

Sociale netwerken en privacy

184

Trefwoorden:

internet, sociale netwerken, identiteit

Sociale netwerksites belichamen de ‘menselijke’ kant van de Web 2.0-revolutie. Zij kunnen zich de laatste tijd verheugen in verhoogde aandacht voor de privacyaspecten van hun dienstverlening. Deze bijdrage geeft een met voorbeelden geardeerd overzicht van die privacyaspecten. Twee hoofdtypen worden onderscheiden: gestolen en gefingeerde identiteiten, en verder gebruik van gegevens op sociale netwerksites. Kinderen en tieners vormen een bijzondere risicogroep.

Gestolen en gefingeerde identiteiten kunnen gebruikt worden om het slachtoffer op te lichten, te pesten of in een kwaad daglicht te stellen. Verder gebruik kan plaatsvinden door de sociale netwerksite en zijn partners, of door personen met wie de gebruiker een relatie heeft of wil aangaan, zoals een werkgever. Ook afgeschermd gegevens blijken niet immuun voor verder gebruik. Betoogd wordt dat de gebruikelijke maatregelen de privacyproblematiek slechts ten dele kunnen oplossen. De reden daarvoor is dat het delen van persoonlijke informatie de essentie vormt van sociale netwerken. Geavanceerd identiteitsbeheer vormt de sleutel tot werkelijk effectieve privacybescherming in de context van sociale netwerksites.

1 Inleiding

Met een briljante *viral marketing*-actie wist het Ministerie van Justitie deze zomer zijn nieuwe campagne voor veilig internetgebruik² op de kaart te zetten. ‘Je bent bekender dan je denkt!’, zo lazen leden van Nederlands populairste sociale netwerksite Hyves³ in een bericht van een mede-hyver. Het bijgevoegde filmpje⁴ toont een groep Oost-Europese criminelen, opgewonden omdat ze op het web een onbeschermd profiel hebben gevonden en dus een kans ruiken. Wat de hyver vervolgens ervaart, beschrijft Marketing Facts als volgt⁵: ‘Stanislav en zijn vriendjes blijken op zoek te zijn naar iemand uit jouw woonplaats met precies het aantal vrienden dat jij hebt en even later rollen er in het filmpje jouw foto’s uit de printer, staat jouw foto op het scherm en staat jouw naam op het bord geschreven. Je blijft kijken en langzaam aan wordt duidelijk dat het écht om jou gaat! Aan het einde van het filmpje komt tot slot de aap uit de mouw en blijkt het

Ministerie van Justitie er achter te zitten. Vervolgens wordt de mogelijkheid geboden het filmpje door te sturen naar je Hyves-vriendjes.’

Van de mogelijkheid om het filmpje door te sturen werd massaal gebruik gemaakt. Koud een week later werd cybercrimineel Stanislav door Justitie alweer op non-actief gesteld, omdat zijn werk erop zat. In die periode hadden zeker drie miljoen mensen hem aan het werk gezien.⁶ De verklaring voor dit fenomenale succes moet gezocht worden in de manier waarop persoonlijke gegevens, inclusief foto’s, in het filmpje werden gewoven. Dat gebeurde technisch vlekkeloos, en werkte daardoor zeer overtuigend. Je had als hyver echt het idee dat er een film over jou gemaakt was. Daarmee kwamen de privacyrisico’s voor velen ineens toch wel heel dichtbij.

In dit artikel – geen juridische of wetenschappelijke analyse⁷, maar een met voorbeelden geardeerde *tour d’horizon* – schets ik de stand van zaken op het gebied van sociale netwerken en privacy. Ik begin in de volgende paragraaf met een inleiding tot Web 2.0 en sociale netwerksites. Vervolgens ga ik in op de privacyaspecten van zulke sites. Daarna komen enkele belangrijke juridische ontwikkelingen aan de orde. Ik sluit af met een conclusie.

