FACULTEIT LETTEREN
TAAL- EN COMMUNICATIE ANTWERPEN
SINT-ANDRIESSTRAAT 2
2000 ANTWERPEN
BELGIE

Masterproef aangeboden tot het verkrijgen van het diploma Master of Arts in de **journalistiek**

The (un)Usual Suspects:

De perceptie van privacybedreigingen door jongeren op verschillende onlineplatformen

Door: Eline Verdegem
Promotor: prof. dr. Michaël Opgenhaffen

ACADEMIEJAAR 2012-2013

0. Woord vooraf

Journalistiek. Het is een beroep dat me al sinds de secundaire school fascineert: op reportage gaan, interessante personen interviewen, meeslepende stukken schrijven… Altijd zag ik alleen de positieve kant van het beroep, de roddelpers hoorde volgens mij daar toch niet bij. Misschien was ik daarom vorig jaar zo gechoqueerd door die heisa rond het busongeval in Sierre.

Nog nooit was ik me ervan bewust geweest dat journalisten aan zoveel informatie kunnen als ze maar willen. Daarna vroeg ik mezelf natuurlijk af of er anderen waren die net zo verrast waren al ik. Het leek me een interessante aanzet voor onderzoek: Heerst er onder studenten angst voor journalisten? Zijn studenten zich ervan bewust dat journalisten met hun gegevens aan de haal kunnen gaan?

Met dat idee stapte ik naar mijn promotor, prof. dr. Michaël Opgenhaffen. Hij stelde voor om het idee volledig open te trekken naar *alle* potentiële indringers op het internet en op sociale media. De vraagstelling werd dus: van welke potentiële geïnteresseerden op onlineplatformen zijn studenten zich bewust?

Wat volgde was een enorm boeiend, maar niet altijd zo gemakkelijk, onderzoek. Daarom wil ik mijn promotor ook bedanken. Intussen begeleidt hij me al twee jaar, en na een leuke bachelorpaper kon hij deze moeilijke klus toch interessant houden. Als ik het even niet zag zitten, hielp hij me altijd weer op weg. Bovendien gaf hij me de kans om deze paper op het *Youth 2.0*-congres voor te stellen, wat een enorm bijzondere ervaring was. Dus bij deze: bedankt voor twee boeiende jaren.

1. Abstract

The bus accident in Sierre (Switzerland) that caused 28 victims and 4 casualties created much fuss in March and April 2012. Journalists had published pictures of the victims (mostly children) which were taken without permission from social media. That is why the *Belgian Society of Professional Journalists* (*Raad voor de Journalistiek*) formulated a new deontological guideline with regard to the use of social media.

From this perspective, it could be useful to investigate in which extent youngsters are aware of their online privacy and which strategies they use in order to protect that. The special focus in this study is that it will be examined which potential parties youngsters consider as interested and how youngsters think those parties will (mis)use their personal information.

First, the concept 'privacy' will be described in a social, political and legal context. Furthermore, privacy on the Internet and on social media will be studied. To conclude, there will be reflected on the potential parties who are interested, both the self-evident parties (i.e. commercial companies, banks, the government and employers) and the less self-evident parties (i.e. family, acquaintances and journalists).

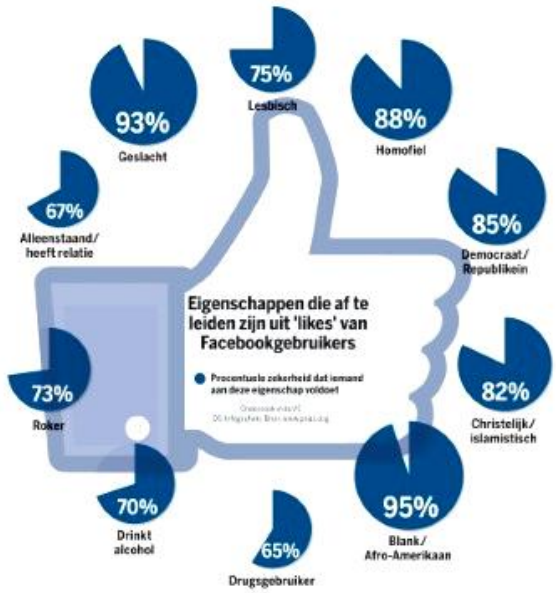
The research method consists of an online survey subjected to 346 Flemish pupils and students between 12 and 26 years old at a high school and the polytechnic group Thomas More. The key findings were the following: privacy awareness among youngsters is very low, but they consider many different interested parties. Apart from the self-evident parties, such as the government, companies, banks and criminals, family and partners are also frequently mentioned. Surprisingly, many youngsters are aware of the potential threat of journalists and consider journalistic research as a privacy violation. Also, the youngsters are abhorrent of the use of their personal information in the media.

The phrasing of the question about potential interested parties is one big limitation of this inquiry. It is not very clear that the focus lies on abuse of the personal data by the potential interested parties. In further research, this can be examined more deeply.

Inhoudsopgave

2. Inleiding

Op woensdag 13 maart 2013 verscheen er in *De Standaard* een artikel over een Brits onderzoek op de sociale netwerksite Facebook. Britse wetenschappers bestudeerden de *likes* van 58.000 Amerikaanse Facebookgebruikers. Daaruit bleek dat ze aan de hand van de *likes* meer te weten konden komen over de persoonlijkheid van een Facebookgebruiker. Eigenschappen zoals geslacht, ras, seksuele aard, politieke voorkeur en het gebruik van alcohol en drugs waren allemaal uit die *likes* af te leiden (zie figuur 1). De onderzoekers konden zelfs met 60% zekerheid zeggen of iemands ouders voor zijn 21ste gescheiden waren. "Hoe meer *likes* iemand heeft, hoe accurater het beeld dat eruit ontstaat", luidde het in de krant. Het nadeel is wel dat de *likes* openbaar zijn en dat iedereen ze kan bekijken. Voor adverteerders is dat een goede zaak, maar de gebruikers kunnen daar anders over denken. Zo blijkt dat gebruikers "hun toestemming er niet voor gaven, dat ze er zich niet van bewust zijn of dat ze niet de intentie hadden sommige informatie bekend te maken" (Sels, 2013).



Figuur 1. Percentage zekerheid dat iemand aan bepaalde kenmerken voldoet (bron: www.pnas.org, DS-Infografiek).

Privacy wordt door de toenemende technologische ontwikkelingen steeds een zeldzamer goed. Op het internet worden gegevens zomaar te grabbel gegooid en sociale netwerksites komen regelmatig in opspraak door commerciële interesse te tonen in de gegevens van hun gebruikers. Zo kreeg het fotoplatform Instagram een golf van kritiek over zich heen nadat dat platform bekendmaakte dat die, na aanpassing van het privacybeleid, foto's van gebruikers kon doorverkopen. Door het grote protest werd die aanpassing uiteindelijk ingetrokken.

Nu kan de vraag gesteld worden hoe bewust gebruikers zich van hun privacy online zijn. Uit verschillende studies blijkt dat bijvoorbeeld Facebookgebruikers vaak onterecht denken dat hun

persoonlijke gegevens binnen hun onlinevriendenkring blijven (Butler et al., 2011; Newell, 2011; Tuunainen et al., 2009; Veltsos & Veltsos, 2010; Walrave et al., 2012; Zansberg & Fischer, 2011). Kennis over het privacybeleid is bedroevend laag en het recente rapport van het *EU Kids Online Project* toont dan weer aan dat amper 1% van jongeren tussen negen en zestien jaar zich zorgen maakt over het onthullen van persoonlijke gegevens op het internet (Livingstone et al., 2013). Bovendien toont recent onderzoek aan dat jongeren nu meer persoonlijke informatie delen dan vroeger (Madden et al., 2013).

Verder worstelt de wetgeving met onlineprivacy. Sommige landen leggen regels in wetten vast, terwijl andere zelfregulering toepassen (Cha, 2011; Barrett & Strongman, 2005). Maar beide manieren zijn soms niet toereikend genoeg om de privacy te beschermen. Het busongeval in Sierre en de afluisterschandalen door de Britse tabloid *News of the Wor*ld zijn daar treffende voorbeelden van.

Sierre gaf hier een aanzet voor verder onderzoek. Hoe bewust zijn internetgebruikers zich van hun onlineprivacy en van minder vanzelfsprekende potentiële geïnteresseerden (zoals journalisten) in hun persoonlijke informatie? Er zijn al wel eerdere studies naar onlineprivacy uitgevoerd, maar meestal is dat voor een beperkt aantal platformen, zoals verschillende sociale media (Facebook, Twitter, LinkedIn, enzovoort) (Russell, 2011; Madden, 2012), Google (Maurer et al., 2007) en commerciële websites (Cha, 2011; Walrave et al., 2011). Het *EU Kids Online Project* heeft wel gefocust op tal van verschillende platformen, maar in dat onderzoek werd vooral de nadruk gelegd op internetrisico's en zaken waaraan jongeren zich op het internet storen (Livingstone et al., 2013). Een onderzoek naar potentiële geïnteresseerden in persoonlijke gegevens online is moeilijk te vinden, en net dat maakt het interessant om daar dieper op in te gaan en een extra focus op journalisten te leggen. Daarom werd dit academiejaar het onderzoek door middel van een onlinesurvey over allerlei verschillende platformen uitgevoerd.

In deze paper wordt eerst een uitgebreide literatuurstudie gegeven, waarin de oorsprong van privacy en de wetgeving ervan worden bekeken. Ook privacy op het internet en sociale media komt aan bod, gevolgd door een groot hoofdstuk over potentiële geïnteresseerden. De literatuurstudie is vrij groot doordat allerlei verschillende platformen die in het onderzoek besproken zullen worden, met betrekking tot privacy onderling kunnen verschillen. Daarna worden er op basis van de literatuurstudie vier onderzoeksvragen geformuleerd over de waargenomen potentiële geïnteresseerden, de waargenomen mogelijke privacybedreigingen, privacybewustzijn en beschermingsstrategieën voor de privacy, waarna de methode wordt uitgelegd. De resultaten worden in een apart hoofdstuk uitgebreid besproken. De paper wordt afgesloten met een besluit, een discussie en suggesties voor vervolgonderzoek.

3. Literatuurstudie

3.1 Privacy

3.1.1 Definitie en oorsprong

Privacy is een begrip dat al sinds de Klassieke Oudheid bestaat, maar ondanks zijn lange bestaan blijft het een vaag concept. Volgens de Van Dale[13] luidt de definitie van privacy als volgt:

> Persoonlijke vrijheid, het ongehinderd alleen, in eigen kring of met een partner ergens kunnen vertoeven; gelegenheid om zich af te zonderen, om storende invloeden van de buitenwereld te ontgaan.

Veltsos en Veltsos geven een andere definitie in de vorm van *The Generally Accepted Privacy Principles*, opgesteld door het *American Institute of Certified Public Accountants* (Veltsos & Veltsos, 2010, p. 464):

> The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

Bovenstaande definities zijn voorbeelden van een reeks van talrijke omschrijvingen die aan het begrip gegeven worden. Bovendien zijn er doorheen de jaren andere betekenissen aan het concept gegeven. Zo is er een verschil tussen "privacy met betrekking tot informatie over het individu en *informational privacy* van een individu" (O'Brien, 2008, p.26). In de negentiende en twintigste eeuw werd er meer aandacht besteed aan 'het recht op privacy' en 'het recht om met rust gelaten te worden'. Fenwick spreekt over *informational autonomy*. Dat betekent dat een individu het recht heeft om informatie over zichzelf te controleren. De basis voor die ideeën is het artikel 'The Right to Privacy', geschreven door rechters Samuel D. Warren en Louis D. Brandeis en verschenen in het tijdschrift *Harvard Law Review* in 1890. Zij schreven dat de wet moest worden gebruikt om de individuele privacy van de burgers te beschermen dankzij een combinatie van 'the right to be left alone' en een reeks van politieke, sociale en economische veranderingen in de late negentiende eeuw. De aanleiding voor het artikel was de pers; in diezelfde periode was de *penny press* in volle bloei en werden journalisten een bedreiging voor de burgers hun privacy. Bovendien toonden Warren en Brandeis de gevaren van de fotografie aan. Fotografie werd als een nieuwe bedreiging voor de privacy bekeken, omdat journalisten zonder iemands toestemming personen op beeld konden vastleggen en vervolgens in kranten publiceerden (Friedman, 2002, p. 1114-1115; O'Brien, 2008, p. 26-27).

Een actueel voorbeeld van de bedreiging voor de privacy door middel van foto's, is het incident met de Britse prinses Kate Middleton. Daarbij nam een fotograaf halfnaakte foto's van de prinses en publiceerde die in het Franse blad *Closer*. Er volgde een rechtszaak waarna de publicatie van de foto's verboden werd. Er loopt nog een strafrechtelijke procedure tegen het magazine, de hoofdredacteur en

de fotograaf. Als ze veroordeeld worden, kunnen ze een celstraf krijgen en zullen ze een boete moeten betalen (Domi, 2012).

3.1.2 Juridische beslissingen rond privacy

Hoewel het artikel van Warren en Brandeis invloed had, waren er weinig rechtszaken waarin de gegeven richtlijnen strikt gevolgd werden. Friedman geeft een voorbeeld van een zaak waarin dat wel het geval was, namelijk in een Californische zaak in 1931: Melvin vs. Reid. De aanklaagster, Gabrielle Darley Melvin, een voormalige prostituee die vrijgesproken was van moord, daagde een filmmaatschappij voor de rechter omdat die een film over haar leven had gemaakt. Ze vond dat ze in haar eer geschonden was en won uiteindelijk de zaak. De rechtbank wilde haar eer, fatsoen en reputatie beschermen zoals Warren en Brandeis het in hun artikel beschreven hadden. Friedman vermeldt ook dat de rechtbank een regime van tweede kansen wilde beschermen, waarna hij aantoont dat het idee van een nieuwe start grenzen heeft. Melvin had die, gezien haar woelige verleden, duidelijk overschreden (Friedman, 2002, p. 1115-1116).

In de zaak Marcel vs Metropolitan Police en gelijksoortige zaken, is beslist dat politieagenten alleen informatie mogen gebruiken als het voor het onderzoek en de vervolging van een misdaad dient of als gestolen goed naar de eigenaar moet worden teruggebracht. Een persoon mag dus informatie weigeren te geven als de politie die onrechtmatig opvraagt (Wlr, 1999).

Ook zijn er zaken rond onlineprivacy. Paul Chambers werd op 10 mei 2010 veroordeeld na een grap over een bombedreiging op Twitter. Hij was de eerste persoon die veroordeeld werd door toedoen van het gebruik van Twitter. Barrett en Strongman tonen daarmee aan dat vrije meningsuiting op het internet wel mogelijk is, maar dan in een *gesloten* gemeenschap (Barrett & Strongman, 2005, p. 134-135).

Joshua Ashby werd op 12 november 2010 veroordeeld nadat hij naaktfoto's van zijn ex-vriendin op Facebook had gepost. In dat geval was de waardigheid van het meisje aangetast, waardoor hij veroordeeld werd (Barrett & Strongman, 2005, p. 136-137). Dat type zaak zou kunnen worden toegepast op de oprichters van de Facebookpagina 'Zelzaatse hoertjes', een pagina die in januari 2013 in Vlaanderen werd opgericht en waarop foto's van schaars geklede meisjes zonder hun medeweten op de pagina werden geplaatst. De waarnemend burgemeester en de waarnemend zonechef van de politiezone Puyenbroeck dienden klacht in "wegens smaad en eerroof". Ook de in januari 2013 opgerichte Vlaamse Facebookpagina 'Failed: Leuven', waarop foto's van dronken studenten gepost worden, is volgens de Leuvense lokale politie "een schending van de privacywetgeving en vormt ook een inbreuk op het portretrecht" (Mtm, 2013; Rdc, 2013).

3.1.3 Wetgeving: politiek en sociaal beleid rond privacy

Sinds 11 september 2001 is de beveiliging in de meeste landen sterk toegenomen. De burgers en de grenzen worden meer en meer gecontroleerd, wat een impact op de privacy heeft. "De Europese 'data retention'-richtlijn verplicht alle operatoren en internetproviders om bij te houden wie met wie gecommuniceerd heeft en wie welke websites bezoekt", schrijft Preneel (2012, p. 18-19). Hij waarschuwt dan ook voor eventueel misbruik van de informatie door de overheid (zie infra).

3.1.3.1 Politiek

Er zijn twee types van wetgeving die gehanteerd worden: via legislatieve bescherming en via zelfregulering door industrieën. De Europese Unie, Australië, Canada en Nieuw-Zeeland worden door wetten gereguleerd, waarbij de Europese Unie het strengst optreedt. Daarbij maakt de EU gebruik van een fundamenteel principe, namelijk het concept *data minimization*. Dat betekent dat enkel de vereiste data gegeven mogen worden, en niet meer dan dat. De Verenigde Staten gebruiken echter het systeem van zelfregulering (Cha, 2011, p. 615-617).

In onderzoek werd aangetoond dat zelfregulering niet altijd tot de gewenste effecten leidt. Zo worden bij websites de klanten amper beschermd, zodat de websites meer voordeel kunnen halen uit de gegevens van de klanten. Het privacybeleid wordt door bedrijven vooral gebruikt om zich tegen rechtszaken te beschermen. Dat doen ze door middel van vage richtlijnen in hun beleid te geven, waarin ze bepaalde cruciale aspecten rond privacy onderbelicht laten. Het intussen in Skype opgenomen chatprogramma MSN vermeldde bijvoorbeeld terloops het gebruik van *cookies*, maar het gebruik ervan wordt in het vage gelaten. Pas bij het gebruiken van links kan de klant meer informatie over *cookies* verkrijgen (Fernback & Papacharissi, 2007, p. 715-733).

In februari 2012 startte de regering Obama een discussie over de zelfregulering van bedrijven. Obama wil dat de burgers beter beschermd worden door een aantal richtlijnen in te voeren waaraan bedrijven zich moeten houden. Die principes krijgen de naam *privacy bill of rights*, maar doordat het een verkiezingsjaar was, is het plan nog niet verder uitgevoerd. In februari 2013 zijn de gesprekken, die door de Europese Unie aangemoedigd worden, weer opgestart (Mg, 2012).

