaarborgd wordt. Onder de mate van controle worden de mogelijkheden die de aanbieder biedt, dus de functies en tools, bedoeld waarmee de gebruikers controle kunnen houden over welke gegevens getoond worden en aan wie zij openbaar worden gemaakt. Onder privacybewustzijn wordt het nadenken over privacy en de actie die wordt ondernomen om privacy te beschermen, bedoeld. De mate van privacybewustzijn is

mogelijk van invloed op hoe zij de functies en tools die worden aangeboden, gebruiken en wat zij wel dan niet openbaar maken.

Vooral de jongere gebruikers vinden de privacypolicy en gebruiksvoorwaarden vaak moeilijk te begrijpen en geven aan deze daarom vaak niet te lezen en gewoon te accepteren. Hoe dit voor Hyves is werd tijdens de focusgroepgesprekken niet direct duidelijk. Aan de respondenten is daarom gevraagd om enkele fragmenten uit de gebruiksvoorwaarden en privacypolicy te lezen en hun mening daarover te geven. Voor de meeste personen was de tekst duidelijk, hoewel zij wel verwachten dat het voor kinderen en jongeren soms moeilijk te begrijpen zal zijn. Ook Sjoerd merkte dit op: (…) voor mensen van ongeveer mijn leeftijd is het toch wel wat te moeilijk te lezen. Met al die nette en moeilijke woorden (Sjoerd, 13 jaar). Peter vermeldt dat het misschien verstandig zou zijn als de tekst simpeler te maken, ook al moeten ouders toestemming geven aan hun kinderen om lid te worden van Hyves wanneer zij jonger dan 16 zijn. Volgens Jacqueline zouden voorbeelden in de tekst misschien helpen. Verder werd over het algemeen aangegeven dat de privacypolicy en gebruiksvoorwaarden wel goed en duidelijk zijn. Van de 7 personen, afkomstig uit beiden groepen, plaatsten slechts twee personen een inhoudelijke opmerkingen bij de fragmenten. ‘Maar, ik vind het wel wat ver gaan dat ze direct stellen de bestanden, die jij ter beschikking stelt, te mogen gebruiken’ (Sander, 26 jaar).‘Het houdt dus eigenlijk in, dat als Hyves eventueel fouten zou maken, zodat er gegevens van gebruikers verloren gaan, Hyves nooit aansprakelijk daarvoor is. Dat vind ik best wel wazig. Ze kunnen ook expres zonder dat ze daartoe aanleiding hebben, gewoon honderden foto's en gegevens enz. verwijderen. Ze kunnen er toch niet voor aansprakelijk worden gesteld. Dus dat zou ik wel anders willen zien’ (Marcel, 16 jaar).

<u>Groep A</u>

Met de stelling: ‘Hyves heeft een goede keuze gemaakt. Als jij je profiel afschermt, mag je ook niet meer bij anderen gluren’ zijn de meeste respondenten in de leeftijd van 24 tot en met 31 jaar het eens. Slechts een persoon is het oneens. Vanuit een commercieel oogpunt wordt deze beslissing als een logische beslissing voor Hyves beschouwd, omdat op deze manier de wet van wederkerigheid gebruikt wordt om de gebruikers zover te krijgen om hun profiel open te stellen. Brenda legt dit als volgt uit: ‘Ja dat is dan slecht voor ons, maar voor Hyves is het gewoon, zoals net al gezegd, de manier om er voor te zorgen het profiel dus toch open te stellen, want anders is het niet meer leuk om op Hyves te zitten, want dan kan je niet meer bij anderen kijken. Dus dan heb je misschien zelf zo iets van, misschien moet ik mijn profiel dan toch maar voor vrienden van vrienden open zetten in plaatst van dat je het misschien eerst alleen voor vrienden had, zodat je dus toch nog wel bij die vrienden van je vrienden kan kijken’ (Brenda, 24 jaar). De persoon die het oneens is met de stelling beroept zich bij de argumentatie op de beperking van de vrijheid. Volgens haar wordt je als gebruiker beperkt in je keuzevrijheid en wordt de keuze als het ware geforceerd.

Aan de respondenten is gevraagd of er diensten, tools of functies zijn die zij graag anders zouden willen zien binnen Hyves. Binnen de groep 24- tot en met 31-jarigen werd ingegaan op twee onderwerpen. Door één van de respondenten werd opgemerkt dat er binnen de vriendengroep weer verschillende soorten 'vrienden' zijn aan te wijzen en dat wellicht niet alles voor iedereen van relevantie is. Peter: 'Maar wat ik net ook al zei: je hebt kennissen en je hebt vrienden' (Peter, 25 jaar). Ook werd ingegaan op het feit dat Hyves vaak standaard dingen aanvinkt en dat de gebruiker deze dan later wel uit kan zetten. De respondenten zijn het er wel over eens: als je dit niet ziet zitten moet je ook niet aan Hyves beginnen. Wel wordt opgemerkt dat vaak van te voren niet duidelijk is voor de gebruiker hoe alles precies werkt. Als gebruiker moet je zelf op onderzoek uitgaan. Peter: 'Nou ik denk niet dat je weet als je eraan begint dat je dingen moet gaan blokkeren denk ik. Het zou wel beter zijn als ze je van te voren vertellen hoe het zit. Maar dat doen ze niet. Je moet zelf op onderzoek uitgaan' (Peter, 25 jaar).

Groep B

Vrijwel alle jongeren in de leeftijd van 13 tot en met 18 jaar, op één persoon na, zijn het oneens met de volgende stelling. 'Hyves heeft een goede keuze gemaakt. Als jij je profiel afschermt, mag je ook niet meer bij anderen gluren'. Zij vinden dat het ook aan de gebruiker zelf is om dit te beslissen. Toch begrijpen ze wel dat Hyves deze beslissing heeft genomen: '(…) Omdat ik ook wel weer snap…ik wil niet dat jij het bij mij doet, dus dan snap ik ook wel weer dat die ander wil dat ze het bij hem ook niet doen' (Sjoerd, 13 jaar).

Ook aan de jongere respondenten is gevraagd of er diensten, tools of functies zijn die zij graag anders zouden willen zien binnen Hyves. Door de jongeren uit groep B worden ook enkele opmerkingen geplaatst die vooral met de veiligheid binnen Hyves te maken hebben. Zo vinden enkele respondenten het een gedoe om het wachtwoord te veranderen en wordt door Sjoerd opgemerkt dat het inloggen soms verkeerd gaat, hoewel dat meer aan hem zelf bleek te liggen dan aan het systeem. Wel wordt door de 13- tot en met 18-jarigen aanbevolen om een extra identificatiecontrole plaats te laten vinden, om op deze manier te controleren of de gebruiker is, wie hij of zij zegt dat hij is. Daarnaast wordt opgemerkt dat het misschien handig is als er extra beveiliging is bij het inloggen door middel van een activeercode.

Samenvattend

De respondenten zijn van mening dat het aan de gebruiker zelf is om de privacy te beschermen, maar dat Hyves er daarnaast alles aan doet om de functies aan te bieden waarmee dit ook mogelijk is. Toch worden door beide groepen enkele opmerkingen of verbeterpunten genoemd. Hierbij werd onder andere ingegaan op de privacypolicy en gebruiksvoorwaarden, identificatiecontrole, verschillende soorten vrienden binnen de vriendengroep en de communicatie over wat kan binnen Hyves en de standaardinstellingen.

6.7 Samenvatting en conclusie

In deze conclusie wordt antwoord gegeven op deelvraag 1: **Hoe beleven gebruikers van sociale netwerksites hun online privacy?** Om deze vraag te kunnen beantwoorden zijn de subdeelvragen c tot en met h opgesteld, die nu één voor één beantwoord zullen worden. Subdeelvraag h zal daarbij niet afzonderlijk beantwoord worden, maar bij alle subdeelvragen aan de orde worden gebracht, indien relevant.

Hoe definiëren gebruikers van sociale netwerksites privacy en welke waarden vinden zij belangrijk met betrekking tot hun privacy?