2 Sociale netwerken

‘Markets are conversations’. Met die centrale these verkondigde het befaamde *Cluetrain Manifesto*⁸ tien jaar geleden aan het bedrijfsleven dat zijn manier van zaken doen door de opkomst van het web fundamenteel en voorgoed zou veranderen. De Cluetrain-auteurs hebben zeker niet in alle opzichten gelijk gekregen. Het manifest kan echter wel gezien worden als een markeringspunt voor het begin van een revolutie die wordt aangeduid met termen als *Web 2.0* en *cloud computing*. Die omwenteling is nog in volle gang. Over de precieze betekenis van deze begrippen en de ontwikkelingen waar zij voor staan bestaat vooralsnog dan ook geen consensus. Centraal staan echter telkens de overweldigende interactiemogelijkheden die internet tegenwoordig biedt. Cloud computing verwijst vooral naar de *technische* en *bedrijfsmatige* aspecten daarvan: het aanbieden van gebruik van infrastructuur, ontwikkelplatforms en programmatuur – en steeds vaker ook kant-en-klare onderdelen van bedrijfsprocessen – als via internet te betrekken dienstverlening. De term Web 2.0 wordt daarentegen vooral gebruikt voor de menselijke kant van het verhaal: het ondersteunen van het

1 Koen Versmissen is redacteur van P&I en eigenaar van IDwise. IDwise doet onderzoek en geeft strategisch advies op het gebied van identiteit en privacy, met name op internet.

2 Zie <www.veiliginternetten.nl>.

3 Zie <www.hyves.nl>.

4 Zie <www.Nis5.nl> | campagnes | rijksoverheid: koepelthema veiligheid | Cybercrime | bekijk, en klik op ‘>’.

5 Zie <www.marketingfacts.nl/berichten/20090813_zo_maak_je_campagne_op_hyves>.

6 Zie <www.justitie.nl/actueel/persberichten/archief-2009/90819werk-van-stanislav-zit-er-op.aspx>.

7 Zie daarvoor bijvoorbeeld: James Grimmelmann, ‘Saving Facebook’, *Iowa Law Review* 94 (2009): 1137-1206. Beschikbaar via <http://works.bepress.com/james_grimmelmann/20>.

8 Christopher Locke, Rick Levine, Doc Searls & David Weinberger, *Cluetrain Manifesto: The End of Business as Usual*, Basic Books, 2001. Zie <www.cluetrain.com/book/index.html>.

aangaan en onderhouden van relaties en samenwerking in de breedst mogelijke zin. Sociale netwerksites vormen daarvan de meest prominente belichaming.

Het is zinvol om een onderscheid te maken tussen sociale netwerksites en sociale mediasites. De onderstaande definities komen (enigszins aangepast) uit een rapport⁹ van het *Online Computer Library Center*:

Sociale netwerksites: Websites die primair ontworpen zijn om interactie te faciliteren tussen gebruikers met gedeelde interesses, opinies en activiteiten. Voorbeelden zijn Facebook, Hyves en MySpace.

Sociale mediasites: Websites die gebruikers in staat stellen om inhoud die zij hebben gemaakt te delen met anderen. Voorbeelden zijn YouTube (delen van video's), Flickr (delen van foto's) en SlideShare (delen van PowerPoint-presentaties). Waar er op sociale netwerksites interactie plaatsvindt, is het primaire doel van sociale mediasites het publiceren en delen van inhoud.

In dit artikel richt ik me vooral op sociale netwerksites. De privacyvraagstukken zijn daar het meest uitgebreid en ingrijpend.

Sociale netwerksites zijn er in allerlei soorten en maten. De grootste zijn te vinden onder de algemene sociale netwerken gericht op de privé sfeer. In de vorige paragraaf kwamen Facebook, Hyves, en MySpace al langs; andere voorbeelden zijn Bebo, Friendster, Hi5, Mixi, Ning, Orkut en Windows Live Spaces, terwijl ook Yahoo! zich steeds meer tot een sociale netwerksite ontwikkelt. Andere algemene sites richten zich op de professionele sfeer; de bekendste daarvan zijn LinkedIn, Ning en Plaxo. De laatste jaren schieten ook meer gespecialiseerde sites als paddenstoelen uit de grond. Soms richten die zich op een bepaald publiek, zoals reizigers (CouchSurfing), kinderen/tieners (Habbo, Sugababes, SuperDudes) of collega's binnen een bedrijf (Yammer). In andere gevallen is sprake van een specifiek soort netwerkactiviteit, zoals *realtime* verslag doen van je wederwaardigheden (Twitter) of het delen van links naar interessante webpagina's (del.icio.us, Digg, StumbleUpon). Te verwachten valt dat deze specialisatietrend sterk zal doorzetten, mede onder invloed van platforms als Google Open Social die het eenvoudig maken om applicaties te bouwen die met verschillende sociale netwerksites kunnen omgaan.