Wel zijn de Verenigde Staten mee verantwoordelijk voor een belangrijke innovatie: de *web seal programs* TRUSTe en BBCOnline. Die programma's staan ten dienste van (beginnende) websites met weinig naamsbekendheid, die met behulp van een certificaat van zulke programma's mensen kunnen lokken. Die sites moeten aan een minimum aantal voorwaarden voldoen om een dergelijk certificaat te krijgen. Surfers kunnen met hun klachten bij die *web seal programs* terecht, waarna de site in kwestie een sanctie kan krijgen. *Web seal programs* kunnen als aanvulling bij de privacywetgeving gezien

worden. Voorbeelden van bedrijven die een TRUSTe-certificaat hebben, zijn Apple (voor iTunes), Disney, eBay, Forbes, Hewlett-Packard en Microsoft (Swire, 2003, p. 865; TRUSTe, 2012).

3.1.3.1.1 Redelijke verwachtingen van privacy

Privacywetten van de Verenigde Staten hebben soms een te enge visie op het begrip privacy. Het gerecht vertrouwt op redelijke verwachtingen van privacy, maar die grenzen tussen wat redelijk en onredelijk is, zijn onduidelijk. Zo zijn er rechtbanken die een privacyverwachting als onredelijk bekijken als de informatie op het internet geplaatst is. Daar is nuancering bij nodig. Sommige informatie is maar voor een select groepje mensen bedoeld, waarbij de internetgebruiker op privacy rekent (Sprague, 2009, p. 400-410):

> New forms of communication allow others to view what are intended to be at least somewhat private conversations. Protecting these conversations requires an attitudinal shift towards acceptance of the idea that just because a few people have access to information does not mean it is no longer private. Privacy law will have to adapt to the notion that information can still be private even it is not concealed. Just because we share confidential information with someone does not mean it is automatically "public" (i.e., no longer private). U.S. privacy law will have to abandon the attitude that "privacy" means "secret" (Sprague, 2009, p. 408-409).

Een voorbeeld om aan te tonen dat die wetten verouderd zijn en dus herzien moeten worden, is de zaak Moreno v. Hanford Sentinel. Een studente postte op haar MySpacepagina een bekritiserende tekst over haar woonplaats Coalinga (Californië). Haar schooldirecteur vond het artikel een stuurde het naar een krant die het vervolgens publiceerde. Doordat er zoveel kritiek op kwam, moest de familie van het meisje verhuizen. Ze klaagden de krant aan, maar in 2009 verwierp de rechtbank de zaak omdat het meisje haar artikel op een openbaar medium had gezet en daar rekening mee had moeten houden. Die zaak toont met andere woorden aan dat het aspect van openbare informatie tegenover privé-informatie online ook verhuld zit in de leidraad voor gebruik van sociale media (Newell, 2011, p. 21-23).

3.1.3.1.2 Privacy in Europa

Tuunainen en collega's klagen aan dat de wetten niet effectief genoeg zijn om sociale netwerksites tegen te gaan. Ze geven het voorbeeld van de Europese wet, die het verwerken van privégegevens verbiedt tenzij de persoon in kwestie zijn goedkeuring geeft. Het probleem daarbij is dat gebruikers van sociale media vaak het privacybeleid niet lezen of niet begrijpen, en dat ze helemaal geen goedkeuring willen geven. De wetten moeten dus volgens de onderzoekers gemoderniseerd worden (Tuunainen et al., 2009, p. 4-5).

Maar op 25 januari 2012 werd in de Europese Unie een nieuw wetsvoorstel gepresenteerd, namelijk een *data-protection package* waarbij voor alle EU-leden eenzelfde privacywet geldt. Tegen 2015 zal

die wet in uitvoering gebracht worden en zullen alle EU-leden onder eenzelfde *data-protection law* opereren (Gilbert, 2012, p. 20-21).

In de Belgische grondwet is de informationele privacy gereguleerd door de wetgeving die de Europese richtlijn volgt. Al is die wet in België aan de Belgische legislatuur aangepast, waardoor er onder andere enkele bijkomende rechten voor individuen zijn toegevoegd (Walrave, 2003, p. 3-4).

Ondanks die wetten en een privacycommissie blijft het concept privacy een heikel punt. Recent was er in Groot-Brittannië heel wat te doen rond het rapport van rechter Brian Leveson, die in opdracht van premier Cameron moest nagaan wat er met de media moet gebeuren na de afluisterschandalen van de tabloid *News of the World*. Leveson stelde een wettelijke instelling voor die als perswaakhond de media moet reguleren om zo onder meer de privacy van de burgers te beschermen. Met *The Press Complaints Commission* was er al wel een waakhond, maar die werd een "waakhond zonder tanden" genoemd. Dus zou een perswet nodig zijn. Aangezien het van de zeventiende eeuw geleden is dat de media door een wet gereguleerd werd, was er heel wat tegenstand. In maart 2013 bereikten de Conservatieven, Labour en de Liberaal-Democraten een akkoord: er wordt een waakhond bij koninklijk besluit opgericht met een extra speciaal statuut om de macht van de instelling te beschermen. Bovendien kan die waakhond zware boetes opleggen en media verplichten om 'rechten van antwoord' te publiceren (Minten, 2012; Minten, 2013).

3.1.3.2 Sociaal belang

Het verlies van privacy kan impact hebben op hoe we ons ontwikkelen, schrijft Van der Spoel. Ze onderbouwt haar stelling door Foucault te citeren, die door de Engelse Verlichtingsfilosoof Jeremy Bentham (1748-1832) geïnspireerd was en zijn metafoor van het panopticum gebruikt:

> Jeremy Bentham ontwierp het panopticum als een gevangenis, waarin de gedetineerden zich in een constructie bevonden waarin ze continu gezien konden worden door een bewaker in één enkele bewakingstoren. Hoewel zij vanuit de toren te allen tijde zichtbaar waren, konden de gevangenen niet de bewaker in de toren zien, waardoor ze nooit wisten of ze nu wel of niet bewaakt werden. Hierdoor zouden de gevangenen, al dan niet in het oog gehouden door een bewaker, zich altijd gedragen alsof ze onder surveillance stonden (Van der Spoel, 2012, p. 37).

Van der Spoel schrijft vervolgens dat we ons anders zullen gedragen als we ons bekeken voelen en dat we misschien onze persoonlijkheid niet meer volledig zullen kunnen ontwikkelen, maar dat "we zouden schikken met een *middle-of-the-road conventionality*". Van der Spoel legt de vergelijking met Facebook, dat als een machtsstructuur in het panopticum kan worden gezien (Van der Spoel, 2012, p. 37-55).

Ook journalisten houden zich met zulke ideeën bezig. Joël De Ceulaer, redacteur bij *De Standaard*, omschrijft hoe mensen van gedrag veranderen als ze zich bekeken voelen. Hij noemt een experiment

waarbij er in de toiletten op de spiegel een gezichtje getekend is. “De toiletbezoekers zullen – onbewust weliswaar – het gevoel hebben dat ze worden bekeken en ze zullen, juist: vaker hun handen wassen”, schrijft hij. Ook als mensen weten dat er camera’s hangen, zullen ze zich beter gedragen. Daarom is een transparantere wereld niet altijd noodzakelijk slecht, citeert De Ceulaer Guillaume Van der Stighelen, auteur van de spirituele bestseller ‘Echt’. Toch wordt het stuk afgesloten met de opmerking dat een controlestaat niet wenselijk is, en wordt er betwijfeld of een volledig transparante wereld tot een betere samenleving leidt (De Ceulaer, 2012).

3.2 Privacy online

De komst van Web 1.0 was een kans om anarchistisch en anoniem een vrije mening te uiten. Het internet was vrij van juridische tradities en sociale druk. Er waren niet echt normen of regels, en als er waren, waren ze grotendeels bepaald door de internetgebruikers en de commerciële websites. Met de ontwikkeling van Web 2.0 veranderde dat. Barrett en Strongman omschreven die verandering als volgt: "Normative expectations have shifted away from a wild-west world in which websites did almost whatever they wanted with impunity to a world in which a significant percentage of websites are explicitly addressing privacy concerns" (Barrett & Strongman, 2005, p. 128). Met andere woorden: privacy op het internet werd belangrijker, en daarvoor was regulering nodig (Barret & Strongman, 2005, p. 127-128).

Toch is regulering van het internet niet vanzelfsprekend. Zo moet er rekening worden gehouden met vier verschillende factoren: (1) de autoriteit van plaatselijke of nationale overheden om controle uit te oefenen op onlineactiviteiten, (2) de effecten van onlinegedrag op individuen of zaken, (3) de legitimiteit van een plaatselijke soevereine staat om plaatselijke regels te formuleren of toe te passen op globaal vlak en (4) de bekwaamheid om aan te geven welke regels op een bepaalde fysieke locatie van toepassing zijn. Bovendien moet er ook rekening worden gehouden met nationale verschillen. Tot vandaag is er nog steeds geen specifieke Internetwet, al wordt het wel grondig bestudeerd (Barrett & Strongman, 2005, p. 129-130).

3.2.1 Dataverzameling en cookies

Het online verzamelen van gegevens kan op verschillende manieren gebeuren. Een gebruiker kan zich online registreren waarbij de nodige gegevens gevraagd worden. Andere mogelijkheden zijn via bulletinboards, elektronische postkaarten of chat rooms. Ten slotte zijn er de *cookies*, elektronische *tracking devices* die nagaan hoe een computer gebruikt wordt of hoe een gebruiker zich online gedraagt. In 2000 werd er via een survey nagegaan hoeveel gebruikers zich van *cookies* bewust zijn, en daaruit bleek dat 56% zich niet van *cookies* bewust is en dat die respondenten niet wisten dat ze iemands sporen op het internet kunnen nagaan. Tegenstanders vinden het gebruik van *cookies* een inbreuk op de privacy, maar toch worden ze veel gebruikt. Zo maken de populaire nieuwssites *The New York Times Online* en *CNN* gebruik van de *tracking devices* (Hong et al., 2005, p. 17-18).

Cookies kunnen voor (internet)bedrijven en adverteerders goed van pas komen om zo veel mogelijk informatie te verzamelen. Hoewel uit recenter onderzoek blijkt dat de meeste internetgebruikers zich van *cookies* bewust zijn, zijn die vaak niet op de hoogte van de (online) context waarin hun gegevens verzameld worden. Bijgevolg hebben ze amper tot geen controle over hun eigen gegevens. Adware is een voorbeeld van een programma dat automatisch geïnstalleerd wordt en vaak zonder het medeweten

en de goedkeuring van de gebruiker informatie verzamelt (Pierson & Heyman, 2011, s.p.; Volkmer, 2004, p. 1-13).

In mei 2011 werd in Europa de *cookiewet* aangepast. Voordien volstond het om in het privacybeleid op de site duidelijk aan te geven of de site *cookies* gebruikte en dat de gebruiker die kon weigeren. Vanaf mei 2011 werd er een kleine nuance aangepast. De "offer the right to refuse" werd "User has given his or her consent", wat betekent dat de gebruiker (impliciet) de toestemming moet geven om *cookies* te gebruiken. In België trad die wet op 04 augustus 2012 in werking (Van der Haegen, 2012).

3.2.2 Internet en e-commerce

E-commerce ontstond midden de jaren 90 en ontwikkelde een eigen privacybeleid omdat de overheid zelfregulering van zulke industrieën steunde. Zulke sites hebben meer succes als ze tonen dat ze rekening houden met juridische regels of als ze al een bepaalde naam hebben. Daardoor komen ze betrouwbaarder over. Andere sites die het vertrouwen van klanten willen winnen, maken bijvoorbeeld gebruik van https-URL's of vragen een faxnummer als de gebruiker zijn kredietkaartnummer niet wil geven (Swire, 2003, p. 847-858).

Een voorbeeld is de opkomst van eBay. Bij de start steunde de site op een *non-legal "feedback" system*, waarbij succesvolle transacties van kopers en verkopers goed of slecht beoordeeld werden. Dat was een succesvol systeem, maar toch toonde eBay meer en meer aandacht voor juridische regels, tot die uiteindelijk een juridisch document met de naam 'Rules and Safety Overview' op de site beschikbaar maakte. Vandaag is eBay nog steeds een heel succesvolle e-commercewebsite (Swire, 2003, p. 855-857).

Hong's onderzoeksteam wijst op het feit dat veel onderzoek op e-commercewebsites gericht is, waarbij de opkomst van de nieuwssites genegeerd is. Onderzoek bij zulke sites kan ook relevant zijn, omdat ze sterk opkomen en ook persoonlijke gegevens verzamelen. Dat doen ze bijvoorbeeld door registratie, zoals *The New York Times*, *Los Angeles Times*, *Chicago Tribune* en *Dallas Morning News*. Het verzamelen van gegevens kan worden gebruikt om nieuwe adverteerders aan te trekken en/of de advertentie-inkomsten bij al aangesloten adverteerders te verhogen. Ook bij nieuwssites moet dus de privacy van de gebruikers in acht worden genomen. Bovendien tonen de onderzoekers dat in vorig onderzoek met betrekking op privacy en e-commerce ontdekt is dat de zorgen om privacy een grote hindernis vormen bij de commerciële ontwikkeling van het internet. Daarom zullen nieuwssites minder snel onelineabonnementen gebruiken (Hong et al., 2005, p. 15-17).

Het onderzoek van Hong toonde aan dat 81,7% van de Amerikaanse nieuwssites gegevens verzamelde over hun gebruikers. 68,4% deed dat door middel van *cookies*, en maar 20,5% met behulp van

registratie. Weinig nieuwssites toonden een privacybeleid. Maar 37% toonde een privacystatement en 28% gaf een uitgebreid privacybeleid. Hong verwijst daarbij naar vorig onderzoek, waaruit bleek dat 41,5% van de e-commercewebsites een privacybeleid toonde. Verder bleek dat hoe meer informatie een nieuwssite verzamelde, hoe sneller die site een privacybeleid aanbood. Ook de nieuwssites die gebruik maakten van *cookies*, toonden sneller een privacybeleid (Hong et al., 2005, p. 23-27).

3.2.3 Google

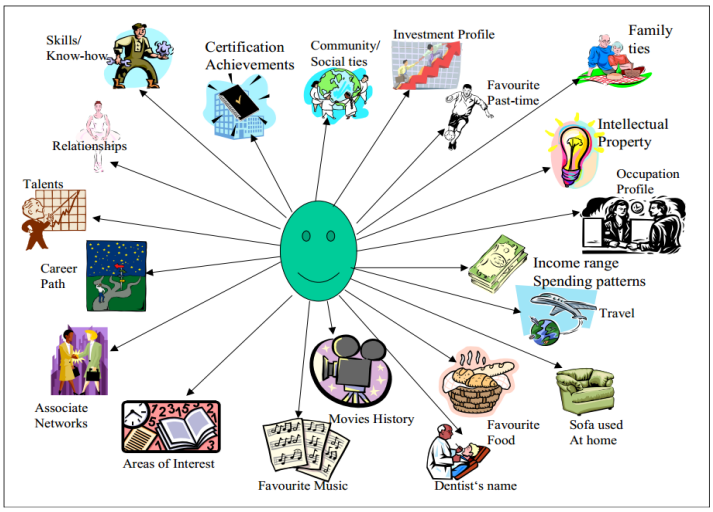
Google, opgestart in 1998 en sinds 11 september 2001 de grootste zoekmachine ter wereld, is een bedrijf met heel wat macht geworden. Zo wordt er gezegd dat het meer dan andere instellingen informatie weet over personen, bedrijven en organisaties en dat Google niet door nationale *data protection laws* beperkt wordt. Google doet aan *data mining*, "a technology that discovers non-trivial hidden patterns in a large collection of data" (Maurer et al., 2007, p. 75-76). Door die technologie verzamelt Google vaak onopgemerkt informatie. Verder doet het bedrijf heel geheimzinnig over zijn beleid en methodes van dataverzameling, waardoor het voor de meeste mensen niet duidelijk is "wat Google kan doen, al doet en zou doen" (Maurer et al., 2007, p. 161). Google kan bijvoorbeeld in de toekomst informatie aan bedrijven doorverkopen (p. 79), want het bedrijf heeft dat al voor de Chinese overheid gedaan om mee te helpen aan de strijd tegen het terrorisme (Maurer et al., 2007, p. 164-165). Ondanks die nadelen is Google nog steeds de meest succesvolle zoekmachine op het internet (Maurer et al., 2007, p. 5-6; Ms, 2011, s.p.).

Door het grote succes trekt Google tal van adverteerders aan, waardoor het bedrijf in 2000 AdWords invoerde. Bij het opzoeken van een bepaald woord verschijnen er advertenties die daar betrekking op hebben. In 2003 kwam daar AdSense bij. Daarbij scant Google de inhoud van de site en linkt het bedrijf passende advertenties aan de site (Ms, 2011, s.p.).

Google biedt ook diensten aan zoals Gmail, Google Earth, YouTube, Google Maps en de daaraan verbonden Google Streetview. Verder heeft de zoekmachine met Google Chrome haar eigen browser. Doordat bijna iedereen gebruikmaakt van één of meerdere diensten van Google, kan het bedrijf nog meer informatie inwinnen en bijgevolg heel machtig worden: "With additional services such as Google Mail and on-line communities, user behavior can be analyzed on a very personal level" (Maurer et al., 2007, p. 161). Google wordt verweten aan data-obesitas te lijden, wat betekent dat Google gebruikersgegevens verzamelt en doorverkoopt aan adverteerders (Maurer et al., 2007, p. 74; Van der Spoel, 2012, p. 3-6).