Door de respondenten wordt een ruime beschrijving gegeven van wat zij onder privacy verstaan, waarbij wel heel duidelijk de informationele dimensie tot uiting komt. Door de respondenten in de leeftijd van 24 tot en met 31 jaar wordt daarnaast de relationele dimensie meegenomen in hun definitie en bovendien gaan zij in op het doel van het beschermen van hun privacy, namelijk imagobescherming. De waarden en criteria die genoemd zijn door de oudere groep respondenten komen aardig overeen met de waarden en criteria die door Smink et al. (1999) zijn beschreven. Het zelf keuzes kunnen maken, ongestoord kunnen leven, bewegingsvrijheid hebben en het vrij blijven van stigmatisering worden door de respondenten allemaal genoemd. Daarnaast blijkt de verwachting van Dubbeld (2000) gedeeltelijk te kloppen. Gebruikers van Hyves blijken inderdaad de zeggenschap en controle die een gebruiker bezit over zijn persoonlijke sfeer ook in het digitale tijdperk als een belangrijke voorwaarde voor de privacy te beschouwen. Verder komt duidelijk naar voren dat het uitgangspunt van Gutwirth, dat privacy onlosmakelijk verbonden is met de individuele vrijheid van de mens, belangrijk is. De jongere groep respondenten blijkt eerlijkheid en vertrouwen erg belangrijk te vinden, waarbij het vertrouwen van hun vrienden en de eerlijkheid die daar onlosmakelijk mee verbonden is, centraal staan. Het nakomen van beloftes is daarbij zeer belangrijk.

In hoeverre houden gebruikers van sociale netwerksites zich bezig met privacyissues in sociale netwerksites?

De respondenten zijn van mening dat zij steeds meer aandacht hebben voor privacy en dat de bezorgdheid over hun privacy is toegenomen. Dit is versterkt door de nieuwsitems die op televisie worden uitgezonden en de politiek die zich ook steeds meer bezig houdt met privacyissues. Toch hebben zeer weinig respondenten de gebruiksvoorwaarden en privacypolicy gelezen. Wel nemen zij maatregelen ten behoeve van hun privacy, zoals ‘zo extreem veel erop zetten, dat je niks meer terug kan vinden wat eventueel belastend zou kunnen zijn, ‘ jezelf Googlen’, en ‘communiceren in geheimschrift’. Beide groepen zijn wel met privacy bezig, maar vooral de 24- tot en met 31-jarigen gaan daarbij in op mogelijke gevaren. De jongere groep zegt niets te verbergen te hebben en blijkt bovendien vaak hun gegevens openbaar te maken. Sommigen weten niet precies wat ze voor wie beschikbaar maken. Bovendien blijken zij niet op de hoogte te zijn van het gebruik van sociale netwerksites door werkgevers. Onderzoeken van Digibewust (2007) en Pew Internet (Lenhart & Madden, 2007) waarin wordt gesteld dat jongeren veel gegevens openbaar maken, worden daarmee bevestigd. Daarnaast is er een verschil in privacybewustzijn van personen waar te nemen binnen beide groepen.

Welke risico's zien zij voor hun privacy in online sociale netwerken?

Door de respondenten wordt een aardig compleet beeld gegeven van de mogelijke risico's binnen Hyves, waarbij wel een duidelijk verschil blijkt tussen de twee groepen. Hoewel er ook overeenkomsten te vinden zijn: beide groepen noemen namelijk (1) binnendringen in iemands leven, (2) openbaarmaking en (3) data-aggregaties, blijkt de oudere groep toch veel meer bezig te zijn met wat andere partijen met hun gegevens kunnen doen en noemen zij ook meer risico's. De jongere groep respondenten in de leeftijd van 13 tot en met 18 jaar is zich niet bewust van deze risico's. De risico's die zij noemen blijven dan ook beperkt tot risico's die binnen hun vriendennetwerk aan de orde kunnen zijn.

In hoeverre vinden gebruikers dat sociale netwerksites hun privacy waarborgen?

Volgens de respondenten is het aan de gebruiker zelf om de privacy te beschermen, maar doet Hyves er daarnaast alles aan om functies aan te bieden waarmee dit ook mogelijk is. Zowel de functies die Hyves biedt als de manier waarop gebruikers hier mee omgaan, blijken van invloed te zijn op hoe zij de privacywaarborging ervaren. Blijkbaar zijn dus privacybewustzijn en controlemogelijkheden die door de aanbieder worden aangeboden aan de gebruiker van invloed op hoe gebruikers hun privacy beleven en het gevoel hebben dat hun privacy gewaarborgd wordt.

Wat willen gebruikers zelf met betrekking tot privacywaarborging op sociale netwerksites?

Door de respondenten zijn enkele aandachtspunten voor Hyves geformuleerd. Zo blijkt dat er binnen de vriendengroep verschillende soorten vrienden zijn aan te wijzen, waarbij wellicht niet alle functies voor iedereen van belang zijn. Ook blijkt dat de respondenten vinden dat Hyves vaak standaard dingen aanvinkt en dat de gebruiker deze dan later wel uit kan zetten. Daarbij wordt opgemerkt dat vaak van te voren niet duidelijk is voor de gebruiker hoe dit werkt. Als gebruiker moet je zelf op onderzoek uitgaan. Volgens een respondent zou het misschien beter zijn als van te voren duidelijk is hoe dit werkt. Bovenstaande aandachtspunten die door de 24- tot en met 31-jarigen zijn geformuleerd, worden door de 13- tot en met 18-jarigen niet vermeld. Zij gaan vooral in op de veiligheid binnen Hyves. Zo vinden enkele respondenten het een gedoe om het wachtwoord te veranderen en wordt door één respondent opgemerkt dat het inloggen soms verkeerd gaat, hoewel dat meer aan hem zelf bleek te liggen dan aan het systeem. Wel wordt door de jongere groep respondenten aanbevolen om een extra identificatiecontrole plaats te laten vinden, om op deze manier te controleren of de gebruiker ook echt is, wie hij of zij zegt te zijn. Daarnaast vinden vooral de gebruikers in de leeftijd van 13 tot en met 18 jaar de privacypolicy en gebruiksvoorwaarden vaak moeilijk te begrijpen en geven zij aan deze daarom vaak niet te lezen en gewoon te accepteren. Na het lezen van delen van de privacypolicy en gebruiksvoorwaarden, blijken vooral de gebruiksvoorwaarden ingewikkeld te zijn voor de jongste respondenten. Door beide groepen werd dan ook vermeld dat het misschien verstandig zou zijn om de tekst simpeler te maken.

7. CONCLUSIE EN DISCUSSIE

'Privacy is the people's right to prevent the disclosure of personal information to others and the right to be free from intrusion and social control by others'.

Bovenstaande definitie is een combinatie van definities van verschillende auteurs: Westin (1967), DeCew (1997) en Woo (2006). Deze definitie is in dit onderzoek vergeleken met hoe gebruikers van sociale netwerksites, als groep, privacy definiëren. Gebruikers van 13 tot en met 18 jaar en 24 tot en met 31 jaar omschrijven privacy op een wijze die nagenoeg overeenkomt met bovenstaande definitie. Daarnaast vinden de gebruikers de drie dimensies van privacy belangrijk, hoewel de meeste aandacht toch uit gaat naar de informationele dimensie. Tussen de onderzochte leeftijdsgroepen zijn overeenkomsten waar te nemen. Toch hanteren 24- tot en met 31- jarigen een breder perspectief ten aanzien van privacy. Dit komt tot uiting in de waarden en risico's die zij noemen. Verder is een verschil in privacybewustzijn en privacybezorgdheid tussen de verschillende leeftijdsgroepen waar te nemen: bij de oudere groep zijn bewustzijn en bezorgdheid verder ontwikkeld. Ook binnen leeftijdsgroepen is dit verschil waarneembaar. Tot slot blijkt uit beide deelonderzoeken (inhoudsanalyse en belevingsonderzoek) dat de privacywaarborging voldoende is, maar dat er nog wel verbeterpunten zijn.

Bovenstaande alinea geeft de belangrijkste conclusies weer van dit onderzoek, waarbij antwoord wordt gegeven op de hoofdvraag: ***'Hoe beleven gebruikers van sociale netwerksites hun online privacy en in hoeverre spelen aanbieders van sociale netwerksites hierop in?'*** Om een antwoord te kunnen geven op bovenstaande vraag is gekozen voor een casestudy van de sociale netwerksite Hyves. In de komende paragrafen zullen de conclusies verder worden toegelicht.