3 Privacy

3.1 *Let op je woorden*

Gebruikers van sociale netwerksites kunnen verbluffend naïef zijn over hoe anderen omgaan met de gegevens die zij op die sites zetten. Een treffend voorbeeld vormt de Amerikaanse studente Stacey Snyder. Deze lerares in opleiding van Millersville University verwierf in 2006 een zekere faam toen zij claimde dat haar een diploma zou zijn geweigerd vanwege

een vrij onschuldige foto op haar MySpace-pagina. Zij spande later een rechtszaak aan, waarin zij eind vorig jaar in het ongelijk werd gesteld.¹⁰ Die uitspraak was vooral gebaseerd op het feit dat de universiteit aannemelijk kon maken dat er ook los van de publicatie van de gewraakte foto voldoende redenen waren om Snyder geen diploma toe te kennen. Interessanter dan de uitspraak op zich zijn dan ook fragmenten uit de verklaringen die Snyder in het kader van de rechtszaak aflegde. Onderwerp is het feit dat een van de leerlingen uit haar stageklas haar MySpace-pagina heeft bekeken. Ik citeer (in vertaling): 'Klaagster verklaarde dat het "ongepast" was voor een leerling om de MySpace-pagina van een docente te bekijken aangezien "er een grens bestaat en er op die pagina persoonlijke informatie staat waarvan een leerling zou moeten beseffen dat hij die als leerling niet moest bekijken." Klaagster legde uit dat de leerling weliswaar best de webpagina van een bekende mocht bekijken, maar dat het onfatsoenlijk was om die van klaagster te bekijken aangezien klaagster "een persoon van hogere positie [*of higher standard*]" was.' Let wel: het gaat hier om informatie die door Snyder bewust in een openbaar profiel was geplaatst!

Hoeveel gebruikers van sociale netwerken vertrouwen er net als Snyder op dat mensen die daar 'niets mee te maken hebben' de ogen zullen sluiten voor de informatie die ze daarop zetten? Hoeveel gebruikers gaan ervan uit dat die informatie zulke mensen nooit zal bereiken? En hoevelen zijn zich überhaupt niet van enig risico bewust? Hoe het antwoord op die vragen ook precies mag luiden, feit is dat het op internet inmiddels bijvoorbeeld wemelt van verhalen over werknemers die als gevolg van indiscrete opmerkingen over hun bedrijf te horen kregen dat ze hun biezen konden pakken.¹¹ Zo ontsloeg luchtvaartmaatschappij Virgin Atlantic eind vorig jaar op staande voet dertien werknemers die op een sociale netwerksite passagiers 'proleten' (*chavs*) hadden genoemd.¹² Profvoetballer Ashley-Paul Robinson van het Engelse Crystal Palace mocht naar een andere club gaan omzien nadat hij op zijn blog had gemeld dat hij graag weg wilde en een proefwedstrijd bij een andere club had gespeeld.¹³ Een medewerkster van GGZ-instelling Talant in Heerenveen werd geschorst nadat zij op Hyves haar werk met verstandelijk gehandicapten vergeleek met dat van een verzorger in een dierentuin.¹⁴ Een medewerker van een Amsterdamse horecagelegenheid, tot slot, werd verdacht van fraude met een bezoeker. Hij ontkende die bezoeker te kennen en kreeg zijn congé toen uit zijn Hyves-pagina bleek dat beide mannen wel degelijk bevriend waren. Dat ontslag hield stand bij de rechter, ook al was het alleen gebaseerd op 's mans leugens in het onderzoek, en niet op bewezen frauduleus handelen.