3.2.3.1 Profiling

Het type informatie dat zoekmachines zoals Google verzamelen, is van allerlei soorten. Maurer en collega's (2007) geven in hun rapport voorbeelden zoals telefoonnummers, huisadressen, news feeds, foto's, boeken, video's, e-mails, schoolwerk en financiële, geografische en chronologische data. Bovendien kunnen zoekmachines inzicht krijgen in het leven van "anonieme" gebruikers. Zo kunnen ze gedrag, houdingen, interesses, levensstijl, intenties, humeur en gedachten opsporen. Maar zoekmachines zijn niet de enigen die data verzamelen. "A great deal of knowledge about users is also being maintained by governments, airlines, medical profiles or shopping consortiums (p. 78)", luidt het. Met behulp van zulke dataverzamelingen, kan er aan *profiling* gedaan worden. *Credit card companies* kunnen bijvoorbeeld uitgavengedrag volgen om fraude op te sporen (Maurer et al., 2007, p. 76-176).



Figuur 2. Informatie die Google via zoekopdrachten allemaal kan verzamelen (Uit: Maurer et al., 2007, p. 175).

Met behulp van persoonlijke gegevens kan Google na een tijd voorspellen wat een gebruiker zoekt op basis van één letter in de zoekbalk. Ook personaliseert Google de aangeboden informatie meer en meer voor de individuele internetgebruiker. Een journalist van het Belgische weekblad *Humo* geeft het voorbeeld van de linkse politicus en internetactivist Eli Pariser, die de zoekopdracht 'olieramp Deepwater' ingaf. Bij de linkse vrienden van Pariser stonden nieuwssites bovenaan in de ranking, terwijl bij de rechtse vrienden "alleen sussende pr-berichten van de olie-industrie" werden gegeven. Verder biedt Google sinds 2004 binnen het mailprogramma Gmail advertenties aan. Die mails worden door middel van een algoritme gescand, waarna er passende advertenties kunnen worden aangeboden. Zo leiden mails die over bijles handelen tot advertenties over bijlessen. Bovendien kan Google zelfs aan gegevens van personen die niet met Gmail werken, maar die wel met iemand met een gmailaccount corresponderen. Sindsdien laait de discussie over privacy steeds meer op (Ms, 2011, s.p.).

3.2.3.2 Incidenten

Google heeft al vele malen onder vuur gelegen. Zo zijn de opt out-mogelijkheden (voor het delen van persoonlijke gegevens) moeilijk te vinden, verandert het privacybeleid voortdurend zonder dat de internetgebruikers ervan op de hoogte worden gebracht en kunnen nieuwe toepassingen van Google vaak tot een massa kritiek leiden. Bij Google Streetview bijvoorbeeld, kwamen er klachten binnen van personen die herkenbaar op de foto's stonden. Bovendien was er ook heisa rond de auto's waarmee de foto's genomen werden. Die verzamelden namelijk persoonlijke informatie zoals e-mails en wachtwoorden via de draadloze internetnetwerken (Ms, 2011, s.p.; X., 2012, p. 8).

In februari 2010 lanceerde het bedrijf Google Buzz, een sociaal netwerk in het systeem van Gmail, waardoor gebruikers updates voor hun contacten konden posten. Wel werden alle contacten van een persoon zichtbaar voor elkaar, wat niet voor iedereen wenselijk was. Zansberg & Fischer illustreren het probleem met het voorbeeld dat dokters en advocaten ook in die lijst zichtbaar waren, en dat een vrouw haar privacy niet tegen haar gewelddadige ex-man beschermd werd. Na heel wat kritiek stopte Google het systeem en verontschuldigde het bedrijf zich aan zijn gebruikers. Op 11 oktober 2011 werd beslist dat Google een uitgebreid privacybeleid moet hebben en aan de richtlijnen voor privacy moet voldoen voor de komende twintig jaar. Overtredingen van die regels leiden tot sancties (Zansberg & Fischer, 2011, p. 30-31).

Op 1 maart 2012 veranderde Google nogmaals zijn privacybeleid. Daardoor mag het bedrijf gebruikersinformatie aan zijn andere diensten doorgeven. Ook vereenvoudigde en condenseerde het bedrijf zijn privacybeleid, waardoor het onduidelijker wordt hoe er met die gegevens zal worden omgegaan. Google komt ten slotte met een nieuwe zoekfunctie met de naam *Search plus Your World*, "waardoor foto's, updates en andere privé-informatie van Google+ in de zoekresultaten verschijnen". Door die veranderingen komt Google weer in opspraak, en moet er over een eventuele sanctie overleg komen, gezien Google sinds Google Buzz geen misstappen meer mocht maken (X., 2012, p. 7).

Ondanks die misstappen en het feit dat de zoekmachine regelmatig bekritiseerd wordt, blijft iedereen van de diensten gebruikmaken. "Zolang er een gepaste stroom is van die persoonlijke informatie voelen we dat niet als een schending van onze privacy", verklaart Nissenbaum (Van der Spoel, 2012, p. 40). Toch raadt Van der Spoel aan om "alert te blijven op een mogelijke schending van de informationele privacy zolang de informatiestroom niet gepast is en privacybeleid van mediabedrijven niet transparant" (Van der Spoel, 2012, p. 40).

Maurer en zijn team houden in hun rapport ook een belangrijke vraag voor ogen: "As more and more people are willing to compromise privacy, the questions that we pose are: Who do we trust as the gatekeeper of all our data? Do we then trust all our private data at the hands of a commercial global company?" (Maurer et al., 2007, p. 79). Het is een vraag waar de maatschappij nog steeds niet uit is.

Bovendien is het bedreigende monopolie van Google niet het enige potentiële gevaar. Online kan de internetgebruiker op allerlei verschillende platformen tal van andere risico's lopen, zoals opgelicht worden op bankensites, last krijgen van virussen via e-mail of seksueel misbruik door tijdens online dating de verkeerde persoon te ontmoeten. In de volgende paragraaf worden de potentiële gevaren uitgebreid besproken.

3.2.4 Potentiële gevaren online

3.2.4.1 Online Banking

Een groot gevaar voor individuen op onlinebankingsites zijn hackers. Die plegen regelmatig financiële fraude door middel van identiteitsdiefstal. Met Trojaanse paarden kunnen ze aan alle accountgegevens van een cliënt en kunnen ze ongeautoriseerde geldtransacties naar eigen rekeningen doorsluizen. Ook werken hackers met valse pop-ups die identiek op de homepage van de bank lijken en waardoor nietsvermoedende klanten hun gegevens op de valse pagina invoeren. Een laatste voorbeeld is het fenomeen *phishing*, waarbij hackers een mail naar de cliënten sturen met de mededeling dat de bank een dataverificatie of een update van de gegevens nodig heeft (Wüeest, 2005, p. 4-8; Zahid et al., 2010, p. 45).

In Pakistan werd bij studenten op drie verschillende universiteiten onderzoek naar het gebruik van online banking gedaan. Daaruit bleek dat studenten het platform sneller aanvaardden als ze zeker waren van de veiligheids- en privacymaatregelen, maar dat ze zich daar niet al te veel zorgen om maakten omdat ze al tevreden waren over hoe de banken dat aanpakten (Zahid et al., 2010, p. 47-50).

3.2.4.2 E-mail

In 2000 werd al aangegeven dat de meeste online problemen aan e-mails gelinkt zijn. Via mail wordt gevaarlijk veel informatie vrijgegeven, zoals bankkaartnummers, rekeningnummers en wachtwoorden van commerciële websites. Enkele voorbeelden die Gibson geeft, zijn het uitwisselen van de pincode van een bankrekening tussen echtgenoten, het sturen van bevestigingsmails met bankkaartnummer en vervaldatum, financiële rapporten naar een accountant en het melden van een weekendje weg, vaak gepaard met een vraag of een vriend of familielid het huis wil nakijken. De reiziger kan in de mail vermelden wat het alarmnummer is of dat de sleutel in de bloempot ligt. Met wat zoeken kan een crimineel in de vorige correspondentie misschien zelfs het thuisadres van de reiziger terugvinden (Fox et al., 2000, p. 13; Gibson, 2002).

Schneider waarschuwt dan weer voor beledigende mails, spam, virussen, worms en *phishing* (zie infra). Die kunnen leiden tot diefstal van persoonlijke en/of financiële gegevens bij banken, e-

commerce, telefoonmaatschappijen en overheidsinstellingen (Fox et al., 2000, p. 13-14; Schneider, 2002).

Enkele maatregelen die Gibson aanraadt om de privacy te beschermen, zijn de volgende: een gebruiker moet zijn e-mail als publieke informatie behandelen. Wat iemand niet aan een beller zou vertellen, moet hij ook niet in een mail zetten. Hij moet zich dus bewust zijn van de gevaren. Een gebruiker kan eventueel als oplossing de informatie doorfaxen of de mail coderen door middel van een programma zoals *Pretty Good Privacy* (PGP), dat voor particulier gebruik geschikt is (Gibson, 2002).

In Amerika is er in de in 2001 opgestelde *USA Patriot Act* een sectie over onlinecommunicatie die de naam *The Pen Register Statute* meekreeg. Dat betekent dat, net zoals bij telefoonverkeer, kan worden nagegaan wie met wie contact heeft. De inhoud van de communicatie mag niet vrijgegeven of bekeken worden, maar de ISP-nummers wel. Daarbij moet de gebruiker ook weten dat de header van een e-mail niet privé is, wat ook voor de grootte van de bijlagen geldt. De gebruiker moet dus een lagere verwachting van privacy hebben als hij mailt, of anders moet hij de mail coderen (Newell, 2011, p. 36-45).

3.2.4.3 Skype

Het gebruik van Skype, een *Voice over Internet Protocol* (VoIP), is niet zonder gevaren en kan tot een inbreuk van persoonlijke veiligheid leiden. Via Skype kunnen per ongeluk virussen en malware gedownload worden en kunnen gebruikers met pedofielen in contact komen. Verder kan Skype voor iemands privacy gevaarlijk zijn. Een indringer kan zich als iemand anders voordoen (zoals een vriend, familielid of een Skypemedewerker) en zo iemands persoonlijke gegevens opvragen die hij vervolgens kan misbruiken. Ook geeft Skype informatie aan overheidsinstanties als ze ernaar vragen. Daarom wordt het aangeraden om nooit een adres of telefoonnummer op het Skypeprofiel te plaatsen (Simmons, 2012).

3.2.4.4 Datingsites

Bij datingsites gaat het vooral om complete vreemden die elkaar online ontmoeten. Het grootste gevaar dat gebruikers op zulke sites lopen, is dat iemand een verkeerde persoon ontmoet. Meestal gaat dat gepaard met het gebruik van een valse identiteit. De gebruiker kan dan slachtoffer worden van identiteitsdiefstal, fraude, cyberstalking, seksueel misbruik of huiselijk geweld. Wat ook kan gebeuren, is dat pedofielen via de gebruiker aan hun kinderen kunnen geraken en hen misbruiken. Iemand kan zich beter beschermen door informatie over de andere op te zoeken, en daarvoor zijn er vier verschillende soorten zoekstrategieën: een interactieve door het gesprek met de andere aan te gaan, een passieve waarbij de gebruiker berichten op een centraal forum en het sociale netwerk kan bekijken, een actieve door op informatie van het sociale netwerk van de andere te vertrouwen en extractie,

waarbij de gebruiker een *background check* kan doen door middel van zoekmachines zoals Google (Gibbs et al., 2011, p. 71-81; Haney, 2012).

3.2.4.5 YouTube

YouTube is een programma van Google, waardoor ook die gegevens naar het bedrijf doorgespeeld kunnen worden (zie infra). Bovendien mag mediagigant Viacom sinds 2008 nagaan wat mensen op YouTube bekijken. Viacom belooft dat die de toegang tot de gegevens niet zal gebruiken om personen te vervolgen, maar om te onderzoeken wat er onder copyright beschermd is. Toch kan die verandering als een inbreuk op de privacy worden aangevoeld (Holahan, 2008, p. 11).

3.2.5 De houding van de internetgebruiker en beschermingsstrategieën

Zestien polls die tussen 1998 en 2002 gedaan werden, gaven aan dat bijna tweederde van de respondenten zich veel of toch een beetje zorgen maakte over onlineprivacy. Bovendien hebben die zorgen invloed op het onlinegedrag, waardoor 90% van de internetgebruikers valse gegevens opgaf of weigerde om persoonlijke informatie te geven. Zo vinden gebruikers dat het internet hen manipuleert, waardoor ze dat terug doen en zich bijgevolg veiliger voelen. Toch merkt Zwarun op dat de internetgebruikers daarom niet per se veel over marketingpraktijken, *cookies* of het privacybeleid weten. Verder beweren die gebruikers veel over beschermingsstrategieën te weten, maar passen ze die zelden toe. Een mogelijke verklaring is dat de gebruikers te weinig kennis hebben van *privacy enhancing technologies* (PETs), en ze daarom niet doeltreffend kunnen toepassen. Zwarun geeft aan dat er vast wel internetgebruikers zijn die *cookies* blokkeren en van firewalls gebruikmaken, maar gaat er niet dieper op in (Zwarun, 2007, p. 2-10).

Er zijn drie verschillende soorten strategieën die iemand kan gebruiken om zijn privacy te beschermen. De eerste groep gaat om gedragsstrategieën, zoals foutieve antwoorden geven en anonieme e-mailadressen en pseudoniemen gebruiken. De tweede groep gaat om PETs, dat spam filters, firewalls en antispyware omvat. De laatste groep gaat om meer gecompliceerde PETs zoals encryptietools, anonieme *remailers*, vertrouwenscertificaten, *anonymisers* (software dat de identiteit van een computer verbergt voor websites die de gebruiker op zijn computer bezoekt), *cookie crunchers*, *password managers* of *vaults* en veilige e-mail (Fox et al., 2000, p. 1; Oomen & Leenes, 2008, p. 121-122).

Een beschermingsstrategie die bij de laatstgenoemde groep hoort, is het gebruik van dataprotectieprogramma's: Freenet en *The Onion Router project* (TOR). Met de TOR-software kan een internetgebruiker anoniem surfen. Zijn gegevens worden gecodeerd over het net gestuurd doordat hij gebruik maakt van verschillende servers. Dat verhindert dat de identiteit van de TOR-gebruiker

wordt gevonden. Zulke softwareprogramma's worden ook *zero-knowledge networking systems* genoemd. Een ander nuttig programma is *Collusion for Firefox* of *Collusion for Chrome*. Dat programma spoort de *cookies* van sites op die alle bewegingen op het internet volgen en bijhouden. In het begin start de gebruiker met een lege kaart, waarop tijdens het surfen de *cookies* in het rood worden aangeduid. Vervolgens kan de gebruiker beslissen om die al dan niet te verwijderen (Barrett & Strongman, 2005, p. 131; Henry, 2012; Van der Spoel, 2012, p. 27).

Alle bovengenoemde strategieën worden gebruikt om zich tegen indringers te beschermen. Internetgebruikers zien namelijk verschillende vijanden op het internet. Bij de ene gebruiker is technologie de vijand, terwijl het bij de andere de dader achter de technologie is. Als niet het systeem, maar de actoren als vijanden gezien worden, kan de situatie voor de actoren nog veranderen. Zij kunnen namelijk nog het vertrouwen van de internetgebruiker winnen door bijvoorbeeld garanties en bescherming tegen fraude aan te bieden of hun reputatie op te bouwen, zoals de e-commercewebsites (Zwarun, 2007, p. 11-12).

De cijfers rond privacyzorgen in 2002 werden vergeleken met cijfers van 2008. Respondenten zijn, vergeleken met 2002, in 2008 meer bezorgd over de *customization* van hun onlinegedrag en over de controle van hun koopgedrag. Ook maken ze zich zorgen over dat hun persoonlijke identificeerbare informatie (PII, *Personally Identifiable Information*) voor onderzoeks- of marketingactiviteiten gebruikt wordt. Over het gebruik van *cookies* maken ze zich dan weer minder zorgen. Ten slotte wilden ze in 2008 vaker op de hoogte worden gebracht over de beveiliging van hun PII (Antón et al., 2009, p. 1-5).

Uit cijfers van TRUSTe uit 2011 blijkt dan weer dat 60% van Amerikaanse volwassenen meer bezorgd is om hun onlineprivacy en dat 58% niet van doelgericht adverteren (*targeted advertising*) houdt. Verder groeit het vertrouwen in certificaten en zegels. 49% kijkt na of een site een certificaat of een zegel heeft. 90% zegt *browser controls* te gebruiken en *cookies* te verwijderen om zijn privacy te beschermen. Privacy wordt door 94% als een belangrijke zaak bekeken, wat ook in het Verenigd Koninkrijk geldt. In de VS en het VK vertrouwen internetgebruikers vooral zichzelf als het om de bescherming van hun persoonlijke gegevens gaat. Uit het *EU Kids Online Project* in 25 Europese landen blijkt dan weer dat amper 1% van de kinderen tussen negen en zestien zich zorgen maakt over het onthullen van persoonlijke gegevens op het internet (Lemmens, 2013; TRUSTe, 2012).

Internetgebruikers zijn zich voldoende bewust van hun privacy en gevaren zoals *targeted advertising* en *cookies*. Toch beschermen nog te weinig gebruikers zich tegen potentieel gevaar, ondanks de ruime keuze aan beschermingsstrategieën en tools. Datzelfde probleem is ook bij sociale media het geval, waarbij jongeren zich te weinig beschermen en te veel vertrouwen in die platformen hebben. In de volgende paragraaf wordt daar dieper op ingegaan.

3.3 Sociale media en privacy

3.3.1 Sociale media: Algemeen

Om te begrijpen waarom sociale media zoals MySpace, Facebook en Twitter een probleem kunnen vormen, moet eerst dieper ingegaan worden op wat sociale media nu precies zijn. Boyd en Ellison geven in hun artikel 'Social Network Sites: Definition, History, and Scholarship' een heel duidelijke definitie.

> Social network sites are web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system (Boyd & Ellison, 2008, p. 211).

Er bestaan natuurlijk verschillende soorten sociale netwerken, die door de organisatie *Privacy Rights Clearinghouse* worden opgelijst. Zo zijn er persoonlijke netwerken zoals Friendster, MySpace en Facebook (met gedetailleerde profielen waarmee gebruikers informatie met anderen kunnen delen en vriendschappen kunnen sluiten), status updatenetwerken zoals Twitter (voor het posten van korte statussen met een beperkt aantal tekens), locatienetwerken zoals Foursquare (voor het aangeven van een real-timelocatie), *content-sharing networks* zoals YouTube en Flickr (voor het delen van muziek, foto's en video's) en *shared-interest networks* zoals LinkedIn (voor professionele relaties en voor mensen met dezelfde hobby's, scholing, politieke voorkeuren, etnische achtergrond, religie, seksuele voorkeur, enzovoort) (Privacy Rights Clearinghouse, 2012).