7.1 Privacybegrip verandert nauwelijks

Allereerst zal in deze conclusie antwoord worden gegeven op de deelvraag: '*Hoe beleven gebruikers van sociale netwerksites hun online privacy?* Daarbij is gekeken in hoeverre de beleving van Hyves-gebruikers overeenkomt met traditionele theorieën over privacy.

Gebruikers vinden de drie dimensies van privacy belangrijk binnen Hyves

Hoewel eerder onderzoek zich nauwelijks gericht heeft op alle drie de dimensies van privacy: de ruimtelijke, relationele en informationele dimensie, blijkt uit dit onderzoek dat deze dimensies voor gebruikers wel degelijk van belang zijn binnen een sociale netwerksite. Gebruikers willen soms graag met rust gelaten worden, zitten niet altijd te wachten op bepaalde sociale contacten en willen graag controle houden over deze sociale contacten. De verwachting van Dubbeld (2000) blijkt te kloppen. Gebruikers van Hyves blijken inderdaad de zeggenschap en controle, die een gebruiker bezit over zijn persoonlijke sfeer en de bescherming van zichzelf, ook in het digitale tijdperk als belangrijke voorwaarden voor de kwaliteit van privacy te beschouwen. Niet

alleen online is privacy belangrijk voor gebruikers, ook wordt privacy doorgetrokken naar het 'echte leven'. Vooral de relationele en ruimtelijke dimensie zijn hierbij belangrijk. Uitsluitend de oudere groep heeft hier oog voor. Bovendien willen de gebruikers hun persoonlijke gegevens beschermen. Verwacht wordt dat deze drie algemene dimensies van privacy ook binnen andere sociale netwerksites, zoals Facebook en Myspace, belangrijk zijn in relatie tot online privacy, omdat deze netwerksites veel overeenkomsten hebben.

Meeste aandacht gaat uit naar de informationele dimensie

De meeste aandacht van gebruikers gaat uit naar de informationele dimensie, wat voor een sociale netwerksite, waarbij het delen en communiceren van informatie één van de belangrijkste zaken is, niet vreemd is. Daarom wordt verwacht dat de informationele dimensie ook binnen andere sociale netwerksites en web 2.0 omgevingen de belangrijkste dimensie zal zijn. Gebruikers van Hyves geven namelijk een ruime beschrijving van privacy waar de informationele dimensie een groot deel van uitmaakt. Hoewel de overige dimensies in de groepsgesprekken wel besproken werden, zijn deze nauwelijks terug te vinden in de definities die door de respondenten zijn opgesteld. Vooral de definitie die Westin in 1967 ter sprake bracht, namelijk privacy als: 'the right to prevent the disclosure of personal information to others' (Westin, 1967), blijkt voor de respondenten belangrijk te zijn. Het privacybegrip is volgens de respondenten niet aan het veranderen, hoewel de invulling ervan door het internet wel degelijk verandert. Zoals Gutwirth (1998) en Lessig (1998) opmerken, is de verwerking, convergentie en digitalisering van informatie versterkt. Dit resulteert in een toename van wat kan worden bijgehouden en waargenomen. De gebruikers gaan hierop in, waarbij wordt opgemerkt dat het makkelijker is om gegevens te achterhalen via internet. Deze informatie is namelijk 'searchable' zoals door Lessig (1998) in zijn studie wordt betoogd.

Gebruikers in de leeftijd van 24 tot en met 31 jaar hanteren een breder privacy perspectief

Er worden veel verschillende waarden genoemd, waarbij de focus binnen de groepen wel op andere waarden ligt. De controle die de gebruiker heeft over zijn gegevens blijkt één van de belangrijkste zaken te zijn in relatie tot Hyves. De waarden en criteria die de gebruikers noemen, komen aardig overeen met de waarden en criteria die door Smink et al. (1999) zijn beschreven. Het zelf keuzes kunnen maken, ongestoord kunnen leven, bewegingsvrijheid hebben en het vrij blijven van stigmatisering blijken voor de gebruikers belangrijk te zijn. De jongere groep respondenten (13 tot en met 18 jaar) vindt eerlijkheid en vertrouwen erg belangrijk. De oudere groep blijkt vooral vrijheid een belangrijke waarde te vinden bij privacy. Het uitgangspunt van Gutwirth dat privacy onlosmakelijk verbonden is met de individuele vrijheid van de mens is dus heel belangrijk. Waar de ouderen zich vooral richten op werkgevers en commerciële bedrijven wanneer over privacy en risico's wordt gesproken, blijft de omgeving van de jongere groep beperkt tot hun vriendenkring. Waarschijnlijk heeft dit met leeftijd en perceptie te maken. Ook bovenstaande conclusie zal naar verwachting gelden binnen andere sociale netwerksites, aangezien er geen aanwijzingen zijn dat privacy door gebruikers van andere sociale netwerksites anders gedefinieerd wordt en dat zij andere waarden zullen noemen.

Verschil in privacybewustzijn en privacybezorgdheid tussen en binnen verschillende leeftijdsgroepen

Gebruikers in de leeftijd van 13 tot en met 18 jaar zijn in vergelijking met de oudere groep minder privacybewust. Onder privacybewustzijn wordt het nadenken over privacy en de actie die wordt ondernomen om privacy te beschermen bedoeld. De jongere groep zegt niets te verbergen te hebben en blijkt bovendien vaak hun gegevens openbaar te maken. Sommigen weten niet precies wat ze voor wie beschikbaar maken. Bovendien zijn zij niet op de hoogte van het gebruik van sociale netwerksites door werkgevers. Onderzoeken van Digibewust (2007) en Pew Internet (Lenhart & Madden, 2007) waarin wordt gesteld dat jongeren in de leeftijd van 12 tot 18 jaar veel gegevens openbaar maken, worden daarmee bevestigd. Wel zijn zij van mening dat steeds meer aandacht uitgaat naar privacy en naar eventuele gevaren voor de privacy. De gebruikers in de leeftijd van 24 tot en met 31 jaar geven dit duidelijk aan en ondernemen bovendien actie. Ieder heeft hier zo zijn eigen manier voor zoals: 'zo extreem veel erop zetten, dat je niks meer terug kan vinden wat eventueel belastend zou kunnen zijn, 'jezelf Googlen', 'niet teveel vertellen aan mensen die je niet goed kent' en 'krabbels oppervlakkig houden'. Beide groepen geven aan dat zowel eigen ervaring als berichtgeving in de media een rol spelen bij deze toename van het privacybewustzijn. Wanneer de vergelijking getrokken wordt met de privacy-segmentation van Westin, kan gezegd worden dat de respondenten van 13 tot en met 18 jaar over het algemeen te plaatsen zijn in de groep van de 'privacy unconcerned', terwijl de oudere groep respondenten (24 tot en met 31 jaar) over het algemeen tot de 'privacy pragmatists' gerekend kan worden. Toch blijkt de mate van privacybewustzijn ook binnen de leeftijdsgroepen flink te verschillen. Mogelijk houdt dit verband met de leeftijden van de respondenten, want ook binnen de groepen verschilden de leeftijden behoorlijk. Ook zou dit met andere factoren te maken kunnen hebben, zoals interesse en kennis over het onderwerp.

Kortom, hoewel de informationele dimensie het meest nadrukkelijk aanwezig is, blijken ook de ruimtelijke en relationele dimensie van belang te zijn bij online privacy. De definities die door de beide groepen zijn opgesteld, kennen veel overeenkomsten met de definitie die in het theoretisch kader is geformuleerd en waarmee tevens deze conclusie is begonnen. Geconcludeerd mag worden dat de definiëring van privacy en privacybeleving van (jonge) gebruikers van Hyves niet wezenlijk anders is dan traditionele theorieën en definities van privacy. Door de respondenten zelf wordt dit ook opgemerkt. Zij zijn van mening dat het privacybegrip zelf niet aan het veranderen is. Het kader blijft hetzelfde, hoewel de toepassing ervan door de komst van het internet wel anders is geworden en steeds (meer) zal veranderen.

7.2 Privacywaarborging voldoende, maar nog mogelijkheden tot verbeteren door Hyves

In de tweede plaats gaat deze conclusie in op overeenkomsten en verschillen tussen wat gebruikers willen ten aanzien van hun privacy en de mate waarin Hyves hierop inspeelt.