Er is overigens zeker niet alleen anekdotisch bewijs dat we hier met omvangrijke problematiek te maken hebben. Zo deed e-mailbeveiliging Proofpoint recentelijk onderzoek bij

9 Sharing, Privacy and Trust in Our Networked World, OCLC, Dublin (Ohio), 2007. Zie <www.oclc.org/reports/sharing>.

10 Zie <<http://voices.washingtonpost.com/securityfix/Decision%202008.12.03.pdf>>.

11 Zie bijvoorbeeld <<http://copsincyberspace.wordpress.com/2009/05/04/ontslag-na-activiteit-op-facebook>>.

12 Zie <www.independent.co.uk/news/uk/home-news/virgin-atlantic-sacks-13-staff-for-calling-its-flyers-chavs-982192.html>.

13 Zie <www.vi.nl/web/show/id=309929/contentid=153289>.

14 Zie <www.zibb.nl/10215261/Nieuws/Nieuwsbericht/Werknemer-geschorst-na-kritiek-op-Hyves.htm>.

Amerikaanse bedrijven met meer dan 1000 werknemers. Daarvan rapporteerde over het afgelopen jaar 17% (tegen 12% in 2008) incidenten met het publiceren van bedrijfsgeheimen of het bedrijf onwelgevallige informatie op sociale netwerksites; bij 8% (tegen 4% vorig jaar) waren zulke incidenten reden tot ontslag van de betrokken werknemers. Met andere woorden: bij één op de twaalf grote Amerikaanse bedrijven is het afgelopen jaar iemand ontslagen vanwege uitingen op een sociale netwerksite.

Hierboven heb ik één privacyaspect van sociale netwerken uitgelicht. De problematiek is echter veel breder, en nauw verweven met het onderwerp identiteit. Dat heeft alles te maken met het privacydilemma dat karakteristiek is voor sociale netwerken: het bekend maken van persoonlijke informatie speelt een essentiële rol bij het opbouwen van vertrouwen en relaties. De gebruiker kan zich weliswaar goed bewust zijn van de risico's van het delen van persoonlijke informatie, maar moet die risico's voortdurend afwegen tegen de voordelen ervan. Deelidentiteiten, pseudoniemen en afscherming van zoekmachines zijn oplossingen die kunnen helpen om de balans te behouden. Voordat ik daar kort op inga, breng ik hieronder eerst de belangrijkste privacyaspecten van sociale netwerken in kaart.

3.2 Gestolen en gefingeerde identiteiten

Het eerste belangrijke type privacyrisico's van sociale netwerken wordt gevormd door het stelen of fingen van identiteiten. Worden die identiteiten vervolgens gebruikt om fraude te plegen, dan spreken we van identiteitsfraude. Bij die term denken we al snel aan criminelen die met methoden als *phishing* en *skimming* achter onze wachtwoorden en pincodes proberen te komen. Maar ook zonder zulke geheime informatie kan een kwaadwillende langzaam maar zeker steeds meer controle over de identiteit van een ander verkrijgen. Op basis van een combinatie van persoonlijke gegevens, zoals NAW-gegevens, geboortedatum en bankrekeningnummer zijn bij veel bedrijven en instellingen gegevens over iemand te verkrijgen door je als die persoon zelf voor te doen. Met de zo verkregen aanvullende gegevens is het weer extra gemakkelijk om de valse identiteit aan te nemen. Sociale netwerken bieden een schat aan zulke informatie, en vormen daarmee een rijke bron voor cybercriminelen als Stanislav. Die kunnen een 'gekaapte' identiteit gebruiken om het slachtoffer op te lichten, maar bijvoorbeeld ook om diens relaties op hun beurt persoonlijke gegevens te ontfutselen. En dat laatste is maar één van de technieken waarover zij beschikken om zich binnen sociale netwerken ook toegang te verschaffen tot geheel of gedeeltelijk afgeschermd informatie. Het ergste voor slachtoffers van identiteitsfraude is dat zij dubbel gepakt worden, aangezien zij zich ook nog eens grote moeite moeten getroosten om de onjuiste informatie die als gevolg van de fraude overal over hen geregistreerd staat gecorrigeerd te kunnen krijgen. Uit de schrijnende ervaringen van Ron Kow-

solea¹⁵ blijkt bovendien dat zij daarbij niet op veel begrip, laat staan steun, van de overheid hoeven te rekenen.