In 2006 startten Hutton en Fosdick een onderzoek naar de globalisatie van sociale media. Al hun bevindingen publiceerden ze in 2011. Ze vonden onder meer dat sociale netwerken de dominante kracht in sociale media zijn. Die stegen van 2006 tot 2010 van 27% tot 74% en die stijging werd een globale beweging, waarbij 61% over 54 landen een profiel op een sociale netwerksite heeft. In oktober 2012 bereikte Facebook de kaap van een miljard gebruikers, en in België zijn er 4,5 miljoen Belgen met een Facebookaccount en 200.000 met een Twitteraccount (Demeyer, 2012; Hutton & Fosdick, 2011, p. 564; X., 2012).

3.3.2 Sociale netwerken, privacy en privacyovertredingen

De meeste websites zetten in hun privacybeleid dat ze persoonlijke informatie verzamelen, waardoor de gebruiker kan zien waarvoor hij toestemming geeft. Dat kan problematisch zijn omdat veel gebruikers dat privacybeleid niet lezen en bijgevolg toestemming geven terwijl ze dat misschien niet willen. Het beleid vermeldt het gebruik van de informatie, hoe het verzameld wordt, eventueel het gebruik van *cookies*, aan wie de informatie doorgegeven kan worden en de veiligheidsmaatregelen die

de site neemt om de gegevens te beschermen. Het beleid is afhankelijk van de wet die in een land van toepassing is. Zo is er een verschil tussen de Europese en de Amerikaanse databeschermingswetten (Tuunainen, 2009, p. 6).

De organisatie *Privacy Rights Clearinghouse* toont op haar site alle zaken die bij sociale netwerken komen kijken. Zo waarschuwen ze dat informatie die een gebruiker deelt vaak voor anderen zichtbaar is zonder de gebruiker zich daarvan bewust is. Dat is onder andere te wijten aan het feit dat weinig gebruikers van het privacybeleid van het sociale netwerk op de hoogte zijn en omdat de sociale netwerksite regelmatig zijn beleid wijzigt zonder dat aan de gebruikers te melden. Ook werken de sociale netwerken samen met derde partijapplicaties (zoals games, polls, quizzen en software waarmee een gebruiker met zijn gsm op een sociaal netwerk terecht kan), die daardoor probleemloos aan informatie van gebruikers kunnen. Ze geven daarbij aan dat ze niet kunnen garanderen dat de derde partij hun privacy respecteert (Privacy Rights Clearinghouse, 2012).

Bovendien gebruiken sociale netwerksites *cookies*, waarmee ze alle internetactiviteiten van de gebruiker kunnen volgen. Als gevolg daarvan kan het gedrag en de persoonlijkheid van de gebruiker geconstrueerd worden. In 2011 is Facebook daarvoor nog in opspraak gekomen omdat de *cookies* zelfs na het uitloggen de gebruiker bleven volgen. De privacy kan ook door de gebruikers zelf bedreigd worden, omdat ze informatie vrijgeven in hun netwerk waaronder ook minder gekende "vrienden" zitten en die ze in het echte leven niet zouden vertrouwen. Afhankelijk van de sociale netwerksite kunnen profielen volledig te zien zijn zonder dat iemand een connectie is. De profielen van Friendster en Tribe.net kunnen via zoekmachines volledig worden getoond. Bij LinkedIn en Facebook kan de gebruiker zelf instellen wat al dan niet zichtbaar is (Privacy Rights Clearinghouse, 2012; Tuunainen et al., 2009, p. 2-4).

Adverteerders kunnen van sociale netwerken profiteren. Sociale netwerken zoals Facebook verkopen informatie van hun gebruikers aan adverteerders door, zodat die op maat gemaakte advertenties naar een gebruiker kunnen doorsturen. Dat proces, dat ook wel *Social Media Advertising* of *targeting* wordt genoemd, is heel voordelig voor de adverteerder, omdat de gebruiker dan meer geneigd zal zijn om een bepaald product aan te schaffen. Op 25 januari 2011 lanceerde Facebook de feature *Sponsored Stories*, waarmee advertenties gebruikmaakten van de *likes* van vrienden van een gebruiker. Als een vriend een bepaald kledingmerk leuk vindt, kan er op de nieuwspagina van de gebruiker in de marge met de advertenties staan dat vriend X het merk Y leuk vindt. Facebook is daarvoor voor de rechter gedaagd en moest in een overeenkomst het privacybeleid aanpassen door expliciet een regel over publiciteitsrechten toe te voegen ("This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information" (Jennings, 2012, p. 3)). Verder moet de gebruiker de keuze krijgen om die feature al dan niet uit te schakelen en

worden enkele regels voor de bescherming van jongeren onder achttien jaar toegevoegd (Desmyttere, 2012; Jennings, 2012, p. 2-3; Privacy Rights Clearinghouse, 2012).

Als adverteerders aan persoonlijke informatie kunnen, kan de overheid dat natuurlijk ook. Heel wat organisaties hebben richtlijnen opgesteld over hoeveel informatie er geraadpleegd en gebruikt kan worden, maar die richtlijnen zijn soms vaag. Zo kan de informatie zelfs in rechtszaken worden gebruikt en kunnen werkgevers sociale netwerken raadplegen om meer informatie over hun werknemers te weten te komen (Privacy Rights Clearinghouse, 2012).

Vrienden van Facebookgebruikers moeten zich bewust zijn van wat ze allemaal op de sociale netwerksite plaatsen. *Comments* op het prikbord van een vriend, het delen van video's en links… Zulke zaken zijn ook voor anderen zichtbaar. Facebookgebruikers kunnen wel kiezen wat ze zichtbaar maken voor wie. Zo is er de keuze tussen informatie tonen aan 'niemand', 'alleen vrienden', 'enkelen van mijn netwerk en al mijn vrienden' en 'al mijn netwerken en al mijn vrienden'. Wat een gebruiker altijd in het achterhoofd moet houden, is dat de informatie die een gebruiker op een sociale netwerksite post eigendom van de site wordt. De gebruiker doet dus afstand van zijn rechten (Tuunainen et al., 2009, p. 8).

Steeds meer zorgen over privacy steken de kop op, en dan vooral als het om minderjarigen gaat. Onderzoeker Barnes spreekt bij de jongeren over een *privacy paradox*: tieners willen hun privacy wel beschermen, maar "ze zijn zich niet bewust van de openbare aard van het internet". Dat gegeven kan verder onderzocht worden. We kunnen de vraag stellen of de huidige jongeren, die al heel vertrouwd zijn met het internet en zulke kwesties al in de media zijn tegengekomen, al meer bewust zijn van hun privacy en of ze er veilig mee omspringen (Boyd & Ellison, 2008, p. 221-222).

3.3.3 Incidenten

De *Beacon feature* op Facebook veroorzaakte in 2007 heel wat opschudding. Gegevens van externe websites werden naar Facebook gestuurd zodat vrienden de aankopen van een gebruiker konden zien. In de rechtbank werd een minnelijke schikking getroffen en in november 2009 werd de toepassing stopgezet (Zansberg & Fischer, 2011, p. 30).

In 2009 werd Twitter omwille van misleidende praktijken voor het gerecht gedaagd. De sociale netwerksite voldeed niet aan de veiligheidsnormen terwijl het bedrijf van wel beweerde. In 2011 werd een akkoord bereikt (Zansberg & Fischer, 2011, p. 30).

In september 2012 braken in het Nederlandse Haren rellen uit nadat een meisje een uitnodiging van een feestje per ongeluk op 'openbaar' had gezet. Dat kwam omdat ze een privacyinstelling was

vergeten aan te vinken. Dat was niet de eerste keer dat zoiets gebeurde. Sinds 2010 is het al in Engeland, Duitsland en Australië voorgekomen (Opgenhaffen, 2012).

Ondanks de fouten die Facebook bij nieuwe ideeën kan maken, introduceerde de site een nieuwe toepassing die doet denken aan de asymmetrische relaties op Twitter. Facebookgebruikers kunnen, als de persoon het toelaat, zich op anderen abonneren en vervolgens statusupdates en dergelijke te zien krijgen zonder met elkaar bevriend te zijn. Verder wil Facebook een nieuwe toepassing invoeren met de naam GraphSearch. Door middel van dat zoekprogramma op Facebook kunnen gebruikers op een bepaalde plaats of met een bepaalde interesse, muzieksmaak of hobby elkaar terugvinden door in de zoekmachine korte zinnen te combineren. Daarbij gaat het niet alleen om mensen binnen de gebruiker zijn netwerk, maar ook om mensen buiten dat netwerk. Maar Zuckerberg verzekert het publiek dat alleen wat al toegankelijk op Facebook is, in de resultaten getoond wordt.

3.3.4 De houding van gebruikers van sociale media

Recent onderzoek toonde aan dat jongeren vandaag meer persoonlijke gegevens delen dan in 2006 of 2012 (Madden et al., 2013, p. 2). Dat kan gevaarlijk zijn, omdat jongeren weinig over privacyrisico's weten en zich niet bewust zijn van de hoeveelheid informatie die ze aan al dan niet bekende personen aanbieden. Ook weten ze meestal niet welke soort data van hen verzameld wordt, hoeveel, waar die opgeslagen wordt en voor hoe lang en voor wat die gebruikt zal worden. De meeste gebruikers lezen het privacybeleid en de gebruiksvoorwaarden niet omdat dat moeilijk is en veel tijd kost. Daardoor weten ze bijvoorbeeld niet dat derden hun informatie kunnen krijgen. Maar ook als ze het weten, maken ze zich er niet al te veel zorgen over. In een studie van Madden en collega's bij Amerikaanse tieners, zegt slechts 9% zegt heel bezorgd te zijn. De jongeren zijn zich echter wel van privacysettings bewust en weten hoe ze die moeten gebruiken, maar velen nemen de moeite niet om de instellingen aan te passen en laten die op de standaardinstellingen staan, die overigens gericht zijn om zo veel mogelijk informatie te tonen. Sociale netwerken moedigen de gebruiker namelijk aan om zo veel mogelijk informatie te geven. Een kleine minderheid heeft zelfs geen weet van die beschermingsmogelijkheden. Sommige gebruikers maken zich soms meer zorgen over wie hun gegevens ziet en hoe die verspreid worden in plaats van zich zorgen te maken over waarom die gegevens verspreid worden. Ten slotte kunnen de verwachtingen ten opzichte van privacy verschillen naargelang de leeftijd en de culturele en geografische normen (Madden et al., 2013, p. 2; Newell, 2011, p. 17; Tuunainen et al., 2009, p. 4-7; Walrave et al., 2012; Zansberg & Fischer, 2011, p. 26).

Op sociale media kan een gebruiker gegevens afschermen en enkel voor een kleinere kring beschikbaar maken. Voor een grotere groep is ook mogelijk, maar een gebruiker zal zelden bewust iets voor een algemeen publiek onthullen. 60% van de Amerikaanse tieners houdt het profiel privé, en de

meesten hebben er vertrouwen in dat ze hun privacysettings goed aanpassen (Madden et al., 2013, p. 2). Toch verwacht de gebruiker soms onterecht dat die informatie binnen een netwerk zal blijven en dat het netwerk de informatie beschermt: "Many, perhaps even the majority, of users of social networks consider their information open only to those within their circle of contacts, no matter how large that circle may be" (Zansberg & Fischer, 2011, p. 28).

Er is een verschil tussen *digital immigrants* (personen die niet met internet opgroeiden) en *digital natives* (personen die wel met internet zijn opgegroeid). De *immigrants* behandelen internet als openbaar, terwijl de *natives* verwachten dat wat ze posten onder degenen blijft die het mogen zien en dat technologische grenzen hun gegevens tegen ongewenste personen beschermen. Daardoor zullen adolescenten eerder *oversharen* dan volwassenen. Ze geven veel meer persoonlijke informatie en hebben laksere privacysettings. Ze zullen sneller informatie vrijgeven in ruil voor beloningen (zoals zelfontplooiing en feedback van anderen) en zijn bijgevolg minder bezorgd over hun privacy dan volwassenen. Ook onder druk van *peers* zullen adolescenten meer onthullen. Hoe ouder een adolescent wordt, hoe bewuster hij zich van zijn privacy wordt (Newell, 2011, p. 18-19; Walrave et al., 2012; Zansberg & Fischer, 2011, p. 30).

In het rapport van Madden, die in 2012 bij Amerikaanse gebruikers (2.277 volwassenen van 18 jaar en ouder) een survey deed, zijn er de volgende bevindingen: vergeleken met 2009, beperken de sociale netwerkgebruikers meer de toegang tot hun profielen en onderhouden ze hun profiel meer. Zo schrappen ze personen uit de vriendenlijst (63% vs. 56%), untaggen ze foto's van zichzelf (37% vs. 30%) en verwijderen ze commentaren van anderen op hun profiel (44% vs. 36%). 58% beperkt de toegang van zijn profiel (alleen voor vrienden), en vrouwen beperken meer dan mannen (67% vs. 48%). Bijna de helft van gebruikers (48%) vindt het moeilijk om zijn privacy te beheren, en 2% heel moeilijk (Madden, 2012).

In de volgende twee paragrafen wordt er specifieker ingegaan op de sociale netwerksites Facebook en Twitter. Aangezien de platformen een groot aantal gebruikers hebben (zie infra) en ze regelmatig het onderwerp van onderzoek zijn, is het interessant om na te gaan wat er in de bestaande literatuur met betrekking tot privacy al over geschreven is.

3.3.4.1 Facebook

Facebook maakt heel wat gebruik van persoonlijke gegevens. Ten eerste hanteert de sociale netwerksite een *real name policy*: om een profiel te kunnen aanmaken, moet de gebruiker zijn echte naam aan het account koppelen. In 2006 ontstond de *News Feed*, die alle activiteiten van vrienden onder elkaar toont en die heel wat kritiek kreeg. Dat gebeurde ook bij de invoering van de Like-knop in april 2010 omdat die knop toont welke interesses vrienden hebben. In 2012 waren de laatste nieuwigheden de *ticker*, die de real-time activiteiten van vrienden weergeeft, en de tijdlijn. Verder

geeft de sociale netwerksite de gebruikers de mogelijkheid om informatie te geven over favoriete muziek, films, boeken, gelezen artikelen van bepaalde kranten, adressen, telefoonnummers en e-mailadressen, scholen, werkgevers, enzovoort. Tegenwoordig kunnen gebruikers hun account koppelen aan de muziekstreamingsdienst Spotify, zodat vrienden kunnen zien welke muziek de gebruiker beluistert. De gebruiker geeft bijgevolg een schat van informatie aan Facebook, maar door het ondoorzichtige privacybeleid dat Facebook en veel andere sites hebben, bedreigt de gebruiker zelf zijn privacy (Van der Spoel, 2012, p. 16-49).

Veltsos en Veltsos zijn zich van de gebrekkige informatie over het privacybeleid bewust. "Facebook received a lot of criticism in 2010 for changing its privacy policy and sharing information that users thought was private", schrijven ze. Facebookgebruikers blijken vrij gemakkelijk persoonlijke informatie vrij te geven, zelfs wanneer ze weten dat ze de toegang ervan kunnen beperken. Als reden wordt gegeven dat ze zich niet van de risico's bewust zijn en denken dat die onlinenetwerken veilig zijn. Zo zijn er tal van gebruikers wier profiel op 'openbaar' staat (Butler et al., 2011, p. 44; Tuunainen et al., 2009, p. 2-3; Veltsos & Veltsos, 2010, p. 465).

In 2009 werd het privacybewustzijn bij Finse Facebookgebruikers onderzocht. De meerderheid gaf alleen toegang aan hun vrienden, maar ze maakten zich niet al te veel zorgen over hun privacy op sociale media, omdat ze de andere gebruikers in het sociaal netwerk leken te vertrouwen. Vergeleken met het internet in het algemeen toonden ze meer zorgen dan wanneer het alleen om Facebook ging. Veel gebruikers vertrouwden Facebook met hun informatie en de meerderheid heeft haar privacyinstellingen aangepast. Een kleine minderheid beweerde het privacybeleid van Facebook gelezen te hebben, maar de 61% daarvan wist niet dat derde partijapplicaties hun informatie van Facebook krijgen. Onder alle ondervraagde respondenten was 55% daar niet van op de hoogte en 71% wist niet dat Facebook volgens het privacybeleid gegevens aan externe derde partijen mag geven voor commerciële doeleinden. Als conclusie gaven de onderzoekers aan dat de Finse Facebookgebruikers heel veel informatie over zichzelf vrijgeven en dat ze, ondanks dat ze anders denken, zich niet bewust zijn van wat ze allemaal tonen aan personen in hun netwerk die ze niet noodzakelijk goed kennen. Het privacybeleid is door de meerderheid niet gekend, wat duidelijk werd bij het noemen van derde partijen (Tuunainen et al., 2009, p. 8-15).

Iets meer dan de helft van de Amerikaanse tieners zegt meer positieve dan negatieve online-ervaringen te hebben (Madden et al., 2013, p. 2). Bovendien kunnen de voordelen van Facebook opwegen tegen de potentiële gevaren en risico's op privacyinbreuken. Zo was er een jongen die twee keer een gehackt profiel had gehad, maar toch naar Facebook bleef terugkeren. Gebruikers zagen eerder die risico's bij anderen gebeuren, waardoor er mogelijk van een *third-person effect* kan worden gesproken. Gebruikers pasten verder sneller hun privacysettings aan als ze zelf een privacyinbreuk ondervonden.

Als het bij anderen gebeurde, waren ze minder snel geneigd om hun instellingen aan te passen (Debatin et al., 2009, p. 94-95).