De controle die de gebruiker heeft over zijn gegevens en de vrijheid om zelf te kunnen beslissen welke informatie openbaar wordt gemaakt en voor wie, blijken het belangrijkst te zijn voor gebruikers binnen Hyves. Hyves speelt hierop in zoals is gebleken in hoofdstuk zes. De afgelopen jaren heeft de sociale netwerksite

namelijk steeds meer mogelijkheden gecreëerd voor gebruikers, waardoor zij zelf kunnen bepalen welke gegevens openbaar worden gemaakt en voor wie. Bovendien heeft Hyves toegezegd zich meer bezig te gaan houden met de bescherming van de privacy. Dit gaat zij onder andere doen met behulp van organisaties zoals Digibewust en Mijn Kind Online (Spits, 2007). Hieruit kan geconcludeerd worden dat Hyves het belang van privacy ziet en het belang van privacy erkent.

Toch zou Hyves nog een extra stap kunnen zetten om het voor de gebruikers gemakkelijker te maken hun privacy te beschermen. Volgens de gebruikers is het namelijk nog steeds hun eigen verantwoordelijkheid om hun privacy te beschermen, waarbij Hyves vooral de tools daarvoor aan moet bieden. Volgens de respondenten doet Hyves dit ook en zijn de mogelijkheden die de site biedt prima. Niettemin worden enkele huidige beperkingen en daarmee toekomstige verbeterpunten genoemd. Door de respondenten worden namelijk een aantal risico's genoemd, die als volgt kunnen worden samengevat: indringen in iemands leven, openbaarmaking van gegevens (voor adverteerders), data-aggregatie, direct marketing, stalking, spam, identiteitsovername, hacken, wachtwoorden kraken/onderscheppen en het bekijken en verzamelen van gegevens door werkgevers worden als mogelijke risico's beschouwd door de respondenten. Door de gebruikers in de leeftijd van 24 tot en met 31 jaar werden meer risico's genoemd dan door de 13- tot en met 18-jarigen. Sommige risico's die door respondenten worden genoemd, probeert Hyves te ondervangen. Doorstuurmailtjes en kettingbrieven die via de Hyves-inbox worden doorgestuurd, probeert Hyves op te sporen. De communitymanagers van Hyves houden zich hier mee bezig. Daarnaast kunnen gebruikers melding maken van stalking en kunnen zij gebruik maken van de blokkeerfunctie op Hyves. De automatisch gegenereerde gegevens, zoals IP-adressen, worden gebruikt om stalkers te achterhalen. Bovendien kan aan Hyves een bericht worden gestuurd of op de 'Dit is niet OK knop' gedrukt worden. Toch blijkt Hyves niet alle risico's die door gebruikers worden genoemd, te kunnen voorkomen of ondervangen. Daarom blijft het belangrijk dat gebruikers zich bewust zijn van deze risico's en dat Hyves hiervan op de hoogte is en actie onderneemt.

7.3 Aandachtspunten voor Hyves

Door de respondenten zijn diverse opmerkingen geplaatst waar Hyves op dit moment (nog) geen (of niet genoeg) aandacht voor heeft. Deze opmerkingen en conclusies zijn vergeleken met de privacywaarborging door Hyves zelf. Hieruit kan worden afgeleid dat Hyves op enkele punten nog verbeteringen kan realiseren. De belangrijkste aandachtspunten zullen hieronder worden beschreven.

Zorg voor transparante en open communicatie naar gebruikers.

Meer duidelijkheid over privacypolicy en gebruiksvoorwaarden

Vooral gebruikers in de leeftijd van 13 tot en met 18 jaar vinden de gebruiksvoorwaarden van Hyves moeilijk te begrijpen en geven daarnaast aan de privacypolicy en gebruiksvoorwaarden vaak niet te lezen. Bovendien wordt ook door de respondenten in de leeftijd van 24 tot en met 31 jaar vermeld dat het misschien verstandig zou zijn om de tekst simpeler te maken. De privacypolicy blijkt al wel redelijk duidelijk te zijn. Vooral de

gebruiksvoorwaarden kunnen simpeler opgeschreven worden. Bovendien zou aangegeven moeten worden wanneer er wijzigingen in de gebruiksvoorwaarden zijn opgetreden en van welke datum de actuele gebruiksvoorwaarden zijn.

Gebruiksvriendelijkheid

Gebruikers zijn niet helemaal tevreden over de standaardinstellingen. Vaak is van te voren niet duidelijk dat gebruikers standaard staan aangemeld voor bepaalde functionaliteiten en dat zij zich hiervoor af kunnen melden. Geconcludeerd mag worden dat zij hier graag vooraf over geïnformeerd willen worden. Uit de groepsgesprekken blijkt dat vooral de jongere gebruikers menen niets te verbergen te hebben en dus vaak veel gegevens openbaar maken. Daarnaast zijn zij niet op de hoogte van het gebruik van sociale netwerksites door werkgevers. Zij gaan bij de risico's nauwelijks in op risico's die kunnen ontstaan buiten hun eigen sociale omgeving. Hyves zou nog een stap kunnen zetten door vooral jonge gebruikers van Hyves voor te lichten over het verstandig omgegaan met hun gegevens binnen de sociale netwerksite en de mogelijke risico's die kunnen ontstaan. Bovenstaande wordt door Kol en door het College Bescherming Persoonsgegevens bevestigd.

Verbeter en behoud de veiligheid binnen Hyves.

Identificatie controle

Omdat zeer veel persoonlijke gegevens openbaar gemaakt kunnen worden en veel mensen dit ook doen, is het vrij gemakkelijk om je voor te doen als iemand anders en allerlei combinaties van correcte en valse gegevens van deze persoon openbaar te maken. Hierbij kan gedacht worden aan persoonsgegevens en contactgegevens, maar ook aan foto's en blogs. Hoewel gebruikers op de hoogte zijn van de 'DitisnietOK-knop, waarmee een melding gemaakt kan worden van een nepprofiel, wordt aanbevolen om een extra identificatiecontrole plaats te laten vinden, om op deze manier te controleren of de gebruiker is, wie hij of zij zegt dat hij is.

Verbeter de controle (mogelijkheden) door gebruikers.

Subgroepen binnen vriendengroepen

Tot op heden blijkt het niet mogelijk te zijn om te bepalen welke gegevens voor subgroepen binnen de vriendengroep te zien zijn. In het soort vriend is dus geen hiërarchie aan te brengen, terwijl het aannemelijk is dat sommige mensen bepaalde informatie wel aan een vriend kenbaar willen maken, maar niet aan een collega. Dat dit inderdaad zo is wordt door een respondent bevestigd. Ook Kol (2008) gaat hier in haar boek op in en spreekt van botsende werelden. Volgens Kol zou Hyves hier wel iets mee kunnen, maar is het wel veel werk voor de gebruiker. Toch mag verwacht worden dat (sommige) gebruikers hier gebruik van willen maken. Daarom wordt aanbevolen om subcategorieën te introduceren binnen de 'vriendengroep'.

Afschermen/openbaar maken van gegevens

Bovendien blijkt Hyves soms beslissingen te nemen die voor gebruikers niet altijd gunstig zijn en waarmee zij beperkt worden in hun vrijheid. Een voorbeeld daarvan is de beslissing die Hyves op 24 april 2008 nam over de

afscherming van de profielen van gebruikers. In het voorjaar van dit jaar besloot Hyves hier regels aan te willen stellen. Volgens enkele respondenten moet de keuze aan de gebruiker zijn om te bepalen of zijn of haar profiel open mag staan voor anderen, terwijl nog wel bij andere gebruikers gekeken mag worden. Daarom zou Hyves in overweging moeten nemen om deze beslissing terug te draaien of nog meer mogelijkheden te bieden om bepaalde delen binnen het profiel van de gebruiker af te schermen.

7.4 Aandachtspunten voor gebruikers

Hoewel blijkt dat gebruikers op een aantal punten kritiek leveren, kan geconcludeerd worden dat ook gebruikers bewuster om moeten gaan met hun privacy. De groep respondenten in de leeftijd van 13 tot en met 18 jaar gaat hier zelf op in, waarbij ze wel opmerken zich steeds meer bewust te worden van de gevaren. De onderstaande drie aanbevelingen zouden vooral jongeren kunnen helpen om beter om te gaan met hun privacy.