Ook het stelen of fingen van identiteiten zonder fraudeoogmerk komt veel voor in sociale netwerken. Het doel is dan bijvoorbeeld om het slachtoffer te pesten of in een kwaad daglicht te stellen. Dit soort identiteitsdiefstal is in de meeste sociale netwerken een fluitje van een cent bij gebrek aan controle van de identiteit van nieuwe gebruikers. Voor het opzetten van een account zijn meestal alleen een e-mailadres en zelfgekozen wachtwoord nodig. Of de gegevens die de gebruiker vervolgens in zijn profiel opneemt ook inderdaad de gebruiker betreffen, wordt door sociale netwerksites zelden gecontroleerd. Een vrij onschuldig voorbeeld van dit soort identiteitsmisbruik betreft de nep-Wouter Bos die in maart van dit jaar een Twitter-conversatie opzette met Maxime Verhagen.¹⁶ Maar aan de andere kant van het spectrum is er het verhaal van de 13-jarige Megan Meier.¹⁷ Anderhalve maand deelde zij lief en leed met haar MySpace-vriendje Josh. Die liet haar echter van de ene op de andere dag zitten, en stuurde haar een zeer kwetsend bericht ('You are a bad person and everybody hates you. Have a shitty rest of your life. The world would be a better place without you.') Nog geen half uur later pleegde Megan zelfmoord. Al snel na haar tragische daad kwam aan het licht dat Josh helemaal niet bestond. De moeder van een ex-vriendin – over wie zij roddels zou hebben verspreid – had het account aangemaakt om informatie over Megan te verzamelen waarmee zij haar vervolgens belachelijk zou kunnen maken.

Een bijzondere vorm van identiteitsdiefstal vormt ten slotte nog het 'kapen' van gebruikersnamen of andere pseudoniemen die personen gebruiken om over verschillende sociale netwerken heen een online reputatie op te bouwen.

3.3 Verder gebruik

Het tweede belangrijke type privacyrisico's van sociale netwerken bestaat uit onbedoeld en ongewenst verder gebruik van de gegevens die daarop te vinden zijn. Die hoeven overigens niet altijd door de gebruiker zelf op het netwerk te zijn geplaatst. Ook familieleden of netwerkvrienden kunnen informatie over iemand openbaar maken. Sommige sites bieden contacten van een gebruiker de mogelijkheid om openbare berichten op diens pagina te plaatsen (op Hyves heten die 'krabbels'). Omgekeerd kunnen de personen uit het netwerk van de gebruiker op de site, die relatief uitgebreide toegang hebben tot zijn persoonlijke gegevens, van die informatie gebruik maken op een manier die de gebruiker onwenselijk vindt.

Eén vorm van verder gebruik kwam al in paragraaf 3.1 aan de orde: werkgevers die in de gaten houden wat hun werknemers allemaal online openbaar maken, om te zien of die geen bedrijfsgeheimen openbaar maken, of het bedrijf in diskrediet brengen door bijvoorbeeld de klanten belachelijk te maken. Tot op zekere hoogte en onder voorwaarden is dat een verdedigbare praktijk. Dat wordt echter al anders als

15 Zie <www.ad.nl/binnenland/3076312/Onschuldig_maar_bekend_als_zware_crimineel.html>.

16 Zie <www.hyped.nl/details/20090325_nep_wouter_bos_op_twitter_rvd_boos>.

17 Zie <http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier>.

iemand wordt ontslagen doordat zijn baas toevallig niet-openbare informatie onder ogen krijgt die het bedrijf onwettig is.¹⁸ En wat let een bedrijf dat van een werknemer af wil om een van de wat minder chique handelsinformatiebureaus eens te vragen of dat op afgeschermd plekken geen al te kritische informatie kan vinden? Onrechtmatig verkregen bewijs, natuurlijk, maar niet zelden toch voldoende reden voor ontslag, ook volgens de rechter.