In 2011 werd er nagegaan of er een verband was tussen het constant veranderende privacybeleid van Facebook en het privacybewustzijn van de Facebookgebruikers waardoor ze hun privacysettings aanpasten. Bij elke verandering worden de gebruikers op de hoogte gebracht door een klein dialoogvenster bovenaan hun startpagina met daarin een link naar verdere informatie over de verandering. In het onderzoek werd bestudeerd of gebruikers dan ook echt de tijd namen om op die link te klikken en te lezen wat veranderd was. Grimmelman (2010) had namelijk aangetoond dat bij een privacybeleidsverandering in december 2009 maar 35% zijn privacyinstellingen aangepast had. De overige 65% ging ofwel volledig akkoord met de verandering, ofwel was die zich niet van de verandering bewust. "Users care deeply about privacy settings, but they have a great trouble achieving it", schrijven Butler en collega's. Verder merken ze op dat gebruikers heel wat informatie delen, en dat ze vertrouwen lijken te hebben dat Facebook een "veilig platform" is (Butler et al., 2011, p. 40-45).

Butlers team maakte gebruik van een survey en een inhoudsanalyse van de respondenten hun Facebookprofielen. In het totaal hadden ze een steekproef van 235 respondenten over de 18 jaar. 102 respondenten lieten de onderzoekers toe om hun profiel bekijken om na te gaan of hun antwoorden over privacybewustzijn en de privacyinstellingen van hun profiel consistent waren (Butler et al., 2011, p. 46-49).

14% van de respondenten was op de hoogte van de laatste versie van het privacybeleid, 17% van de respondenten las het privacybeleid toen ze hun account aanmaakten, maar zijn zich niet van de laatste versie bewust. 27% las enkel delen ervan, 29% had het niet gelezen, maar wist het indien nodig wel te vinden. 12% had het niet gelezen en wist ook niet waar te zoeken als het nodig zou zijn. De meerderheid was dus gedeeltelijk of helemaal niet op de hoogte van Facebooks huidige privacybeleid, al beweerde ze dat ze bewust was van het privacybeleid van de sociale netwerksite en was ze ervan overtuigd dat de site haar gegevens goed beschermt (Butler et al., 2011, p. 49-50).

Bij de inhoudsanalyse gaf 65,7% van de respondenten toe dat ze niet op de hoogte bleven van de veranderingen in het privacybeleid van Facebook, en ze waren zich ook niet van hun privacyinstellingen bewust. 12,7% van de respondenten zei dat ze de veranderingen volgden en dat ze zich ook van hun instellingen bewust waren. "Thus, it can be inferred that a relationship exists between the efforts users make to keep up with Facebook's changing privacy policies, and the levels of awareness they retain of their personal privacy settings", besluiten Butler en collega's in hun resultaten. Door de vele veranderingen zijn veel gebruikers zich niet van hun privacy bewust, en als gebruikers de tijd niet nemen om van de veranderingen op de hoogte te blijven, zijn er inconsistenties tussen de privacysettings die ze denken te hebben en de werkelijke settings (Butler et al., 2011, p. 52-53).

3.3.4.2 Twitter

Twitter is moderne versie van een blog, een onlinedagboek waarop een blogger alles kan zetten wat hij wil. Om zijn privacy te beschermen, kan hij gebruikmaken van een of meerdere pseudoniemen. En omdat het een publiek sociaal netwerk is, kan een *tweep* beter eerst nadenken over wat hij al dan niet post. Twittergebruikers bestaan uit twee verschillende *content camps*: de meerderheid focust op zichzelf terwijl een kleinere groep meer gericht is op het delen van informatie. Omdat de standaardinstellingen van Twitter op openbaar staan, kan het vrijgeven van een locatie soms tot inbraken leiden. *Tweeps* zijn minder met de bescherming van privacy bezig en bij de meeste *tweeps* zijn de *tweets* openbaar. Uit onderzoek blijkt dat *tweeps* niet vaak expliciet vermelden wanneer ze waar zijn en ze delen bijna nooit persoonlijke identificeerbare informatie op Twitter. Slechts 3% deelde informatie over zichzelf en over de tijd en plaats. In de discussie geven Humphreys en collega's aan dat ze de "Twitter users' conceptions of their audience" niet volledig begrijpen. Ook halen ze aan dat het interessant kan zijn om te onderzoeken of *tweeps* een ander beeld van hun publiek hebben dan gebruikers op andere sociale netwerksites (Humphreys et al., 2010, p. 1-18; Kobayashi, 2012, p. 59-69; Naaman et al., 2010, p. 191-19).

3.3.5 Bedreigingen en gevaren op sociale media

Uit verschillende studies blijkt dat sociale media zwak zijn in hun beveiliging en dat ze gemakkelijk aan te vallen zijn. Bij de verklaringen die worden gegeven, blijkt het vooral aan de gebruiker te liggen die zich niet al te bewust is van de gevaren en privacyrisico's en bijvoorbeeld te snel vriendschapsverzoeken aanvaardt, commentaren op iemands prikbord post, personen tagt op foto's, te veel informatie[1] vrijgeeft, enzovoort. Het kan ook aan het privacybeleid liggen, dat complex wordt opgesteld, of door een complexe interface en de gebruiksonvriendelijke richtlijnen. Doordat alle informatie door één provider wordt gecentraliseerd en de veiligheid en de privacy niet als prioriteit worden gezien, wordt de beveiliging verzwakt (Cutillo et al., 2009, p. 95; Hasib, 2009, p. 288-291).

Hasib verdeelt mogelijke bedreigingen in vier verschillende groepen. De eerste groep gaat om privacygerelateerde bedreigingen, zoals onder andere het maken van een digitaal dossier van een gebruiker, *face recognition* en de moeilijkheid om informatie weer van het net te verwijderen. De nadelige gevolgen van die problemen kunnen stalking, chantage, laster en het verlies van controle over de gegevens zijn. Iemand kan bijvoorbeeld ook zijn baan verliezen door een beledigende status over zijn baas te schrijven die hij nadien niet meer kan verwijderen. De tweede groep gaat om de sociale

[1] Persoonlijke informatie zoals naam, leeftijd, geslacht, adres, foto's, enzovoort (Hasib, 2009, p. 289). Debatin et al. geven het voorbeeld van het vrijgeven van adressen en lessenroosters, wat het gemakkelijker maakt om iemand te stalken (Debatin et al., 2009, p. 86).

netwerksites (SNS) zelf, die aangevallen kunnen worden door spammers, virussen en *SNS Aggregators*. Gevolgen bij zulke aanvallen zijn bijvoorbeeld *phishing attacks*. *SNS Aggregators* zijn applicaties met een zwakke authenticatiemethode, waardoor gebruikers het slachtoffer van identiteitsdiefstallen kunnen worden. De derde groep zijn de identiteitsgerelateerde bedreigingen, waardoor de gebruiker door *phishing* en informatielekken zijn paswoorden, bankkaart- en rekeningnummers bekendmaakt of overstelpt wordt met spamberichten. Ook kunnen gebruikers het slachtoffer worden van valse profielen, waardoor de reputatie van de gebruiker door het slijk wordt gehaald. De vierde en laatste groep gaat om sociale bedreigingen, zoals cyberpesten, inbraken thuis (door vakantieplannen online te zetten) en stalking on- of offline. Zelfs bedrijven kunnen hier problemen door ondervinden als hun bedrijfsnetwerken worden gehackt en er gevoelige informatie wordt vrijgegeven (Hasib, 2009, p. 289-291; Walrave et al., 2012; X., 2011).

Jennings brengt het begrip *twitterjacking* ter sprake, wat betekent dat een gebruiker zich registreert op naam van een beroemdheid en valse berichten onder die naam plaatst. Dat kan negatieve gevolgen voor het slachtoffer hebben, zoals het schaden van de reputatie. In 2008 loste Twitter dat probleem op door geverifieerde accounts aan onder andere beroemdheden, politici, sportlui en bedrijven toe te wijzen. Al kunnen sommige accounts toch heel misleidend blijven, waardoor een vals account toch door Twitter wordt geverifieerd. Zo werd het valse account van de hockeyspeler T.J. Oshie geverifieerd als het officiële account en werd in België de Vlaamse actrice Veerle Baetens ook al slachtoffer van *twitterjacking* (Dka & Hmp, 2012; Jennings, 2012, p. 5-11; Jung, 2011, p. 403-404).

3.3.6 Strategieën om de privacy te beschermen

Hasib geeft verschillende aanbevelingen om de veiligheid te vergroten. Enkele voorbeelden: de gebruiker moet zich bewust zijn van alle informatie die hij over zichzelf vrijgeeft, hij moet de privacyinstellingen best zo veel mogelijk aanpassen, en niet op de standaardinstellingen laten staan die ingesteld zijn om zo veel mogelijk openbaar te laten staan, en hij moet opletten voor spelletjes en quizzen, omdat die applicaties vaak (onnodig) gebruik maken van persoonlijke gegevens. Verder kan de wetgeving rond sociale netwerksites herzien en verbeterd worden waar mogelijk. Veltsos & Veltsos raden aan om het privacybeleid en de gebruiksvoorwaarden van een dienst te bekijken. Belangrijk is dat een gebruiker zich ervan bewust is dat alles op het internet permanent is: “What students say today online could cost them jobs later” (Bradley, 2009, p. 110-112; Hasib, 2009, p. 292; Veltsos & Veltsos, 2010, p. 464).

Jurgenson en Rey omschreven twee praktijken die bepaalde sociale mediagebruikers uitoefenen, namelijk *social steganography* en *white-walling*. Bij *social steganography* plaatsen gebruikers statussen openbaar die niet voor iedereen begrijpelijk of betekenisvol zijn, maar enkel voor een select

aantal vrienden. Als voorbeeld geven ze het posten van een liedjestekst. Voor bepaalde mensen is dat gewoon een liedje, maar de groep 'in the know' kunnen ervan afleiden dat de persoon in kwestie een pijnlijke breuk achter de rug heeft (Jurgenson & Rey, 2011, p. 289).

Het concept *white-walling* geeft aan dat een gebruiker heel wat informatie over anderen en zichzelf post, maar alles op een gegeven moment verwijdert. Het ene moment is de gebruiker heel openbaar, terwijl hij op een ander moment zich heel bewust is van zijn privacy. De *white-waller* is niet gelijk aan de *limited user*, die beperkt wat hij op het internet zet en bijgevolg risico's op schending van de privacy al van in het begin vermijdt (Jurgenson & Rey, 2011, p. 289).

Ook derde partijen kunnen een bedreiging vormen. Daarvoor is de gesplitste veiligheidsprotocol OAuth een oplossing. OAuth is ontworpen voor gebruikers die hun informatie met derde partijen willen delen zonder hun gebruikersnaam en paswoord te moeten geven. Sociale media zoals Facebook en Twitter maken er gebruik van, maar ook andere sites beginnen het meer en meer te gebruiken (Dannen & White, 2011, p. 11-12).

Ten slotte worden er regelmatig nieuwe alternatieven verzonnen. Zo is er Safebook, een sociaal netwerk waarin de informatie niet door één instantie wordt verzameld, maar door meerdere onafhankelijke instanties waarbij de relaties tussen de gebruiker en de instanties, in het onderzoek *peer-to-peer architectures* genoemd, op vertrouwen gebaseerd is. Verder is er de site AdjustYourPrivacy.com. Die site verzamelt alle belangrijke privacyinstellingen voor meerdere diensten, zodat een gebruiker van op die pagina voor alle diensten tegelijk dingen op 'opt out' kan zetten. Ook proberen Facebookgebruikers soms hun privésfeer te beschermen door een openbare fanpage op hun naam aan te maken, waarbij ze onder een pseudoniem een tweede profiel aanmaken waarop ze al hun gegevens kwijt kunnen en bepaalde zaken privé kunnen houden (Cutillo et al., 2009, p. 95-101; Gordon, 2012; Rainey, 2012, p. 21).

Studenten maken eerder gebruik van een zwakke verdedigingsstrategie, omdat velen denken dat het aanpassen van de privacyinstellingen voldoende is. Er wordt te weinig rekening gehouden met het feit dat zichzelf beschermen ook inhoudt dat de gebruiker niet zomaar iedereen als vriend moet aanvaarden, dat hij er bepaalde criteria voor gebruikt en dat hij de hoeveelheid informatie die hij over zichzelf geeft, beperkt is. Studenten maken ook gebruik van een psychologische strategie, waarbij ze de bedreigingen in een betekenisvolle en onbedreigende context zetten. Zo kan het kennen van de identiteit van de indringer een gevoel van controle en geruststelling geven (Debatin et al., 2009, p. 99-103).

Vanuit de gedachte van het kennen van de indringers hun identiteit kan een nieuwe onderzoeksvraag gesteld worden: wie zien studenten dan allemaal als indringers?

3.4 Apps en privacy

Op de veelgebruikte sociale media worden er ook tal van apps aangeboden. Een voorbeeld is het spelletje FarmVille op Facebook. FarmVille is een derde partijapplicatie die Facebook in het privacybeleid vermeldt. Zulke applicaties kunnen een inbreuk op de privacy zijn. Ze vragen namelijk persoonlijke gegevens op voordat de gebruiker die app mag gebruiken. En zelfs als de gebruiker geen gebruik van de app maakt, kan de app via vrienden (die de app wel gebruiken) aan de nodige informatie geraken.

Ook op smartphones en iPads zijn apps heel populair. Toch zijn er verscheidene apps die op het randje van 'eng' balanceren. Zo is er de afgevoerde app *Girls Around Me*, waarmee iemand kan zien welke jongens en meisjes in zijn buurt zijn. *Background Check* laat de gebruiker toe om alle criminele feiten, sociale netwerkinformatie, eigendomsgegevens, en dergelijke van eender wie na te gaan. Voor de ouders is er de app *Stealth SMS Parental Control*, waarmee ouders, na het installeren van de app op de smartphone van hun kind, alle binnenkomende en uitgaande berichten van hun kind kunnen lezen (Palis, 2012).

In januari 2013 was er heel wat heisa rond Instagram. De app, die in 2012 door Facebook overgenomen werd, onderging een verandering in het privacybeleid waarin stond dat het bedrijf het recht had om foto's van gebruikers te verkopen. Dat stuitte op een storm van protest, waarna Facebook meteen besloot om het beleid aan te passen waarin het duidelijker wordt wat er met de foto's kan gebeuren (Beaubien, 2013, p. 6; Shaer, 2012).

Facebook werkt intussen aan een app die "voortdurend de locatie van gebruikers bijhoudt". Als vrienden van een gebruiker in de buurt zijn, waarschuwt de app de gebruiker. Die app moet eerst geactiveerd worden, maar na de activering blijft de app op de achtergrond werken, waardoor de app niet telkens opnieuw geactiveerd moet worden. De uitvinding is niet nieuw. Er bestaan al zulke apps, zoals Glympse en Highlight (Stevens, 2013).

3.4.1 Attitudes van de gebruikers

Bij smartphonegebruikers identificeert 42% privacy en veiligheid als prioriteit, waarbij 85% van de gebruikers een app niet zal downloaden als die de app niet vertrouwt. Amper 14% gelooft dat mobiele *app stores* enkel betrouwbare apps verkopen die de privacy beschermen. 62% van de smartphonegebruikers zijn zich ervan bewust dat adverteerders hun mobiele activiteiten volgen en slechts 1% vindt dat leuk. Minder dan 10% wil zijn specifieke locatie, surfgedrag, thuisadres of contactlijst onthullen (TRUSTe, 2012).

Onderzoek van het PEW Research Center geeft cijfers over Amerikanen hun gsm- en smartphonegebruik. 54% van de eigenaars die apps gebruiken hebben al beslist om een app niet te

installeren als ze ontdekten hoeveel persoonlijke gegevens ze zouden moeten geven om die te mogen gebruiken. 30% heeft al een app van zijn gsm verwijderd omdat het informatie verzamelde die gebruikers liever voor zichzelf hielden. In datzelfde onderzoek bleek ook dat 32% van de gsm-eigenaars zijn zoekgeschiedenis verwijderd had en dat 19% de *location tracking feature* op zijn gsm uitgeschakeld had uit angst dat individuen of bedrijven die informatie zouden verzamelen. In het onderzoek wordt kort het probleem van een gebrek aan transparantie aangekaart. De *Federal Trade Commission* ontdekte dat het privacybeleid van apps helemaal niet transparant was. De grootste appverdelers (Apple, Google, Microsoft, Amazon en Hewlett-Packard) hebben in 2012 besloten om hun privacybeleid van apps duidelijker te verwoorden (Boyles et al., 2012, p. 2-8).

3.5 Geïnteresseerden in persoonlijke gegevens

Achter alle privacyinbreuken zitten natuurlijk actoren. Ook daaronder zijn er verschillende instanties te onderscheiden. In de literatuur en media zijn adverteerders, werkgevers, overheden en hackers veelgenoemde gevaren voor de privacy. Maar onderzoek toont ook aandacht voor minder evidente actoren, zoals familie en vrienden (Debatin et al., 2009; West et al., 2009). Bovendien wijst het busongeval in Sierre op privacyschendingen door journalisten, een groep die zeker niet onderschat mag worden.

3.5.1 Commerciële bedrijven en websites

In het bedrijfsleven is het verzamelen van informatie belangrijk. Via een klantenkaart van de Colruyt kan het concern informatie verzamelen en op maat gesneden reclamefolders naar de klant sturen. Die praktijk wordt nu ook gretig op het internet gebruikt (Luyten, 2010, p. 13).

"In tegenstelling tot de offline wereld beschikken marketeers online over een extra manier om persoonlijke informatie over de individuele consument te verzamelen", luidt het in het rapport 'E-marketing & minderjarigen' van het Observatorium van de Rechten op het Internet (2011, p. 128). Gegevens kunnen via meegedeelde informatie, zoals elektronische formulieren, en elektronische voetafdrukken (door middel van *cookies*) verzameld worden. Zo kunnen verkopers hun aanbod beter op een individuele consument afstemmen. Een voorbeeld is de boekensite Amazon, een commerciële website die *cookies* gebruikt om bestellen te versnellen en om op basis van een gebruikersprofiel aanbevelingen te doen. Ook Zalando maakt gretig gebruik van *cookies*, waardoor de gebruiker tijdens het surfen in advertenties de schoenen te zien krijgt die hij voordien op de schoenensite bekeken heeft. Dat fenomeen heet *retargetten*, en betekent dat iemand na het verlaten van een site met een banner er terug naartoe gelokt wordt. De gepersonaliseerde reclame wordt bovendien in de advertentie rechtsboven aangegeven met een blauw driehoekje (►) (Deckmyn, 2013; Fox et al., 2000, p. 7; Walrave et al., 2011, p. 128).