Let op welke gegevens je online zet en voor wie deze beschikbaar zijn.

Wanneer mensen zich niet bewust zijn van wat zij openbaar maken op hun profiel en voor wie zij dat doen, kan dat vervelend uitpakken. Zoals bleek uit de theorie en uit de groepsgesprekken, gebruiken onder andere werkgevers informatie uit Hyves voor het screenen van kandidaten. Jongeren in de leeftijd van 13 tot en met 18 jaar zijn hier niet tot nauwelijks van op de hoogte. Aanbevolen wordt om te bekijken welke gegevens openbaar gemaakt worden en voor wie en eventueel als gevolg hiervan aanpassingen te doen.

Geef nooit je wachtwoord aan een ander.

Ten tweede blijkt uit het gesprek met de 13- tot en met 18-jarigen dat het voorkomt dat gebruikers wachtwoorden verstrekken aan vriendjes en vriendinnetjes. Ook Hyves zelf is zich hiervan bewust en heeft in haar privacypolicy daarover het volgende opgenomen: ‘Houd ook je wachtwoord geheim om te voorkomen dat anderen, zonder jouw toestemming, gebruik maken van jouw Hyves account’ (Hyves-Privacypolicy, 2008). Kortom, aanbevolen wordt om geen wachtwoorden aan vrienden of vriendinnen te geven. Tenslotte is het niet zeker of dit wachtwoord wordt doorgegeven aan anderen en is het bovendien niet duidelijk bij wie het dan terechtkomt.

Lees de privacypolicy en gebruiksvoorwaarden door.

In de derde plaats wordt in de privacypolicy van Hyves geattendeerd op het feit dat zaken die je op je profiel zet ook publiek worden. Wanneer gebruikers zich registeren, moeten ze aangeven dat ze de gebruiks-voorwaarden en privacypolicy hebben gelezen en dat ze hiermee akkoord gaan. Echter, gebruikers lezen deze documenten nauwelijks. Aanbevolen wordt om toch de privacypolicy en gebruiksvoorwaarden globaal te lezen. Dit kost tijd, maar is wel belangrijk. Als je niet begrijpt wat er staat, vraag het dan aan iemand anders of vraag toestemming.

7.5 Beperkingen van het onderzoek

Hoewel bovenstaande conclusie meer inzicht geeft in hoe jongeren hun privacy beleven binnen een sociale netwerksite, zijn er enkele kritische kanttekeningen te plaatsen. De belangrijkste is het gevaar van mogelijke subjectiviteit van de onderzoeker. De focusgroepgesprekken zijn geleid door een gespreksleider en geanalyseerd door dezelfde persoon. Wel was een tweede persoon (Dustin van Horik Msc) aanwezig bij de groepsgesprekken. De resultaten en conclusie zijn aan deze persoon voorgelegd. Op deze manier is getracht te controleren of de interpretatie juist was. Het onderzoek zou qua betrouwbaarheid hoger scoren, wanneer de analyse door twee onderzoekers onafhankelijk van elkaar zou zijn uitgevoerd en geanalyseerd. Dit was echter niet mogelijk, aangezien budget en tijd hiervoor ontbraken. In de tweede plaats zou op basis van meer focusgroepsgesprekken een meer eenduidig beeld gevormd kunnen zijn en zouden meerdere sociale netwerksites onderzocht kunnen zijn. In plaats van één groepsgesprek per leeftijdsgroep hadden bijvoorbeeld twee groepsgesprekken plaats kunnen vinden. In verband met de tijd, was het niet mogelijk om deze verbreding uit te voeren. Ten derde is getracht met de twee focusgroepen een zo goed mogelijke representatie van de doelgroep van Hyves vorm te geven. Het bleek echter moeilijk te zijn om genoeg respondenten te vinden en een evenwichtige verdeling wat betreft leeftijd, geslacht en opleidingsniveau te realiseren. Toch waren twaalf personen bereid om mee te werken. Ten vierde is het op basis van dit onderzoek niet mogelijk om uitspraken te doen over Hyves-gebruikers in het algemeen. Dit was ook niet de opzet van dit onderzoek. Dit onderzoek is explorerend van aard en biedt daarom veel mogelijkheden voor vervolgonderzoek. Tot slot bleek het moeilijk te zijn om experts te vinden die bereid waren om te praten over Hyves en hoe zij omgaat met de waarborging van privacy. Hyves zelf wilde niet meewerken, waarschijnlijk deels omdat het onderwerp erg actueel is.

7.6 Aanbevelingen voor vervolgonderzoek

Dit onderzoek heeft aangetoond, dat gebruikers van sociale netwerksites in de leeftijd van 13 tot en met 18 jaar en 24 tot en met 31 jaar hun privacy belangrijk vinden, dat de informationele dimensie daarin een grote rol speelt, maar dat ook de twee overige dimensies in de huidige samenleving nog steeds van grote waarde zijn. Verder blijkt dat lang niet alle risico's die in eerdere studies naar voren zijn gekomen, door gebruikers zijn opgemerkt. Toch blijkt dat zij zich wel redelijk bewust zijn van de mogelijke gevaren, hoewel dit van persoon tot persoon flink verschilt.

Hoewel dit onderzoek een aanvulling is op eerdere studies over privacy op sociale netwerksites, omdat hierin het perspectief van de gebruiker wordt meegenomen, is dit niet meer dan een eerste stap waarin de beleving van gebruikers ten aanzien van privacy bloot gelegd wordt. Meer onderzoek is nodig om te achterhalen wat gebruikers belangrijk vinden en welke acties zij precies ondernemen om hun privacy te beschermen. Er blijkt een verschil te zijn in privacybewustzijn tussen de jongere en de oudere groep. Interessant is om hier in vervolgonderzoek op door te gaan en te onderzoeken of leeftijd inderdaad de belangrijkste factor is waardoor privacybewustzijn toe neemt. Hiertoe zou hetzelfde onderzoek over vijf jaar nog een keer uitgevoerd kunnen

worden met dezelfde twee groepen: is het privacybewustzijn en de privacybezorgdheid bij beide groepen toegenomen?

Bovendien wordt aanbevolen om een grootschalige survey uit te zetten onder gebruikers van verschillende sociale netwerksites (ook internationaal) waarin uitkomsten uit dit onderzoek getoetst kunnen worden. Tot slot zou ook een breder en internationaal perspectief als uitgangspunt kunnen dienen voor een onderzoek waarbij niet alleen naar sociale netwerksites wordt gekeken maar naar web 2.0 en web 3.0 diensten/omgevingen in het algemeen. Dit werd ook in één van de focusgroepgesprekken aan de orde gesteld.

Kortom, aanbevolen wordt om een breed perspectief te hanteren, waarin alledrie de dimensies worden meegenomen, bij het doen van vervolgstudies. Wellicht is het interessant om meer focus te leggen op de ruimtelijke en relationele dimensie en daarbij een vergelijking te maken tussen online en offline privacy-beleving.