Een andere vorm van verder gebruik is het gebruik door de sociale netwerksite zelf, zijn partners of derden aan wie de gegevens van gebruikers worden doorverkocht. Het zal dan vaak juist gaan om door de gebruiker niet voor iedereen toegankelijk gemaakte gegevens. In veel gevallen worden de persoonlijke gegevens gebruikt om de gebruiker reclame op maat toe te kunnen zenden. Volgens een recent artikel in Wired is dit in de langetermijnstrategie van Facebook zelfs de belangrijkste bron van inkomsten.¹⁹ In februari van dit jaar wijzigde die sociale netwerksite zijn algemene voorwaarden zonder zijn gebruikers daarover te informeren. Voortaan zou het automatisch een onbepert en oneindig gebruiksrecht krijgen op alle door gebruikers gepubliceerde informatie. Na een storm van kritiek moest Facebook inbinden, maar na een stemming onder de gebruikers is alsnog een afgezwakte versie van de gewraakte voorwaarden van kracht geworden. Meestal worden gegevens opzettelijk aan derden verstrekt, maar soms ook uit onachtzaamheid of onwetendheid. Zo kwam de Stanislav-campagne van Justitie kortstondig in opspraak toen bleek dat er, in strijd met het privacybeleid van Hyves, afgeschermd gegevens verstrekt werden aan het reclamebureau.

Eveneens een populaire vorm van verder gebruik is het vergaren van openbare informatie die op sociale netwerksites te vinden is met als doel een beeld of indruk te krijgen van iemand. Het googelen van sollicitanten is natuurlijk al een wijd verbreid gebruik, maar steeds vaker bekijken werkgevers ook de sociale netwerkprofielen van aspirant-werknemers. En dit gebeurt niet alleen door potentiële werkgevers, maar bijvoorbeeld ook door onderwijsinstellingen met hun aspirant-studenten²⁰ en door verenigingen met hun aspirant-leden. Ook criminelen maken natuurlijk dankbaar gebruik van gegevens die mensen op sociale netwerken plaatsen.²¹ Wie zich daarvan bewust is, zal zich wel twee keer bedenken voordat hij op een openbare pagina meldt dat hij een maand met vakantie gaat of dat de nieuwe Porsche vandaag geleverd wordt.

Twee laatste voorbeelden dienen ter illustratie van het feit dat zelfs het goed afschermen van informatie op een goed beveiligde sociale netwerksite niet alle problemen kan voorkomen. Een Amerikaanse ziektekostenverzekeraar weigert een declaratie te betalen en wil Facebook- en MySpace-pagina's van de verzekerde – ook de niet-openbare – gebruiken als bewijs dat diens eetstoornissen 'emotionele oorzaken' zou kunnen hebben.²² En Marie-José Klaver beschrijft op haar

weblog²³ wat een cheerleader uit Mississippi overkwam: 'Een coach van een cheerleading team in Mississippi eiste alle loginnamen en wachtwoorden van de Facebook-accounts van de leden. Hij wilde weten of de meisjes zich met seks en drugs bezig hielden en eventueel de goede naam van de school in gevaar brachten. Wie de coach geen toegang gaf werd uit het team gezet. Alle meisjes gaven de coach zijn zin en wisten vervolgens hun accounts via hun mobiele telefoon, op één na. De online activiteiten van de toen 14-jarige cheerleader Mandi Jackson werden door de coach gevolgd en offline verspreid. De coach deelde de inhoud van Mandi's profiel met andere leraren, coaches, de directie van de school en een sponsor. Mandi werd uit het team gezet vanwege haar internetgedrag. Ze mocht ook niet meer meedoen aan andere schoolactiviteiten. Haar misdaad: privéboodschappen uitwisselen met een andere cheerleader waarin schuttingwoorden voorkwamen.'

Bij veel gevallen van verder gebruik bestaat er een serieus risico dat niet alle gegevens over de gebruiker juist zijn. De gebruiker kan daardoor bijvoorbeeld imagoschade oplopen of het slachtoffer worden van onterechte beslissingen. Voor onjuiste beeldvorming zijn twee hoofdoorzaken aan te wijzen. Allereerst kunnen identiteiten met elkaar verward worden, waardoor ten onrechte bepaalde gegevens of uitspraken aan een persoon worden toegeschreven. In gevallen die goed uitgezocht worden is dit risico niet zo groot, maar bij het snel screenen van een groot aantal sollicitanten is een foutje gauw gemaakt. Een andere oorzaak van onjuiste beeldvorming is het gevolg van het per definitie als waar aannemen van informatie die op sociale netwerkpagina's wordt aangetroffen. Zeker jongeren zetten als gevolg van *peer pressure* echter vaak onware gegevens over zichzelf op internet, bijvoorbeeld door op te scheppen over hun drankgebruik of seksuele escapades – precies de zaken die hen later kunnen achtervolgen.