Commerciële websites kunnen een bedreiging voor klanten vormen, omdat die sites steeds meer persoonlijke informatie vragen. Een nadeel daarvan is dat er inbreuken op privacy kunnen optreden en dat er steeds meer klanten bang zijn om de controle over hun gegevens te verliezen. Een survey toonde in 2010 aan dat 87% van de Amerikanen ongerust zijn over de veiligheid van hun persoonlijke informatie op het internet (Cha, 2011, p. 613-614).

Ten slotte beschermt een privacybeleid op de site niet noodzakelijk de privacy. Onlinediensten kunnen hun eigen regels overtreden en staan zelf machteloos tegenover hackers, die maar al te graag het vertrouwen van de klant misbruiken. *Phishing* is namelijk gebaseerd op de visie dat er bij e-commerce vertrouwen tussen de klant en de onlineverkoper ontstaat. De klant krijgt een e-mail van de verkoper

die hij vertrouwt, waarin gevraagd wordt om persoonlijke informatie te geven. Zo kunnen kredietkaart- en rekeningnummers en dergelijke geroofd worden en kunnen malware en spyware de computer binnendringen (Beatty et al., 2011, p. 14:9-14:10; Cha, 2011, p. 628-629).

3.5.1.1 Incidenten

Preneel waarschuwt voor een massief bewakingssysteem waardoor alles en iedereen in de gaten wordt gehouden, en ook voor de zwakke plekken van een dergelijk systeem. Als voorbeelden geeft hij Sony, het bedrijf dat in 2011 de persoonlijke gegevens en kredietkaartgegevens van meer dan 100 miljoen gebruikers verloor, en giganten zoals Apple, Google en Microsoft, die bekenden dat ze locatiegegevens van hun gebruikers een lange termijn bijhielden. Verder kunnen databanken van bedrijven fouten bevatten waardoor er informatielekken ontstaan. In het najaar van 2012 stonden gegevens van gebruikers van zonnepanelen online en werd er op 1 januari 2013 een lek bij de NMBS vastgesteld, waardoor de gegevens van ongeveer 1,5 miljoen klanten een aantal maanden onbeschermd op het internet stonden. NMBS wordt er nu voor vervolgd. Het is de eerste keer in België dat een 'data breach'-dossier naar het gerecht wordt doorgestuurd (Preneel, 2012, p. 18-19; Van Belle, 2012; Vanhecke, 2013; Van der Spoel, 2012, p. 33).

3.5.1.2 Attitude van de consument

Volgens meerdere studies lezen consumenten zelden het privacybeleid van websites (Cha, 2011, p. 615). In een survey van 2006 bedroeg het aantal slechts 20%. Ook vermelden meerdere studies dat de wil om informatie te geven afhankelijk is van het type informatie dat gevraagd wordt. Zo zijn telefoon- en rekeningnummers, inkomen en medische gegevens informatie die consumenten liever niet geven. De angst voor matige beveiliging van geldtransfers en kredietkaartgegevens bij online shoppen kan als een rem werken om online spullen aan te kopen. Hoe hoger de risico's, hoe minder zin iemand zal hebben om online te kopen (Liao & Cheung, 2001, p. 299-305).

Walrave gaf dan weer aan dat er bij e-commercewebsite interesse is in jongeren als een doelgroep. Zeven op de tien tieners geven sneller persoonlijke informatie, zoals lievelingsproducten en -winkels, hobby's en geslacht, als ze in ruil een geschenk krijgen. Daar staat tegenover dat maar drie tot vier op de tien tieners hun eigen contactgegevens (telefoonnummer en gsm, thuisadres) geeft. Ook de contactgegevens van ouders en vrienden worden meer beschermd, net zoals het beroep van de ouders. Ongeveer de helft van de tieners zou wel hun e-mailadres geven in ruil voor een geschenk (Walrave et al., 2011, p. 129-130).

Belgische jongeren tussen de twaalf en achttien jaar staan wel sceptischer tegenover websites die data verzamelen. 72,8% vraagt zich af waarom websites die gegevens nodig hebben. 69,2% maakt zich zorgen om de verwerking van die gegevens, 73,5% zoekt informatie over het beleid van de

informatieverwerking voordat ze gegevens doorgeven en 60,6% heeft toegegeven dat ze al eens opzettelijk foutieve informatie hebben doorgegeven (Walrave & Heirman, 2011, p. 21).

Maar ondanks die sceptische houding onthullen jongeren vrij snel persoonlijke gegevens over zichzelf voor marktgerichte doeleinden. Ze zullen wel eerder *profile data* (voornaam, leeftijd, geslacht, hobby's, favoriete producten en winkels) doorgeven dan *contact data* (thuis- en e-mailadres van zichzelf en ouders, telefoon- en gsm-nummer). Hoe meer zorgen jongeren zich over hun privacy maken, hoe minder snel ze bereid zijn om persoonlijke informatie te onthullen. Vrouwelijke tieners maken zich meer zorgen om hun privacy en geven bijgevolg minder informatie op het internet vrij. Jongens doen het dus meer, maar zij geven ook vaker foutieve informatie op hun profielpagina (Walrave & Heirman, 2011, p. 14-22).

In de VS is 85% van de burgers zich bewust van het fenomeen *online behavioural advertising* (OBA) en 61% is sneller geneigd om zaken te doen met bedrijven die de klant de keuze geven om het OBA uit te schakelen. 35% is gestopt met zaken doen door privacyzorgen. In het VK gaat het om 29%. 79% van de burgers van het VK zijn zich van het OBA bewust en 53% houdt er niet van, al zou 55% sneller geneigd zijn om met een bedrijf zaken te doen als die de mogelijkheid geven om dat uit te schakelen. 42% van de consumenten gelooft dat PII gelinkt is aan het OBA, maar als PII niet aan het OBA gelinkt is, stijgt de welwillendheid tegenover het OBA van 17% naar 30% (TRUSTe, 2012).

3.5.2 Overheden

Sinds 11 september 2001 is het privacylandschap heel wat veranderd. Terwijl privacy voordien heel belangrijk was, vinden burgers het niet erg om in ruil voor veiligheid hun privacy op te geven. De overheid mag ons bijgevolg controleren of aan *cybersnooping* doen als we in ruil tegen terrorisme beschermd worden. Dat is mogelijk omdat de burgers vertrouwen hebben in de overheidsinstellingen en hun ambtenaren (*informational trust*). Ze zijn ervan overtuigd dat die instellingen informatietransfers veilig en beschermd zullen houden, met als gevolg dat ze sneller zullen toegeven om zich te laten controleren (Nisbet & Gay, 2007, p. 8).

Toch haalt Brynko in haar artikel enkele cijfers aan om haar stelling "Today, people are worried about Big Brother tracking their digital footprints" te ondersteunen. Uit onderzoek van het *Center for the Digital Future* op de *University of Southern California* blijkt dat 48% van de internetgebruikers van zestien jaar en ouder zich zorgen maakt over *corporate intrusion*, waarbij bedrijven hun activiteiten op het internet nagaan. Angst voor controle van de overheid geldt voor 38% van de gebruikers (Brynko, 2011, p. 11).

Gebruikers van sociale media kunnen zich zorgen maken over hun gegevens die ze op hun sociale netwerken zetten. Zo is het bijvoorbeeld geweten dat de fiscus profielen opzoekt om te controleren of de levensstijl wel past met wat er op de aangifte vermeld staat. De fiscus gebruikt daarbij Facebook en andere netwerksites, maar eBay gebruikt hij het meest. In 2007 zijn een wildplasser en zelfs een getuige tot een boete veroordeeld in een zaak waarin Facebook is gebruikt. De getuige beweerde dat hij die wildplasser niet kende. De politie ging vervolgens op Facebook na of dat waar was en vond de wetsovertreder in de vriendenlijst van de getuige. De getuige kreeg, net als de overtreder, een boete omdat hij het onderzoek vertraagd had (Debatin et al., 2009, p. 85; Van Leemputten, 2009).

Controle door de politie kan tot bezorgdheid over privacy leiden. De politie heeft namelijk de bevoegdheid om informatie online na te trekken om misdaden te verkomen of op te lossen. In Amerika heeft de *New York Police Department* zelfs een officiële *media monitoring branch*, waarin de agenten de taak hebben om Twitter en Facebook te volgen om informatie te verzamelen (Zansberg & Fischer, 2011, p. 32).

Toch is hun bevoegdheid niet oneindig, zoals de zaak Marcel vs Metropolitan Police aantoonde (zie infra). Telefoontap mag alleen in ernstige gevallen gebruikt worden, zoals terrorisme, mensenhandel, drugszaken en afpersing. Computertap is zelfs enkel toegelaten in gevallen van verdenking van terrorisme. In 2000 kwam de *Federal Office of National Drug Control Policy* in opspraak nadat aan het licht kwam dat *cookies* gebruikt werden om na te gaan wie informatie over drugs opzocht. Aangezien het op een illegale manier gebeurde, werd besloten dat *cookies* op overheidssites niet gebruikt mogen worden. In januari 2013 was er dan weer ophef rond een mishandeling in Eindhoven. Acht jongemannen trapten een weerloze jongen in elkaar. Dat werd allemaal gefilmd, maar die opname bood na twee weken speuren geen resultaat. Daarom verspreidde de politie het filmpje via sociale media. Twee dagen later werden de daders geïdentificeerd, maar werd er ook een ware heksenjacht op de daders gestart waardoor er discussie ontstond over de werkwijze van de politie (Fox et al., 2000, p. 5; Luyten, 2010, p. 10; Neyt, 2013; Trudel, 2009, p. 319).

Een ander punt van discussie ontstond in januari 2013. Toen kwam het omstreden bericht dat Amerikaanse spionnen dankzij de *Patriot Act* zonder het bevel van een rechter de *cloud* van elke Europeaan mogen volgen. Het gaat dan wel alleen om data die bij een Amerikaans bedrijf zijn ondergebracht ("één link met Amerika is voldoende om alle gegevens van iemand te mogen blootleggen"). Alle gegevens die online worden opgeslagen, zoals mail, Facebook, Googlezoekopdrachten en Dropbox kunnen worden bekeken. Het is niet de eerste keer dat Amerika zich met Europa bemoeit. In 2006 kwam de SWIFT-affaire aan het licht. In die affaire werd ontdekt dat de CIA inzage heeft in de databanken van SWIFT, een internationale verkeersregelaar met 8.300 bankinstellingen over overheidsklanten uit 128 landen. De reden voor die inzage was dat de CIA onder de Europese burgers terroristen wilde opsporen. De mogelijkheid om data in de *cloud* op te slaan

dankzij programma's zoals Dropbox en Microsoft Skydrive, zorgen ook in Europa weer voor extra discussie over de bescherming van de gegevens (Luyten, 2010, p. 14; Vanhecke, 2013).

Rond het project Echelon is er dan weer heel wat geheimzinnigheid. Het project van de *U.S. National Security Agency* scant al het internetverkeer (e-mail, chat rooms, en nu ook waarschijnlijk sociale media), alle (langeafstands)telefoongesprekken, faxen, elektronische signalen van communicatiesatellieten, *pager signals*… Kortom, alle vormen van elektronische communicatie. Echelon maakt gebruik van Engelse sleutelwoorden zoals 'bomb', 'gun', 'militia', 'Delta Force' en 'explosive'. In een halfuur kan Echelon een miljoen *message inputs* verwerken, maar enkel 10 van de 1 miljoen *inputs* worden gedetailleerd geanalyseerd. Verder wordt er over het project weinig losgelaten. Enkel twee fragmentarische documenten werden vrijgegeven onder de federale *Freedom of Information Act*, die slechts uit zeven zwaar gecensureerde pagina's bestaan. Het is ook niet duidelijk of alleen criminelen of alle burgers worden gescreend (Wallace, 2000, p. 66).

E-Government is een informatie- en communicatietechnologie om de diensten en handelingen te verbeteren voor burgers, bedrijven, en andere overheidsinstellingen en werkt via elektronische kanalen zoals SMS, internet en mail. Vertrouwen is een van de meest belangrijke aspecten om E-Government te kunnen invoeren, en die bestaat uit twee dimensies: vertrouwen in de overheid en vertrouwen in het internet (Al-Jaghoub et al., 2010, p. 1-4).

Maar in het *Benchmarking Security and Trust in the EU and US report* uit 2003 blijkt dat individuele zorgen over veiligheid en vertrouwen in de elektronische diensten tot gebrek aan vertrouwen leiden, waardoor toepassing van E-Government verhinderd wordt. Voor 74% van de Europese burgers was het bewustzijn van veiligheidsmaatregelen op websites een belangrijke factor om te beslissen om online transacties te voeren of om online te handelen (Colesca, 2009, p. 8-13).

3.5.3 Hackers

Hackers zijn in deze paper al meerdere keren genoemd. De grote meerderheid van computergebruikers zal waarschijnlijk wel van dat gevaar bewust zijn. Vaak hebben hackers met financiële fraude te maken, al staan ze ook regelmatig in de kranten als ze overheidsinstellingen aangevallen hebben. Zo vermeldde de Vlaamse krant *De Standaard* op februari 2013 de aanval van cyberspionnen op België. In België ging het om vier computers die besmet waren met MiniDuke, een programma dat de harde schijf binnenvalt en cyberspionnen toelaat om documenten bij overheden te stelen. Bij vijftig overheden en instituten in ruim twintig landen werden computers aangevallen. Via een lek in het pdf-programma Adobe Reader kregen de hackers het programma verzonden. Als het slachtoffer dan het document in pdf opende, werd de MiniDuke geïnstalleerd. Opvallend bij die aanvallen was dat de

sociale netwerksite Twitter gebruikt werd. Andere recente slachtoffers zijn Twitter zelf, Facebook, Apple, *Wall Street Journal* en *The New York Times* (Deckmyn, 2013).

3.5.4 Professionele relaties en privérelaties

Als internetgebruiker moet iemand zich ervan bewust zijn dat ook potentiële werkgevers alle openbare informatie over hem op het internet en op sociale media kunnen terugvinden. Er zijn namelijk werkgevers die zulke informatie gebruiken om op basis daarvan iemand aan te werven. Onderzoek in 2006 toonde aan dat 63% van de werkgevers kandidaten afgewezen heeft op basis van de informatie op profielen van sociale netwerken. Zo kunnen werkgevers problemen vermijden als de werknemer niet geschikt blijkt te zijn. Sprague haalt hierbij het begrip *negligent hiring* aan, waarbij een werkgever de verantwoordelijkheid moet dragen voor het risico dat hij neemt of voor potentiële schade die hij aanricht als de werknemer niet in zijn werkomgeving past. Het internet is daarbij een handig hulpmiddel geworden (Genova, 2009, p. 98; Sprague, 2009, p. 398-400).

3.5.4.1 De houding van een jongvolwassene tegenover professionele relaties en privérelaties

Op sociale media kunnen dingen verschijnen die een gebruiker misschien liever niet toont. Daarom is het van belang dat een gebruiker zich bewust is van de openbaarheid van zijn gegevens op zulke media. Gênante foto's en beledigende statussen kunnen tot negatieve gevolgen leiden. Zo was er eind april 2013 een relletje rond de Vlaamse weerman Luc Trullemans op de Waalse zender RTL. Hij werd ontslagen nadat hij racistische uitspraken op Facebook had gemaakt.

Maar in Californië is er een wet ingevoerd die werknemers tegen werkgevers beschermt. Werknemers die door hun (potentiële) werkgever gedwongen worden om hun gebruikersnaam of paswoord te geven, het profiel te openen in aanwezigheid van de werkgever of het vrijgeven van informatie op het sociale platform, zijn nu tegen zulke wanpraktijken beschermd. Alleen bij onderzoek naar misdragingen en overtredingen van een werknemer mag dat nog wel als bewijs gevraagd worden. Die wet komt er na meerdere incidenten waarbij de werkgever de inloggegevens van een potentieel werknemer opvraagt. Velen durven dat niet te weigeren omdat ze anders de baan kunnen mislopen. Ook bij een school voor atleten werden de studenten gedwongen om een coach als vriend toe te voegen, waarna de school alles in de gaten kon houden (Rainey, 2012, p. 19-21; Tochner, 2012, p. 18).

In de Verenigde Staten mogen werkgevers werknemers controleren, maar dan wel met het medeweten van de werknemer. In Europa is dat ook het geval, al zijn ze daar veel strenger en zijn er meer regels omtrent die kwestie. Wel moeten de werknemers daar geen verwachting van privacy hebben als ze e-mail en internet op het werk gebruiken (Deschenaux, 2010, p. 99-104).

Ook de houding van studenten tegenover Facebookvrienden werd al onderzocht. Daarbij werd nagegaan in welke mate studenten oudere volwassenen, waaronder hun ouders, als vrienden aanvaardden en hoe studenten tegenover zulke (potentiële) vriendschappen stonden. Zestien studenten, zeven jongens en negen meisjes tussen 21 en 26 jaar, werden daarvoor geïnterviewd (West et al., 2009, p. 616-619).

De meerderheid van de studenten zag de komst van ouders op de sociale netwerksite als ongewenst en wilde aparte werelden. Redenen waren schaamte, sociale normen en zorgen over hun moeder. Voor het aspect schaamte werd het voorbeeld gegeven van een jongen die bang was dat zijn moeder beschamende berichten op zijn prikbord zou posten. Bij sociale normen werd er aangegeven dat er grenzen nodig zijn. Zo was er een studente die het raar zou vinden om haar moeder als een vriendin te zien. Verder zouden hun ouders in hun wereld binnendringen, en zouden ze op beschamende dingen, zoals dronken foto's, kunnen stuiten, iets wat een student liever voor zijn ouders verborgen houdt. Daardoor verliest de student zijn rol als tussenpersoon. De student kan als tussenpersoon beslissen wat hij aan zijn ouders vertelt en wanneer zijn ouders met zijn vrienden omgaan. Als zijn ouders op Facebook zouden zitten, zouden ze alles over hem te weten kunnen komen en kunnen ze zonder de student zijn toestemming contact leggen met zijn vrienden. Het laatste aspect gaat om het verlangen om de moeder tegen inbreuk van vrienden te beschermen. Studenten zouden het bijvoorbeeld niet leuk vinden dat hun vrienden jeugdfoto's van hun moeder konden zien (West et al., 2009, p.620-622).