LITERATUURLIJST

- Alexa. 2008. Hyves.nl. URL: http://www.alexa.com/data/details/traffic_details/Hyves.nl Geraadpleegd op 8-05-2008

- Auteur onbekend. 2007. Web users ignore their own privacy knowledge. Collector 72 (7) pp 19 URL: http://findarticles.com/p/articles/mi_qa5315/is_200702/ai_n21282042. Geraadpleegd op 9-02-2008

- Bertrams, J. 2008. Interview Raymond Spanjar, medeoprichter Hyves - deel 2. Over Myspace en Facebook en de API. URL: http://www.hyped.nl/index.php/details/20080318_interview_raymond_spanjar_medeoprichter_hyves_deel_2. Geraadpleegd op 8-05-2008

- BN – de Stem. 2007. Populaire sociale netwerksites. 8 december 2007 URL: http://www.bndestem.nl/algemeen/binnenland/2287466/Populaire-sociale-netwerksites.ece. Geraadpleegd op 13-05-2008

- Boyd, D. 2007. Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life (electronische versie) *MacArthur Foundation Series on Digital Learning – Youth, Identity, and DigitalMedia Volume* (ed. David Buckingham). Cambridge, MA: MIT Press

- Broek, M. van den. 2007. Cijfers bewijzen: social networking is booming. Marketingfacts. URL: http://www.marketingfacts.nl/berichten/cijfers_bewijzen_social_networking_is_booming/ Geraadpleegd op 14-06-2008

- Broekman, L. 2007. Het verschil tussen een netwerk en een community. Marketingfacts, 8 november 2007. URL: http://www.marketingfacts.nl/berichten/20071108_het_verschil_tussen_een_netwerk_en_een_community/ Geraadpleegd op 13-05-2008

- Bruin, J. de, en Bruin, J.D. de,2001. 'Sociale Virtuele Werelden', Bezien vanuit een sociologisch en beleids- en organisatiewetenschappelijk perspectief, *Kubit* 8 (1) URL: http://drcwww.uvt.nl/its/voorlichting/kubit/k81/k81bru.htm. Geraadpleegd op 27-03-2007

- Buchanan, T., Paine, C., Joinson, A., Reips, U. 2007 Development of measures of online privacy concern and protection for use on the internet. *Journal of the American society for informationscience and technology*, Vol 58, Issue 2, pp. 157-165

- College bescherming persoonsgegevens.2007. *Publicatie van persoonsgegevens op internet. CBP Richtsnoeren*. http://www.cbpweb.nl/downloads_rs/rs_persoonsgegevens_op_internet.pdf. Geraadpleegd op 15-03-2008.

- Dekker, V. 2008. Privacy is een politieke keuze. 18 januari 2008, Trouw

- Derksen, M. 2007. Statistieken voor Myspace, Youtube, Digg en Myspace. Marketingfacts. 21 juni 2007 URL:http://www.marketingfacts.nl/berichten/20070621_statistieken_voor_myspace_youtube_digg_en_facebook/ Geraadpleegd op 18-04-2008

- Digibewust. 2007. Social networking Factsheet. URL: http://www.digibewust.nl/news/item/Tieners_moeten_nog_veel_leren_over_online_privacy/ Geraadpleegd op 8-02-2008

- Dubbeld, L. 2000. Privacy in het tijdperk van informatie, communicatie en technologie. URL: http://www.leidenuniv.nl/philosophy/publicaties/overige/filosofiedag/acta/dubbeld.pdf. Geraadpleegd op 28-03-2008.

- Dwyer, C., Hiltz, S., Passerini, K. 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. Proceedings of the thirteenth Americas conference on information systems, Colorado. 9 december 2007. URL: http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf. Geraadpleegd op 15-03-2008.

- ECP.nl, platform voor eNederland (2007) Identity management

- Ernst & Young .2007. Eyeballs & Communities. Mediabarometer. URL:http://www.krem.nl/Downloads/DEF_14112007_Mediabarometer_Ernst&Young.pdf. Geraadpleegd op 15-05-2008

- Facebook. 2008. Homepage. URL: http://www.facebook.com/ Geraadpleegd op 8-05-2008

- Facebook Factsheet. 2008.URL: http://www.facebook.com/press/info.php?factsheet. Geraadpleegd op 8-05-2008.

- Facebook Statistics .2008.URL: http://www.facebook.com/press/info.php?statistics. Geraadpleegd op 8-05-2008.

- Glaser, B. & Strauss, A. 1967.*The Discovery of Grounded Theory: Strategies for Qualitative Research.* Aldine Transaction. Piscataway, New Jersey

- Gutwirth, S. 1998. *Privacyvrijheid. De vrijheid om zichzelf te zijn*. Rathenau Instituut: Den Haag

- Gross, R. and Acquisti, A. 2005. Information revelation and privacy in online social networks (The Facebook case). Pre-proceedings version. ACM Workshop on privacy in the electronic society (WPES)

- Hogben, G. (Ed.) .2007. Security issues and recommendations for online social networks. ENISA Position Paper No. 1

- Hyves. 2008. Wat is de Buzz?. URL: http://www.hyves.nl/help/contact/. Geraadpleegd op 15-05-2008

- Hyves. 2008. Gebruiksvoorwaarden. URL: http://www.hyves.nl/useragreement/ Geraadpleegd op 25-05-2008

- Hyves. 2008. Privacypolicy. URL: http://www.hyves.nl/privacy/ Geraadpleegd op 25-05-2008

- Joinson, A.N & Paine (Schofield), C. B. 2007. Self-disclosure, privacy and the Internet. Institute of Educational Technology. URL: http://www.york.ac.uk/res/e-society/projects/15/PRISD_report2.pdf Geraadpleegd op 22-02-2008

- Jones, H. & Soltren, J.H. 2005. Facebook: Threats to privacy. 14 december 2005 URL: http://www.scribd.com/doc/2458/Facebook-Threats-to-Privacy. Geraadpleegd op 22-02-2008

- Kohnstamm, J. & Dubbeld, D. 2007. Glazen samenleving in zicht. NJB, Focus, Afl. 2007/37, 19 oktober 2007.College Bescherming Persoonsgegevens. NJB. Geraadpleegd op 28-02-2008 URL: http://www.cbpweb.nl/documenten/art_jko_2007_glazen_samenleving.stm

- Kol, E. 2008. *Hyves.* Kosmos Uitgevers, Utrecht/Antwerpen

- Kool, L. 2007. User generated privacy. TNO

- Koops, B. & Vedder, A. 2004. Opsporing versus privacy: de beleving van burgers, Nationaal Programma Informatietechnologie en Recht

- Lampe, C., N. Ellison, and C. Steinfield. 2007. "A face(book) in the crowd: Social searching versus social browsing." Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work, Banff, Alberta, Canada, 2007, pp. 167-170

- Lenhart, A. & Madden, M. 2007. Teens, Privacy and Online Social Networks. How teens manage their online identities and personal information in the age of Myspace. Pew Internet en American Life Project. URL (voor link naar pdf): http://www.pewinternet.org/ppf/r/211/report_display.asp. Geraadpleegd op 8-02-2008

- Lessig, L. 1998. The architecture of privacy. Essay prepared for Taiwan Net Conference, March 1998. URL: http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf. Geraadpleegd op 3-02-2008 Louis Harris & Associates.

- Marketingfacts. 2008. RSS Dossier. URL: http://www.marketingfacts.nl/dossiers/rss/ Geraadpleegd op 13-05-2008

- NRC Handelsblad. 2006. Maandag: Wij het web. 8 mei 2006. URL: http://www.nrc.nl/media/article308151.ece. Geraadpleegd op 4-03-2008

- Nu.nl. 2007. Internetters bewust bezig met hun identiteit. 28 december 2007 URL: http://www.nu.nl/news/1370586/50/rss/Internetters_bewust_bezig_met_hun_digitale_identiteit.html. Geraadpleegd op 4-03-2008

- O'Neil, D. 2001. *Analysis of internet users' level of online privacy concerns* (electronische versie) Social Science Computer Review: 19;17

- O'Reilly, T. 2005. What is Web 2.0. Design Patterns and Business Models for the next generation of software. 30 september 2005 URL: http://www.oreilly.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html Geraadpleegd op 2-04-2008

- Paine, C., Reips, U., Stieger, S., Joinson, A., Buchanan, T. 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions' (electronische versie) *International journal of human-computer studies*, Vol 65, Issue X, pp. 526-536

- Peters, V. 2001. *Case-study.* In: Huttner, H.Renckstorf, K. & Wester, F. 2001. *Onderzoekstypen in de communicatiewetenschap*. Kluwer, Alphen aan den Rijn.

- Phelps, J. Nowak, G. & Ferrell, E. 2000. *Privacy concerns and consumer willingness to provide personal information*. Journal of public policy and marketing

- Riphagen, D. 2008. Persoonlijke informatie op een online sociaal netwerk: niet zo veilig als het lijkt. URL: http://www.xs4all.nl/opinie/2008/02/27/persoonlijke-informatie-op-een-online-sociaal-netwerk-niet-zo-veilig-als-het-lijkt/

- RTL Nieuws.nl.2008. Joop van den Ende stapt in Hyves. 4 april 2008. URL: http://www.rtl.nl/(/actueel/rtlnieuws/entertainment/articleview/)/components/actueel/rtlnieuws/2008/04_april/04/entertainment/0404_0600_hyves_ende.xml. Geraadpleegd op 13-05-2008

- Selm, M. van, Wester, F. 2006. In: Wester, F. Renckstorf, K. & Scheepers, P. 2006. Onderzoekstypen in de communicatiewetenschap, Kluwer, druk 2

- Smink, G., Hamstra, A. en van Dijk, H. 1999. Privacybeleving van burgers in de Informatiemaatschappij. Rathenau instituut.