3.4 Kinderen en tieners

Privacyrisico's gelden des te sterker voor bepaalde kwetsbare groepen. Als het gaat over sociale netwerksites, dan zijn kinderen – en in het bijzonder tieners – zonder meer de meest kwetsbare groep. We hebben het dan over mensen die met internet zijn opgegroeid en het als vanzelfsprekend beschouwen dat er daar veel informatie over ze te vinden is. Ook zijn zij gevoelig voor sociale druk, en geven ze sowieso gemakkelijk gegevens over zichzelf en hun gezinsleden prijs. Maar het grootste risico vormen ongetwijfeld pedofielen en loverboys die met sociale netwerken beschikken over een krachtig nieuw middel om slachtoffers te vinden en contact met ze te leggen. Begin dit jaar werd bekend dat MySpace de afgelopen twee jaar niet minder dan 90 000 gebruikers heeft ontmaskerd als plegers van seksuele misdaden, en hun accounts heeft verwijderd.²⁴

18 Zie <www.theage.com.au/news/technology/web/social-notworking-facebook-snitches-cost-jobs/2009/04/08/1238869963400.html> voor een aantal voorbeelden.

19 Zie <www.wired.com/techbiz/it/magazine/17-07/ff_facebook-wall?currentPage=all>.

20 Zie <<http://online.wsj.com/article/SB122170459104151023.html>>.

21 Zie <<http://news.ninemsn.com.au/technology/855542/burglars-exploiting-facebook-twitter>>.

22 Zie <www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html>.

23 Zie <<http://weblogs3.nrc.nl/klaver/2009/08/07/coach-bekijkt-facebook-profiel-14-jarige-cheerleader>>.

24 Zie <www.guardian.co.uk/technology/2009/feb/09/children-online-safety-agreement>.

3.5 *Privacybevorderend identiteitsbeheer*

Hoe kunnen de in het voorgaande geschetste privacyrisico's het beste worden ondervangen? Voor een deel is die vraag prima te beantwoorden met het klassieke arsenaal aan privacybevorderende maatregelen: zorg voor bewustwording bij gebruikers en exploitanten van sociale netwerksites; dwing af dat sociale netwerksites transparant zijn over hun gegevensverwerkingen; verplicht ze ook om in software gebruikers een ruim scala aan privacybevorderende instellingen te bieden, en om die instellingen standaard aan te zetten; bied gebruikers effectieve mogelijkheden om hun recht te halen; draag zorg voor adequate beveiliging; en zo zou ik nog wel even door kunnen gaan.

Al deze maatregelen, hoe belangrijk ook, gaan echter grotendeels voorbij aan het feit dat het delen van persoonlijke informatie de essentie vormt van sociale netwerken. Alleen de standaardmaatregelen zullen daarom onvoldoende effect sorteren. Zoals Pekárek en Leenes schrijven²⁵: 'Even when SNS users are privacy aware, they do not tend to use available privacy tools. It appears that, in practice, individuals disclose more information than they intend to. Stronger still, research suggests that any tool or technique limiting the social aspects of SNSs is doomed to fail: users are simply not interested in them.'

Het is mijn overtuiging dat geavanceerd identiteitsbeheer de sleutel vormt tot werkelijk effectieve privacybescherming in de context van sociale netwerksites. Ik denk daarbij aan oplossingen die het gebruikers mogelijk maken om op een praktische, overzichtelijke en effectieve manier (al dan niet pseudonieme) deelidentiteiten op te bouwen en te beheren, inclusief de bijbehorende privacyregels. Aan zulke oplossingen wordt momenteel bijvoorbeeld gewerkt in het PrimelLife-project²⁶ uit het 7e Kaderprogramma van de EU. Interessant is in dit verband dat juist enkele grote sociale netwerksites zich de laatste tijd hebben opgeworpen als providers van online identiteiten.²⁷ Het zal interessant zijn om te zien of faciliteiten voor privacybevorderend identiteitsbeheer een factor van betekenis gaan vormen in de strijd om een plek op de markt voor sociale netwerksites en online identiteit die ophanden is.