Wat opviel in het onderzoek, was dat studenten spontaan ook naar werkgevers verwezen als ze het over Facebook hadden. Een aantal studenten houdt het liefst informatie voor de werkgever verborgen en heeft de toegang tot persoonlijke gegevens beperkt. Dat is ook het geval voor collega's. Onder de studenten is er duidelijk een bewustzijn van de mogelijkheid dat werkgevers, collega's en zelfs docenten hun gegevens kunnen zien. Daardoor letten ze op wat er allemaal op hun profiel te zien is omdat ze hun carrièremogelijkheden niet willen verknallen. Het kan interessant zijn om na te gaan in welke mate dat bewustzijn ook bij de andere potentiële geïnteresseerden het geval is. Tot slot beseffen studenten dat hun gegevens openbaar staan, maar zij verstaan dat vooral als openbaar voor 'hun publiek'. Tegenover hun ouders is die publieke sfeer een privésfeer, ondanks de openbaarheid van de gegevens. Daaruit kan geconcludeerd worden dat de grenzen tussen privésfeer en publieke sfeer op sociale netwerken onduidelijker worden (Debatin et al., 2009, p. 98; West et al., 2009, p. 623-625).

Ten slotte moet er rekening worden gehouden met het concept vrienden. Wie verstaan gebruikers van sociale netwerksites zoals Facebook onder vrienden? Het kan namelijk van hechte vrienden tot oppervlakkige kennissen en zelfs complete vreemden gaan. Onderzoek van 2009 toonde aan, door middel van surveys bij 119 studenten op een Amerikaanse universiteit, dat 10% eender wie als vriend accepteerde, 37% aanvaardde personen die hij kende van "horen zeggen" en 52% aanvaardde mensen die de studenten persoonlijk kenden. Vrienden op Facebook werden niet noodzakelijk als vrienden in

het echte leven gezien, waardoor het interessant kan zijn in hoeverre gebruikers al hun vrienden op Facebook bijvoorbeeld vertrouwen en wie ze eventueel als een potentiële indringer kunnen zien (Debatin et al., 2009, p. 87-97).

Maar ook echte vrienden en partners kunnen iemands privacy schenden. In november 2010 werd Joshua Ashby veroordeeld nadat hij als wraakactie naaktfoto's van zijn ex-vriendin op Facebook had gezet (zie infra). Gebruikers moeten zich bewust worden van potentieel gevaar van familie, vrienden en kennissen, die evengoed met hun gegevens aan de haal kunnen gaan.

3.5.5 Journalisten

Door de opkomst van de sociale media maken journalisten steeds meer gebruik van zulke media. Ze kunnen dienen als research- en presentatietechnieken en zorgen ervoor dat een journalist een persoon binnen het uur kan vinden. Hoewel sociale media voor journalisten dus als informatievergaring kunnen dienen, moet hier ook rekening worden gehouden met de privacy van anderen. Sir William Blackstone, een reactionair van de achttiende eeuw die de *English common law* samenstelde, zei bijvoorbeeld dat de persvrijheid niet misbruikt mag worden. Zo mogen journalisten de burgerrechten niet schenden of de publieke of huiselijke orde verstoren (Opgenhaffen & Van Belle, 2012; Smith, 2008, p. 81).

3.5.5.1 Journalisten en privacy

Deltour geeft aan dat de journalisten de beroepsplicht hebben om verslag uit te brengen over de actualiteit omdat het publiek recht heeft op informatie. Maar er zijn natuurlijk enkele tegenwaarden waar de journalist zich aan moet houden, zoals privacy. Deltour schrijft dat een journalist wel informatie moet geven, maar daarbij niet noodzakelijk moet zeggen over welke personen het gaat. "De journalist moet steeds zorgvuldig nagaan of en in welke mate hij 'herkenbaarheidsinformatie' vrijgeeft", zegt hij. Met het vrijgeven van namen, persoonsgegevens zoals adres, nationaliteit of seksuele geaardheid of afbeelding, moet voorzichtig worden omgegaan (Deltour, 2003, p. 5-6).

3.5.5.2 Journalisten en privacy online

Door de komst van de digitale media is het medialandschap heel wat veranderd. Zo kan door middel van digitale media en sociale netwerken essentiële informatie uitgewisseld, bronnen gezocht, fouten verbeterd en interconnectiviteit bij het publiek gecreëerd worden (Whitehouse, 2010, p. 310). Uiteraard zijn er ook nadelen aan verbonden. Er is geen controle over wat er allemaal op het internet kan worden gezet, waardoor er ethische vragen over de privacy kunnen worden gesteld. Daarvoor zijn er richtlijnen nodig, maar Whitehouse zegt wel dat vaste grenzen onmogelijk zijn (Whitehouse, 2010,

p. 311), omdat elke zaak anders is en van de context afhangt (Whitehouse, 2010, p. 313). Een context kan namelijk helpen bij het maken van ethische keuzes. Als voorbeeld geeft Whitehouse de keuze tussen de waarheid aan het licht brengen door middel van liegen of misleiding (Whitehouse, 2010, p. 313). Hier is dus conflict tussen twee deugden: eerlijk onderzoek naar iets doen waarbij de journalist toch niets bezwarends zal vinden of als journalist liegen om aan de waarheid te komen. Met andere woorden: moet een deugd voor het hogere goed soms verloochend worden? Die keuze moest de Australische journalist Chris Masters maken. Hij wilde de corruptie van de politie in de Australische staat Queensland aantonen, maar dat ging niet via de eerlijke manier. Dus plaatste hij verborgen camera's en audiorecorders in het bureau. Zo geraakte hij aan voldoende bewijsmateriaal waar hij anders nooit aan zou hebben gekund om de ernstige corruptie aan het licht te brengen. Die case duidt op het feit dat misleiding soms nodig is om het goede te bereiken (Quinn, 2007, p. 171).

Een andere zaak toont aan dat misleiding niet altijd mag worden gebruikt. De krant *The Spokesman Review* onderzocht of de vorige *Spokane Mayor* Jim West regelmatig chat rooms voor homo's bezocht en kinderen pijn had gedaan. Daarvoor maakten ze gebruik van een federale forensische expert die met pensioen was en die zich als een *high school student* voordeed om zo te zien of de berichten wel degelijk van West kwamen. De krant vond enkel bewijs dat burgemeester afspraken maakte met jongere mannen die hij in chat rooms leerde kennen. Bovendien was er heel wat heisa rond de manier waarop de krant te werk was gegaan, omdat ze met wat meer geduld ook aan voldoende bewijsmateriaal waren geraakt (Whitehouse, 2010, p. 318-319).

Uit die case laat Whitehouse een vraag volgen die een journalist kan helpen om een keuze te maken: "Does the information involve such great public peril that the harm done by journalists failing to engage in deception outweighs the harm the deception will bring to individuals, the profession, and the public trust (Whitehouse, 2010, p. 320)?"

Daarenboven bestaan er internetgebruikers die zich helemaal niet bewust zijn van wat anderen allemaal over hen kunnen zien (Whitehouse, 2010, p. 312). Die opmerking is een interessante invalshoek voor onderzoek. Zo kan bijvoorbeeld onderzocht worden of Vlaamse studenten er zich wel voldoende bewust van zijn wat anderen, waaronder journalisten, allemaal over hen kunnen zien. Bij die kwestie geeft Whitehouse het voorbeeld over Trent Lockett, een inwoner van Tennessee die per ongeluk door zijn twaalfjarige broer werd doodgeschoten terwijl hij zijn broer de scherpschutterskunst aan het aanleren was. Diezelfde tijd werd zijn vader verdacht voor verduistering, wat, net als informatie die van Facebook geplukt was, ook in het artikel vermeld werd. Dat veroorzaakte heel wat kritiek (Whitehouse, 2010, p. 322).

Hieraan kan een laatste vraag en een laatste voorbeeld gekoppeld worden. Tijdens de *Green Revolution* in Iran werd op YouTube een filmpje gepost waarin te zien is hoe een vrouw sterft. Sommige organisaties gebruikten dat filmpje om het geweld aan te klagen, terwijl anderen vonden dat

haar gezicht wazig moest worden gemaakt, omdat haar laatste seconden een inbreuk zijn op haar privacy. De vraag die Whitehouse dan stelt is de volgende: "Is the information gained by reporting from social networking pages worth more than the harm done to the profession and the private pain that pulling information from those pages might bring (Whitehouse, 2010, p. 322-323)?"

Hoewel er voor de gewone media tal van richtlijnen zijn, ligt dat moeilijker bij de digitale en sociale media. Raden verbieden dat journalisten zich online niet anders mogen voordoen in forums en chat rooms, maar soms is het door sociale netwerken onduidelijk om te zien wat nu publiek en privé is (Whitehouse, 2010, p. 315).

3.5.5.3 Case Zwitserland

Op 12 april 2012 was de *Raad voor de Journalistiek* genoodzaakt om een nieuwe richtlijn te introduceren na een golf van kritiek op de mediaberichtgeving over het busongeval in Sierre. Die richtlijn geeft meer informatie aan journalisten over hoe ze voor hun berichtgeving met sociale media moeten omgaan. Hieronder worden de feiten even op een rijtje gezet.

Op 13 maart 2012 botste een Belgische bus frontaal op een muur in de Sierretunnel in Zwitserland. Die bus vervoerde schoolkinderen en begeleiders waarbij 28 doden vielen. Onder dat aantal waren 22 kinderen, 2 chauffeurs en 4 begeleiders van de scholen. Daarenboven raakten 24 kinderen gewond. Dat ongeval werd het zwaarste verkeersongeval in Zwitserland sinds 30 jaar genoemd en lokte wereldwijd de aandacht van de pers. Journalisten betraden de speelplaatsen van de betrokken scholen en kranten, waaronder *Het Nieuwsblad* en *Het Laatste Nieuws*, publiceerden foto's van de minderjarige slachtoffers op de voorpagina. Dat laatste, net als de excessieve berichtgeving en de gehanteerde journalistieke technieken, werd toen het onderwerp van een debat dat op gang kwam nadat familieleden van een slachtoffer bij de *Raad voor de Journalistiek* een klacht hadden ingediend (Cochez, 2012; Wikipedia, 2012).

In de case Zwitserland is er dus duidelijk een overtreding begaan door verscheidene journalisten. Daardoor is de journalistieke code nu uitgebreid met een richtlijn[2] over het gebruik van informatie en beelden afkomstig van sociale netwerksites en persoonlijke websites. Daarbij zal de journalist altijd de aard van de site en het (beeld)materiaal moeten nagaan, net als wie het materiaal op de website heeft geplaatst en of die de toegang tot de pagina's al dan niet beperkt heeft. Maar dat laatste kan eventueel *overruled* worden als er sprake is van voldoende maatschappelijk belang. Wel moet de journalist dat belang kunnen aantonen en moet hij voorzichtig blijven als het om minderjarigen en slachtoffers gaat (Cochez, 2012; RVDJ, 2012).

[2] Zie bijlage 1: De nieuwe richtlijn na de busramp in Zwitserland.

3.5.5.4 Houding van burgers tegenover journalisten

Journalisten hebben de laatste jaren geen al te beste reputatie meer bij de burgers. De redenen zijn de overvloed aan aanbod, schandalen die journalisten blootleggen, schandalen rond de werkwijze van journalisten, de commercialisering, het vergrootte aanbod van negatief nieuws en de nieuwe communicatietechnologieën, waardoor er verschillende media ontstaan (zoals blogs, wiki's, YouTube) en waardoor de grenzen tussen burgerjournalistiek en de professionele journalistiek vervagen (Donsbach et al., 2009, p. 2-3).

Tweederde van de West-Europese bevolking en bijna de helft van de Amerikaanse bevolking betwijfelt de betrouwbaarheid van journalisten. In verkennend onderzoek van Donsbach en collega's is het aantal Duitsers dat journalisten vertrouwt 35%, terwijl 61% wel respect toont. 90% verwacht dat journalisten andere personen respecteren, maar amper een derde denkt dat journalisten dat ook daadwerkelijk doen. Van de Duitse bevolking is er maar 31% dat het werk van de journalisten vertrouwt. In Frankrijk is dat 28%, in Groot-Brittannië 25% en in Nederland 24%. Dat grote gebrek aan vertrouwen kan een aanzet zijn om te onderzoeken in welke mate internetgebruikers met journalisten rekening houden terwijl ze surfen (Donsbach et al., 2009, p. 9-16).

3.6 Besluit

Privacy is vandaag nog steeds een problematisch gegeven. In de huidige maatschappij zijn er twee tendensen om privacy te beschermen: door wetgeving en door zelfregulering. Die laatste is niet altijd even doeltreffend, maar ook in de wetgeving zijn er gaten te vinden waardoor er regelmatig aanpassingen moeten gebeuren. Zo mag de VS dankzij de *Patriot Act* via de *cloud* spioneren en bleek na de busramp in Sierre hoe gemakkelijk journalisten aan persoonlijke informatie geraken.

Internet heeft informatievergaring veel eenvoudiger gemaakt. *Cookies* volgen gebruikers online, Google houdt alles zorgvuldig bij wat iemand in de zoekbalk ingeeft en kan door middel van diensten zoals Gmail, Google+, Google Streetview en YouTube nog aan veel meer informatie geraken. Die informatie kan vervolgens gebruikt worden voor gepersonaliseerde reclame. Ook banken, nieuwssites, webwinkels, datingsites, en dergelijke verzamelen informatie om hun diensten zo goed mogelijk aan de klant aan te passen. En de sociale media zoals Facebook, Twitter, LinkedIn en Instagram zorgen ervoor dat een internetgebruiker helemaal geen geheimen meer heeft.

Een van de problemen rond privacy is dat er nog al te vaak een tekort aan bewustzijn bij de gebruikers is. Het *EU Kids Online Project* in 25 Europese landen toonde aan dat amper 1% van de kinderen tussen negen en zestien zich zorgen maakt over het onthullen van persoonlijke gegevens op het internet (Livingstone et al., 2013). Jongeren, die nochtans als *digital natives* heel vertrouwd zijn met het internet, hebben te weinig kennis over de dataverzameling (hoe, hoeveel, voor hoe lang…), ze lezen het privacybeleid niet, ze veranderen de privacyinstellingen niet en hebben te veel vertrouwen in de veiligheid van de platformen waardoor ze *oversharen*. Bovendien weten ze niet hoe ze zich moeten beschermen. Onderzoek toonde aan dat het aanbod van verschillende strategieën om zichzelf te beschermen er is, maar dat ze zelden of niet toegepast worden (Newell, 2011, p. 18-19; Walrave et al., 2012; Zansberg & Fischer, 2011, p. 30).

Het kan dus interessant zijn om op verschillende onlineplatformen na te gaan hoe jongeren tegenover privacy staan en in welke mate ze van potentiële geïnteresseerden in hun persoonlijke gegevens op de hoogte zijn. De schrijnende case Zwitserland toont namelijk aan dat ook minder vanzelfsprekende partijen, hier journalisten, persoonlijke informatie kunnen misbruiken.

De onderzoeksvragen voor deze paper zijn dus de volgende:

1. Wie zien jongeren als potentiële geïnteresseerden in hun informatie op verschillende onlineplatformen?
2. Welke mogelijke privacybedreigingen zijn er volgens hen per platform mogelijk?
3. In welke mate zijn jongeren zich van hun onlineprivacy bewust?
4. Welke strategieën gebruiken jongeren online om hun privacy te beschermen?

4. Methode

Als methode wordt een onlinesurvey[3] als kwantitatieve methode gekozen. Met een survey kunnen er sneller heel veel respondenten bereikt worden. Online biedt ook voordelen tegenover enquêtes op papier, omdat de respondenten de vervolgvragen nog niet kunnen zien. Daardoor kan de onderzoeker hen zo onbevooroordeeld laten antwoorden en ze leiden naar het punt dat hij wil. Enkele nadelen zijn de representativiteit (misschien krijgen niet alle doelgroepen een even grote kans om de enquête in te vullen), een lage respons en de kwaliteit van de antwoorden. Zo kunnen de respondenten de vragen niet ernstig invullen en is er geen controle mogelijk.

Voor het onderzoek werd de onlinesurvey, opgesteld in het programma Qualtrics, via de schoolmail naar een secundaire school in Sint-Niklaas (ongeveer 800 studenten) en enkele hogescholen van Thomas More gestuurd (ongeveer 800 studenten). De doelgroep bestond dus uit Vlaamse studenten en scholieren tussen de 10 en 26 jaar. Die survey werd van 24 februari 2013 tot 7 maart 2013 afgenomen. Omdat het om een grote survey ging, werd er een beloningssysteem aan vastgekoppeld. De scholieren van de secundaire school maakten kans op een bon van de Standaard Boekhandel ter waarde van 50 euro. Bij de hogeschoolstudenten ging het om een Fnac-bon van 60 euro.

Onlinesurvey: opbouw

De onlinesurvey bestond uit 5 onderdelen: de sociaaldemografische gegevens waaronder het gebruik van onlineplatformen, de waargenomen potentiële geïnteresseerden, de mogelijke waargenomen privacyinbreuken, het privacybewustzijn met beschermingsstrategieën en een vragenset over journalisten en onlineprivacy.

Bij de sociaaldemografische gegevens werd er gevraagd naar het geslacht, de leeftijd, de opleidingsgraad en het gebruik van onlineplatformen. Voor die laatste vraag werd een zevenpuntenschaal opgesteld die van 'nooit' naar 'de hele dag door' ging ((1) nooit, (2) enkele keren per jaar, (3) enkele keren per maand, (4) enkele keren per week, (5) dagelijks (1X per dag), (6) meerdere keren per dag en (7) de hele dag door). Die schaal werd voor platformen gebruikt zoals zoekmachines, mailboxen, chatprogramma's, sociale media, nieuwssites en online banking.