- Soest, van T. 2007. Gebruikers Hyves sluiten de gordijnen. 9 oktober 2007, Volkskrant. URL: http://www.volkskrant.nl/binnenland/article467612.ece/Gebruikers_Hyves_sluiten_de_gordijnen. Geraadpleegd op 20-05-2008

- Solove, D. 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477

- Spanjar, R. 2008. Buzz, alle BH'ers verzamelen & zichtbaarheid. URL: http://hyvers.hyves.nl/forum/1798145/gSdS/Buzz_alle_BH_ers_verzamelen_zichtbaarheid/#show_reactions_1=1&hub_threadlist_1=1&searchhyver=&__state__=1 Geraadpleegd op 25-4-2008

- Spits. 27 november 2007. Profielensites breken wet. Hyves en andere sites op de vingers getikt door CPB.
  URL: http://spitsnet.nl/nieuws.php/1/8317/online/profielensites_breken_wet.html?p=home%20links. Geraadpleegd op 26-06-2008

- Starkenburg, A. 2008. Van den Ende & Deitmers stappen in Hyves. Emerce.nl
  URL: http://www.emerce.nl/nieuws.jsp?id=2459689. Geraadpleegd op 13-05-2008

- Stutzman, F. 2006.“Student Life on the Facebook,” URL: http://ibiblio.org/fred/facebook/stutzman_fbook.pdf Geraadpleegd op 4-03-2008

- Tomesen, R. 2007. Hyves noemt groei geen Hype. 12 maart 2007, Emerce
  URL: http://www.emerce.nl/nieuws.jsp?id=1896944, geraadpleegd op 2-07-2008

- Vermeulen, S. 2006. *Hyves kan je zo je carrière kosten*. 25 oktober 2006, NRC Handelsblad, p.18

- Verschoore de la Houssaije, M. 2007. Hyves: privé of publiek? Bachelorthesis. Erasmus Universiteit Rotterdam

- Vos, H. & Van Geel, A. 2007. The Next Web 2007 highligts. RuigrokNetpanel, Amsterdam, mei 2007

- Wester, F. 2006. In: Wester, F. Renckstorf, K. & Scheepers, P. 2006. Onderzoekstypen in de communicatiewetenschap, Kluwer, druk 2

- Wester, F., & Peters, V. 2004. Uitgangspunten voor kwalitatief onderzoek. In: F. Wester & V. Peters. 2004. *Kwalitatieve analyse. Uitgangspunten en procedures*. Bussum: uitgeverij Coutinho

- Weyns, W. 1998. Grensschermutselingen, Een sociologische verkenning van de grens tussen privé en publiek domein. Tijdschrift van de Sociologie: 3: 1

- Woo, J. 2006. The right not to be identified: privacy and anonymity in the interactive media environment. (electronische versie) New Media & Society, Vol 8(6):949–967, Sage, Londen

- Ymerce-Hyves. 2008. 7 maart 2008. Leuke Hyves cijfertjes voor het weekend. Ymerce.nl. URL: http://www.yme.nl/ymerce/2008/03/07/leuke-hyves-cijfertjes-voor-het-weekend/). Geraadpleegd op 13-05-2008

- Ymerce-Social Networking. 16 maart 2008. Social networking diensten in Nederland. URL: http://www.yme.nl/ymerce/category/community/ Geraadpleegd op 13-05-2008

OVERZICHT TABELLEN EN FIGUREN

Tabellen

Figuren

Afbeeldingen

BIJLAGE 1: TOPICLIJST FOCUSGROEP 24- TOT EN MET 31-JARIGEN

Controleren opname-apparatuur

Verwelkomen participanten + koffie en thee

Voorstellen van jezelf

Uitleg doel en duur van focus-group

Garanderen van discretie/anonimiteit

Uitdelen van een pen, papier post-its en een rood en groen papiertje. De stellingen worden later uitgedeeld.

IJsbreker: Kunnen jullie jezelf even voorstellen en daarbij vermelden wanneer je voor het laatst op Hyves bent ingelogd en wat je toen precies gedaan hebt?

Topic 1: Hyves

Wat vinden jullie van Hyves?

Wat doen jullie op Hyves?

Topic 2: Privacy

Aan welke woorden denken jullie wanneer het woord privacy ter sprake komt?

- (iedere respondent schrijft drie woorden op en plakt dit op)
- →daarna discussie
- →resultaat is een definitie

Waar hechten jullie waarde aan als we het hebben over privacy?

- (Iedere respondent schrijft minimaal drie waarden of criteria op en plakt dit op)
- →daarna discussie
- →resultaat is een lijst met belangrijkste waarden

Topic 3: Privacy-risico's

Wanneer wordt de privacy geschonden? Kunnen jullie hier voorbeelden van geven?

(Let op: Waar mogelijk doorvragen door in te spelen op voorbeelden en hier nuances in aan te brengen)

Lukt dit niet dan onderstaande voorbeelden geven:

1. Een vriend of vriendin zet een 'extreme' foto van jou in zijn of haar fotoalbum
2. Ook als een persoon niet lid is, is het mogelijk om de foto van iemand te zien en wanneer deze persoon zijn of haar profiel niet heeft afgeschermd is ook deze door niet leden te bewonderen
3. Iemand anders zet persoonlijke informatie over jou in zijn of haar blog.
4. Iemand anders maakt een profiel aan onder jouw naam.

5. Gegevens worden verzameld voor marketingdoeleinden.
6. Er wordt een digitaal dossier bijgehouden over welke informatie jij beschikbaar maakt.

- Is dit anders op internet (schending van de privacy) dan in real life? Hoe ervaren jullie dat?
- En binnen sociale netwerken zoals Hyves?

Hebben jullie zelf wel eens iets vervelends meegemaakt op Hyves of door Hyves?

- Welke risico's zijn er volgens jullie voor je privacy in een sociale netwerksite zoals Hyves?
- Maken jullie je hier zorgen om? Waarom wel/waarom niet?

PAUZE

Topic 4: Privacy waarborging

Stellingen:

(deze worden uitgedeeld)

Over 20 jaar bestaat er geen privacy meer.

Door internet is het begrip privacy aan het veranderen.

Hyves neemt het niet zo nauw met privacy.

- Wat zou Hyves nog moeten doen dan? Welke mogelijkheden zouden jullie willen hebben om eventueel privacy beter te kunnen beschermen?

Gebruikers hebben het zelf in de hand in welke mate zij hun privacy opgeven dan wel beschermen.

Hyves heeft een goede keuze gemaakt. Als jij je profiel afschermt, mag je ook niet meer bij anderen gluren.

- →wordt gestemd (d.m.v. rode en groene briefjes) stemmen worden geteld.
- → discussie

Stel je bent aan het solliciteren. Wat zou je toekomstige werkgever allemaal te weten kunnen komen over jou?

Hoe vinden jullie dat Hyves omgaat met jullie privacywaarborging?

- Bijvoorbeeld wat in de privacy policy staat?
- Zijn jullie op de hoogte van de gebruiksvoorwaarden en de privacy policy?
- Schermen jullie bepaalde gegevens af voor anderen en waarom?
- Hoe komt het dat gebruikers hier soms niet op letten?

Afsluiting:

Alle topics behandeld?

Nog vragen en opmerkingen?

Dankje wel!

BIJLAGE 2: TOPICLIJST FOCUSGROEP 13-TOT EN MET 18-JARIGEN

Controleren opname-apparatuur

Verwelkomen participanten + koffie en thee

Voorstellen van jezelf

Uitleg doel en duur van focus-group

Garanderen van discretie/anonimiteit

Uitdelen van een pen, papier post-its en een rood en groen papiertje. De stellingen worden later uitgedeeld.