4 Juridische ontwikkelingen

Wanneer we het tijdperk van de sociale netwerken laten beginnen met de oprichting van (het inmiddels al weer lang ter ziele gegane) SixDegrees in 1997, kunnen we constateren dat juridische aandacht voor de privacyaspecten in het eerste decennium van hun bestaan zich goeddeels beperkte tot rechtszaken over concrete privacyschendingen. De laatste jaren heeft het fenomeen echter een zodanige vlucht genomen dat ook wetgevers en toezichthouders zich in toenemende mate met sociale netwerksites zijn gaan bezighouden.

25 Martin Pekárek & Ronald Leenes, 'Privacy and Social Network Sites: Follow the Money!', *Position paper for the W3C Workshop on the Future of Social Networking*, Barcelona, January 15-16, 2009. Zie <www.w3.org/2008/09/msnws/papers/tilt.pdf>. Uit het citaat zijn enkele literatuurverwijzingen weggelaten.

26 Zie <www.primelife.eu>.

27 Zie <www.readwriteweb.com/archives/janrain_rpx_distributed_social_interscope_geffen_am.php>.

Privacy is daarbij steevast een belangrijk onderwerp. In maart vorig jaar publiceerde de *International Working Group on Data Protection in Telecommunications* zijn *Report and Guidance on Privacy in Social Network Services*.²⁸ Dat najaar volgde de internationale conferentie van privacytoezichthouders met haar *Resolution on Privacy Protection in Social Network Services*. Afgelopen juni publiceerde de Artikel 29 Werkgroep *Opinie 5/2009* over online sociale netwerken. De analyses en aanbevelingen in deze documenten zijn op hoofdlijnen vergelijkbaar en volgen min of meer de geijkte patronen. Zoals ik aan het einde van de vorige paragraaf al aangaf blijft daarmee identiteit als fundamentele invalshoek onderbelicht. Het feit dat aspecten daarvan wel aan de orde komen, bijvoorbeeld dat gebruikers de mogelijkheid moet worden geboden om pseudonieme profielen te maken, doet daar niet wezenlijk aan af.

De hierboven genoemde documenten zijn richtinggevend voor het privacybeleid en -toezicht, maar brengen niet direct concrete verplichtingen met zich mee voor sociale netwerksites. Een verdergaande stap was dan ook de overeenkomst die de Europese Commissie begin dit jaar sloot met een aantal belangrijke sociale netwerksites.²⁹ Deze had als doel om de privacy en veiligheid van kinderen en tieners die gebruik maken van sociale netwerken te verbeteren. Nog directer effect had een diepgaand onderzoek van de Canadese *Privacy Commissioner* naar de privacypraktijken van Facebook. Die oordeelde dat het bedrijf op een aantal punten de Canadese privacywet overtreedt. Naar aanleiding van de bevindingen van dit onderzoek kondigde Facebook eind augustus van dit jaar een aantal concrete verbeteringen in zijn privacybeleid aan.³⁰ Een week eerder hadden vijf inwoners van Californië een rechtszaak aangespannen tegen het bedrijf wegens het overtreden van privacywetgeving van de staat. Het heeft er alle schijn van dat sociale netwerksites het de komende tijd aanmerkelijk drukker zullen krijgen met privacy governance en compliance. Te hopen valt dat zij zich daarbij niet defensief opstellen, maar uitstekende privacybescherming onderkennen als een noodzakelijke voorwaarde voor hun bloei op lange termijn.

5 Conclusie

Sociale netwerken zijn volwassen geworden – nu hun privacybeleid nog. Verstandige sociale netwerksites onderkennen uitstekende privacybescherming als een noodzakelijke voorwaarde voor hun bloei op lange termijn. Die bescherming gaan ze alleen weten te bieden als bij de vormgeving ervan de omgang met identiteiten als fundamentele bouwsteen wordt erkend.

28 Zie <www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf>.

29 Zie <http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm>.

30 Zie <http://priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm> en <www.facebook.com/press/releases.php?p=118816>.