IJsbreker: Kunnen jullie jezelf even voorstellen en daarbij vermelden wanneer je voor het laatst op Hyves bent ingelogd en wat je toen precies gedaan hebt?

Topic 1: Hyves

Wat vinden jullie van Hyves?

Wat doen jullie op Hyves?

Topic 2: Privacy

Aan welke woorden denken jullie bij het woord privacy?

- (iedere respondent schrijft drie woorden op en plakt dit op)
- →daarna discussie
- →resultaat is een definitie

Wat vind je belangrijk aan privacy? Waar moet het voor zorgen?

- Iedere respondent schrijft minimaal drie waarden of criteria op en plakt dit op)
- →daarna discussie
- →resultaat is een lijst met belangrijkste waarden

Topic 3: Privacy-risico's

Hebben jullie zelf wel eens iets vervelends meegemaakt op Hyves of door Hyves?

Wanneer wordt de privacy geschonden? Kunnen jullie hier voorbeelden van geven?

(Let op: Waar mogelijk doorvragen door in te spelen op voorbeelden en hier nuances in aan te brengen)

Lukt dit niet dan onderstaande voorbeelden geven:

1. Een vriend of vriendin zet een 'extreme' foto van jou in zijn of haar fotoalbum
2. Ook als een persoon niet lid is, is het mogelijk om de foto van iemand te zien en wanneer deze persoon zijn of haar profiel niet heeft afgeschermd is ook deze door niet leden te bewonderen
3. Iemand anders zet persoonlijke informatie over jou in zijn of haar blog.

4. Iemand anders maakt een profiel aan onder jouw naam.
5. Gegevens worden verzameld voor marketingdoeleinden.
6. Er wordt een digitaal dossier bijgehouden over welke informatie jij beschikbaar maakt.

- Is dit anders op internet (schending van de privacy) dan in real life? Hoe ervaren jullie dat?
- En binnen sociale netwerken zoals Hyves?
- Welke risico's zijn er volgens jullie voor je privacy in een sociale netwerksite zoals Hyves?
- Maken jullie je hier zorgen om? Waarom wel/waarom niet?

PAUZE

Topic 4: Privacy waarborging

Stellingen:

(deze worden uitgedeeld)

Over 20 jaar bestaat er geen privacy meer.

Door internet is het begrip privacy aan het veranderen.

Hyves neemt het niet zo nauw met privacy. (Hyves biedt niet genoeg mogelijkheden voor gebruikers om hun privacy te beschermen.)

- Wat zou Hyves nog moeten doen dan? Welke mogelijkheden zouden jullie willen hebben om eventueel privacy beter te kunnen beschermen?

Het is aan de gebruiker om te bepalen of zij hun privacy opgeven of beschermen.

Hyves heeft een goede keuze gemaakt. Als jij je profiel afschermt, mag je ook niet meer bij anderen gluren.

- →wordt gestemd (d.m.v. rode en groene briefjes) stemmen worden geteld.
- → discussie

Stel je bent aan het solliciteren. Wat zou je toekomstige werkgever allemaal te weten kunnen komen over jou?

Hoe vinden jullie dat Hyves omgaat met jullie privacywaarborging?

- Bijvoorbeeld wat in de privacy policy staat?
- Zijn jullie op de hoogte van de gebruiksvoorwaarden en de privacy policy?
- Schermen jullie bepaalde gegevens af voor anderen en waarom?
- Hoe komt het dat gebruikers hier soms niet op letten?

Afsluiting:

Alle topics behandeld?

Nog vragen en opmerkingen?

Dankje wel!

BIJLAGE 3: TOPICLIJST INTERVIEW

Controleren opname-apparatuur

Verwelkomen geinterviewde

Voorstellen van jezelf

Uitleg doel en duur van interview

Garanderen van discretie

IJsbreker: Joop van den Ende en Hyves? Gaan gebruikers de gevolgen hiervan zien?

Topic 1: Hyves algemeen

Waar heeft Hyves zijn succes aan te danken?

Topic 2: Privacy en de gebruiker

Wat vinden gebruikers volgens jou belangrijk als het gaat om privacy?

Houden ze zich hiermee bezig en hoe doen ze dat dan?

Kun je hier voorbeelden van geven?

Is dit volgens jou anders op het internet dan in real life?

Topic 3: Privacy-risico's en waarborging

Welke risico's zijn er volgens jou voor de privacy van gebruikers in sociale netwerksites (Hyves?

Hoe gaat Hyves hiermee om?

Moet Hyves de privacy van gebruikers waarborgen? Hoe sta je hier tegenover?In hoeverre is dit aan de gebruiker zelf?

Hoe komt het dat gebruikers hier soms niet op letten?

Topic 4: Toekomst van Hyves

Hyves is constant bezig met het vernieuwingen van de site en de tools die zij biedt. Heeft dit eventuele gevolgen voor de privacy? En zo ja waarom dan?

Wat kunnen we de rest van dit jaar nog verwachten van Hyves?

Hoe ziet de toekomst eruit voor Hyves?

Afsluiting:

Alle topics behandeld?

Nog vragen en opmerkingen?

Dankje wel!

BIJLAGE 4: WAARDEN EN CRITERIA (SMINK ET AL.1999)

Hieronder zijn per waarde de genoemde meest relevante criteria weergegeven.

Zelfstandigheid
- doel van gegevensverzameling;
- zelf kunnen bepalen wie wat van je weet;
- relevantie van gegevens;
- wat doen ze met gegevens;
- uitwisselen en koppelen van gegevens;
- keuzemogelijkheid, mogelijkheid om te weigeren;
- controleerbaarheid, wie weet wat over mij;
- wie heeft inzage in gegevens;
- doel uitwisseling gegevens;
- mogelijkheid om je af te schermen;
- type doel van gegevensverzameling;
- toestemming geven voor doorgeven van gegevens;
- inzage in wat met gegevens gebeurt;
- vertrouwen;
- zorgvuldig omgaan met gegevens;
- toestemming geven.

Bewegingsvrijheid
- wie heeft inzage in gegevens;
- koppelen van gegevens;
- doel van gegevensverzameling;
- type doel van gegevensverzameling;
- zelf kunnen bepalen wie wat te weten komt;
- ongevraagd confronteren met gebruik van gegevens;
- toestemming geven voor doorgeven gegevens;
- manier van gegevensverzameling (persoonlijk).

Ongestoord leven
- mogelijkheid om je af te schermen;
- keuzevrijheid.

Stigmatisering
- relevantie van gegevens;
- interpretatie;
- hoeveelheid verzamelde gegevens;
- hoe zijn ze aan mijn gegevens gekomen?
- zelf kunnen bepalen wie wat te weten komt;
- wie heeft inzage in gegevens;
- hoeveel mensen hebben inzage in gegevens;
- wat wordt met de gegevens gedaan;
- toestemming geven;
- mogelijkheid om gegevens te corrigeren;
- traceerbaarheid van gegevens naar persoon;
- type doel van gegevensverzameling
- bewaartermijn gegevens

Manipulatie
• mogelijkheid om je af te schermen (bijvoorbeeld reclame);
• zelf kunnen bepalen wie wat te weten komt;
• wie heeft inzage in gegevens;
• wat gebeurt er met de gegevens;
• hoeveelheid verzamelde gegevens;
• toestemming geven;
• keuzevrijheid.

Eigenwaarde
• vertrouwen;
• wie heeft inzage in gegevens;
• uitwisselen van gegevens;
• hoeveelheid verzamelde gegevens;
• zelf kunnen bepalen wie wat te weten komt;
• toestemming vragen;
• wie verzamelt de gegevens;
• wat gebeurt er met de gegevens;
• doelbinding van gegevens.

Gelijkheid
• relevantie van gegevens;
• wat doen ze met gegevens?
• doel van gegevensverzameling;
• wie moet gegevens verstrekken.

Integriteit
• uitwisselen en koppelen van gegevens;
• zorgvuldige behandeling van gegevens;
• zelf kunnen bepalen wie wat te weten komt;
• wat gebeurt er met gegevens?
• toestemming vragen;
• vertrouwen;
• keuzevrijheid.

Autonomie
• mogelijkheid om je af te schermen;
• controleerbaarheid, wie weet wat over mij;
• uitwisseling van gegevens;
• zelf kunnen bepalen wie wat te weten komt.