De volgende vragenset over de waargenomen potentiële geïnteresseerden werd gestart met een open vraag die als volgt luidde: ''Als er gesproken wordt over schending van privacy, aan welke soort van mensen of instanties denk je dan? Met andere woorden: wie denk jij dat er geïnteresseerd kan zijn in wat je online doet of welke data je achterlaat om er gebruik of zelfs misbruik van te maken?". Daarbij moesten de respondenten opschrijven aan welke personen of instanties ze spontaan dachten die in hun gegevens geïnteresseerd zouden zijn. Vervolgens kregen ze per platform een lijst van potentiële

[3] Zie bijlage 2: Survey bij scholieren en studenten.

geïnteresseerden, gaande van onder andere de website zelf, hackers, commerciële bedrijven en journalisten. De invulvraag daarbij was de volgende: “In dit deel van de vragenlijst gaan we per platform / onlinetoepassing na in welke mate je denkt dat de volgende personen of instanties geïnteresseerd zijn in wat je op die platformen doet en/of welke data je er achterlaat.” Bij die vraag moesten ze per instantie op een vijfpuntenschaal aangeven in welke mate die instantie in hun informatie geïnteresseerd zou zijn: (1) helemaal niet geïnteresseerd, (2) niet geïnteresseerd, (3) neutraal, (4) geïnteresseerd en (5) heel geïnteresseerd.

Het onderdeel over privacyinbreuken bevatte per platform een lijstje met mogelijke inbreuken zoals fraude, identiteitsdiefstal en doorverkoop aan derde partijen. De respondenten moesten per platform aanvinken welke inbreuk daarop mogelijk zou zijn.

Het privacybewustzijn werd met twee vragen bestudeerd. Bij de eerste vraag moesten de respondenten op een vijfpuntenschaal aanduiden in welke mate ze met een eventuele schending van hun privacy op onlineplatformen rekening houden: (1) helemaal niet, (2) amper, (3) een beetje, (4) veel en (5) heel veel. Bij de tweede vraag moesten de respondenten aanduiden welke strategieën ze gebruiken om hun privacy op het internet te beschermen. Enkele voorbeelden van het lijstje zijn het aanpassen van privacysettings, het verwijderen van *cookies* en letten op wat je schrijft of online plaatst. De respondenten kregen bij het vakje ‘andere’ de mogelijkheid om nog andere strategieën aan te geven.

De allerlaatste vragenlijst had enkel betrekking op journalistiek. Onder andere werd nagegaan of jongeren beseffen dat journalisten hun gegevens kunnen gebruiken. Ook ethische vragen over het gebruik van foto’s en statusupdates in de media werd door middel van concrete voorbeelden bevraagd.

Voor de analyse van de data werd het statistiekprogramma SPSS gebruikt. Daarmee werden beschrijvende en vergelijkende analyses uitgevoerd om eventuele verschillen tussen leeftijd en jongens en meisjes te vinden.

5. Resultaten

5.1 Sociaaldemografische gegevens van de steekproef

In het totaal deden 346 respondenten aan de onlinesurvey mee, wat zorgt voor een *response rate* van 11,25% voor de secundaire school (90 respondenten) en 31,88% voor Thomas More (255 respondenten)[4]. Amper een derde (29,3%) van de respondenten was mannelijk, terwijl de overgrote meerderheid vrouwelijk was (70,7%). De respondenten van de steekproef (N = 346) hebben een gemiddelde leeftijd van 19,62 jaar (M = 19,62; SD = 3,55). De opleidingsgraad is als volgt verdeeld:

Opleidingsgraad	**Aantal (in %)**
Secundair onderwijs	26,1
Hoger onderwijs – professionele bachelor	9,3
Hoger onderwijs – academische bachelor	37,4
Hoger onderwijs – masteropleiding	24,1
Afgestudeerd en aan het werk	2,3
Afgestudeerd en werkzoekende	0,9

Tabel 1. Verdeling van de opleidingsgraad

5.2 Gebruik van de onlineplatformen

Analyse van de data toont aan dat niet alle platformen evenveel gebruikt worden. In onderstaande tabel is af te lezen hoe vaak de verschillende platformen die in de enquête genoemd werden, gebruikt worden:

DAGELIJKS TOT DE HELE DAG DOOR (%)	
Zoekmachines	92,1
Facebook	83,5
(Web)mail	80,3
Schoolsites	58,3
YouTube	47,4
Nieuwssites	47,0
ENKELE KEREN PER WEEK OF PER MAAND (%)	
Chatprogramma's	41,8
Online banking	41,1
NOOIT (%)	
Koopplatformen	37,3
Downloadplatformen	39,3
Apps	40,5
Streaming muzieksites (vb. Spotify, Deezer)	58,6
Fora	62,3
Blogs	63,2
Twitter	68,2
Fotoplatformen (vb. Instagram, Flickr)	72,8
LinkedIn	82,0
Foursquare	91,5

Tabel 2. Frequentie van gebruik onlineplatformen

[4] Eén respondent gaf geen opleiding op en is bijgevolg niet in de berekening van de *response rate* opgenomen, waardoor het een steekproef van 345 respondenten wordt.

5.2.1 De invloed van leeftijd en geslacht op gebruik

Om eventuele verschillen tussen jongens en meisjes te vinden, werd er gebruik gemaakt van onafhankelijke T-testen. Bij de meeste onlineplatformen is er in gebruik geen significant verschil tussen jongens en meisjes. Al treden er verschillen op bij Facebook, schoolsites, YouTube, fora, apps, muzieksites en downloadsites (zie tabel 3). Meisjes gebruiken vaker Facebook en schoolsites dan jongens. Jongens gebruiken dan weer meer Youtube, meer fora, meer apps, meer muzieksites en meer downloadsites dan meisjes.

	Meisjes M	**Meisjes SD**	**Jongens M**	**Jongens SD**	**t(…) = …**	**p**
Facebook	5,61	1,362	5,14	1,842	t(146,064) = -2,294	0,023
YouTube	4,53	1,149	5,01	1,321	t(339) = 3,357	0,001
Fora	1,67	1,178	2,41	1,770	t(136,831) = 3,831	0,000
Schoolsites	4,80	0,964	4,54	1,136	t(342) = -2,107	0,036
Apps	2,91	2,024	3,70	2,076	t(343) = 3,270	0,001
Muzieksites	2,02	1,535	2,54	1,921	t(155,553) = 2,418	0,001
Downloadsites	2,22	1,315	2,89	1,624	t(156,855) = 3,676	0,000

Tabel 3. Invloed van geslacht op gebruik

Met een meervoudige regressieanalyse werd nagegaan welke eigenschappen als predictoren fungeren. Dat wordt in de onderstaande tabel weergegeven.

Platform	**Leeftijd**			**Geslacht (Man = 1, Vrouw = 2)**		
	β	t	p	β	t	p
Zoekmachine	0,196	2,198	0,029	-0,147	-2,835	0,005
(Web)Mail	0,324	3,840	0,000			
Chat						
Facebook				0,133	2,434	0,015
Twitter						
Linkedin						
Foursquare						
Youtube				-0,187	-3,435	0,001
Fotoplatform						
Nieuwssite	0,246	2,947	0,003	-0,161	-3,329	0,001
Blog						
Forum				-0,260	-4,911	0,000
Koopplatform						
Online banking	0,530	6,888	0,000			
Schoolplatform						
App				-0,133	-2,547	0,011
Streaming muzieksite				-0,130	-2,385	0,018
Downloadsite	0,283	3,118	0,002	-0,213	-4,017	0,000

Tabel 4. Invloed van leeftijd en geslacht op gebruik

De predictor leeftijd toont aan dat, hoe ouder iemand is, hoe vaker hij platformen gebruikt. En uit de resultaten blijkt dat meisjes meer Facebook (communicatie) en schoolsites (educatie) gebruiken,

terwijl jongens meer voor entertainment op het internet zitten (muziek, video's en spelletjes). De factor 'opleiding' is niet in de analyse opgenomen, omdat het om een nominale variabele ging en omdat uit de analyses geen duidelijke invloed op te meten was.

5.3 Waargenomen potentiële geïnteresseerden

Uit de antwoorden op de open vraag blijkt dat zowel de scholieren als de studenten heel inventief zijn. Allen noemen heel uiteenlopende geïnteresseerden. Toch is er een groot aantal (99 van de 346 respondenten) dat vraag 11 heeft opengelaten, namelijk bijna een derde (28,6%). Daaronder heeft 69,7% van de vrouwen niet geantwoord, tegenover 29,3% van de mannen (de respondent zonder het aangegeven geslacht heeft ook die vraag opengelaten). Dat geeft een vertekend beeld omdat er meer vrouwelijke respondenten waren: Op het totaal van de vrouwen heeft maar 28,3% van de vrouwen niet geantwoord, bij de mannen gaat het om 28,7%. Er is dus geen noemenswaardig verschil, net zoals bij de opleidingsgraden (N = 345): secundair onderwijs (middelbare school) (37,8%), hoger onderwijs – professionele bachelor (28,1%), hoger onderwijs – academische bachelor (27,1%), hoger onderwijs – masteropleiding (20,5%), afgestudeerd en aan het werk (37,5%) en afgestudeerd en werkzoekende (33,3%). Eén respondent speelde vals door alle genoemde onlineplatformen in de enquête op te sommen. Dat antwoord is niet in de resultaten opgenomen.

In de spontane antwoorden is er een heel gamma aan potentiële geïnteresseerden gegeven, maar toch valt het op dat vooral de meest bekenden het vaakst worden genoemd. Die zijn onder andere de criminelen (zoals hackers, pedofielen, fraudeurs), het sociale netwerk Facebook, de zoekmachine Google, de overheid en politie, toekomstige werkgevers, commerciële bedrijven en de daaraan verbonden adverteerders. Wanneer de geïnteresseerden echter worden opgelijst, verschillen de resultaten soms aanzienlijk. Die verschillen worden in de volgende paragraaf uitgebreid besproken.

De jongeren somden ook minder evidente geïnteresseerden op, zoals familie, vrienden, ex-liefjes en journalisten. Bovendien worden er twee categorieën genoemd waar in het onderzoek zelf niet aan werd gedacht. Daarbij gaat het om (academisch) onderzoek en auteursrechtenorganisaties. Voor de categorie '(academisch) onderzoek' worden onderzoeksbureaus en onderzoekers (2,4%), (communicatie)wetenschappers (0,8%), informatici (0,4%) en scholen (0,4%) genoemd. Onder de categorie 'auteursrechtenorganisaties' vallen SABAM (1,6%), de muziek- en filmindustrie (2,0%), bioscopen (0,4%), beheerders van data (0,4%), auteurs / artiesten (0,4%) en concurrenten (0,8%) (zie bijlage 3 voor de uitgebreide lijst).

5.3.1 Waargenomen geïnteresseerden op verschillende onlineplatformen

5.3.1.1 De meest gebruikte platformen per gepercipieerde geïnteresseerde

In de volgende paragrafen wordt aangegeven hoe respondenten denken over welke platformen potentiële geïnteresseerden het meest (volgens de categorieën 'geïnteresseerd' en 'heel geïnteresseerd') zullen gebruiken om persoonlijke gegevens te bemachtigen. Niet alle platformen worden steeds vermeld, maar enkel de meest opvallende.

De site of het platform zelf wordt hoog ingeschat als een potentieel geïnteresseerde. De frequenties schommelen namelijk tussen 53,5% (Foursquare) en 83,1% (koopplatform). De frequentie bij de koopplatformen is bijgevolg het hoogst, gevolgd door YouTube (80,5%) en Facebook (80,1%). Ook de sites van de banken (76,2%) en de zoekmachines (75,6%) zijn volgens de jongeren grote geïnteresseerden, net zoals nieuwssites (77,2%), muzieksites (79,0%) en downloadplatformen (76,9%). Als die resultaten vergeleken worden met de spontane antwoorden op de open vraag, is er toch een groot verschil in frequenties. Zo noemt amper 1,2% de websites zelf en 2,8% de oprichters van de website. Sociale media worden door 2,0% genoemd, Facebook het vaakst door 10,9%. Google wordt door 4,9% als een potentieel geïnteresseerde gezien. Ten slotte worden ook in die vraag koopplatforms vaker genoemd, namelijk met 7,3%[5].

De politie en overheid scoren op Facebook (73,4%), online banking (79,1%) en downloadplatformen (75,3%) het hoogst. Ook in de spontane antwoorden worden de politie (6,5%) en de overheid (18,2%) vaker genoemd. In bijlage 3 wordt de overheid ook in andere bewoordingen aangehaald, zoals de CIA en de regering. Wanneer al die antwoorden samen opgeteld worden en allemaal onder de noemer 'overheid' geplaatst worden, bedraagt de overheid 35,2% van de antwoorden.

Commerciële bedrijven en banken gebruiken volgens de respondenten het liefst informatie van zoekmachines (82,7%), online banking (81,2%), Facebook (79,0%), koopplatformen (78,1%) en LinkedIn (66,2%). Bij de spontane antwoorden worden de adverteerders vaak genoemd (30,0%), gevolgd door de commerciële bedrijven met 20,6%. De (online)banken hebben een frequentie van slechts 1,6%. Maar als alle antwoorden onder de noemer 'economie' geplaatst worden, heeft 'economie' een frequentie van 68,8%. De grote meerderheid van de jongeren denkt dus aan het commerciële aspect bij potentiële geïnteresseerden.

De partner of het lief is het meest geïnteresseerd in informatie op Facebook (85,8%), maar ook in de informatie op chat (74,3%), fotoplatformen (71,1%), blogs (63,1%) en Twitter (62,4%). Opvallend is

[5] Door de grote verscheidenheid aan antwoorden liggen alle procenten vrij laag. De bovengenoemde procenten horen echter tot de hoogste scores die genoteerd konden worden (zie bijlage 3).

dat de partner volgens de respondenten ook in de e-mail geïnteresseerd is (56,2%). Bij de spontane vraag wordt de partner echter door niemand genoemd.

De ex-partner of het ex-lief is algemeen genomen niet geïnteresseerd in de informatie, al valt het op dat er interesse is op Facebook (64,9%) en op muzieksites (40,5%). Spontaan wordt het ex-lief maar één keer genoemd (0,4%).

Voor **vrienden en vriendinnen** is Facebook met 85,0% de interessantste bron van informatie, gevolgd door fotoplatformen (70,3%), blogs (62,0%) en Twitter (61,1%). Spontaan worden vrienden maar voor 2,4% genoemd.

Voor **ex-vrienden en ex-vriendinnen** zijn, net zoals bij de vrienden, Facebook (51,6%) en de fotoplatformen (30,9%) het populairst. Opvallend is dat respondenten denken dat ex-vrienden nog hun blogs zouden lezen (24,6%). In de open vraag scoren ex-vrienden en boze vrienden laag met slechts 1,2%.

Familie maakt zoals de twee voorgaande potentiële geïnteresseerden het meest gebruik van Facebook (75,6%) en fotoplatformen (60,8%). Ook hier zijn de blogs verrassend populair (54,3%). Spontaan worden familie en ouders tezamen voor 2,0% genoemd.

Voor **criminelen** is online banking het populairste doelwit met 85,5%, gevolgd door zoekmachines (60,7%), Facebook (64,5%), mail (58,2%) en Foursquare (56,2%). Opvallend is dat koopaccounts volgens de respondenten maar voor 46,9% gebruikt worden. Bij de open vraag tellen criminelen, zoals hackers, dieven, stalkers, fraudeurs en spammers, voor 62,4% van de antwoorden. Voor dat cijfer werden de pedofielen niet meegerekend.

Pedofielen worden daarentegen maar voor 4,1% genoemd. Bij de invulvraag maken ze het meest gebruik van Facebook (68,0%), chat (56,5%), fotoplatformen (55,3%), LinkedIn (48,9%) en Foursquare (46,8%).

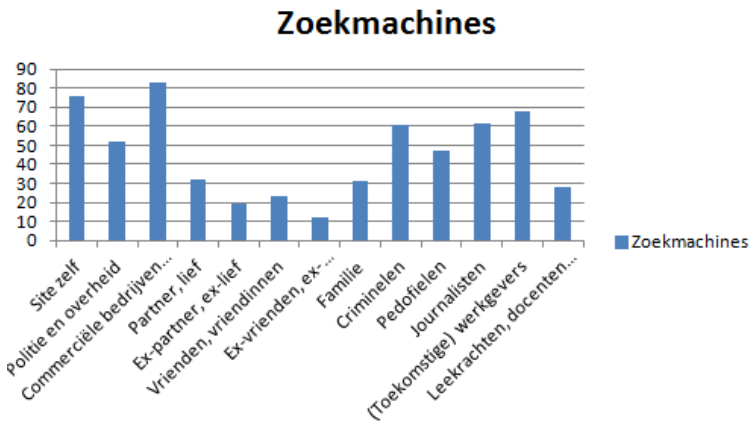
Journalisten worden amper spontaan genoemd (2,0%), net zoals ‘media’ in het algemeen (5,3%). De invulvraag toont daarentegen grotere verschillen. Journalisten zijn het meest geïnteresseerd in gegevens op nieuwssites (68,0%), Twitter (66,2%), Facebook (63,4%), zoekmachines (61,7%) en blogs (53,1%). Die vraag toont dus een veel groter bewustzijn van journalisten dan de open vraag.

(Toekomstige) werkgevers gebruiken volgens de respondenten het liefst sociale media om persoonlijke informatie op te zoeken: Facebook met 84,7%, LinkedIn met 70,9% en Twitter met 64,5%. Ook zoekmachines (67,9%) zijn volgens de respondenten een populair hulpmiddel. Spontaan worden de werkgevers met 13,8% genoemd.

Leerkrachten, docenten en directie tonen volgens de respondenten bijna in geen enkel platform interesse, op schoolplatformen na (83,7%). Spontaan werden ze maar één keer genoemd (0,4%).

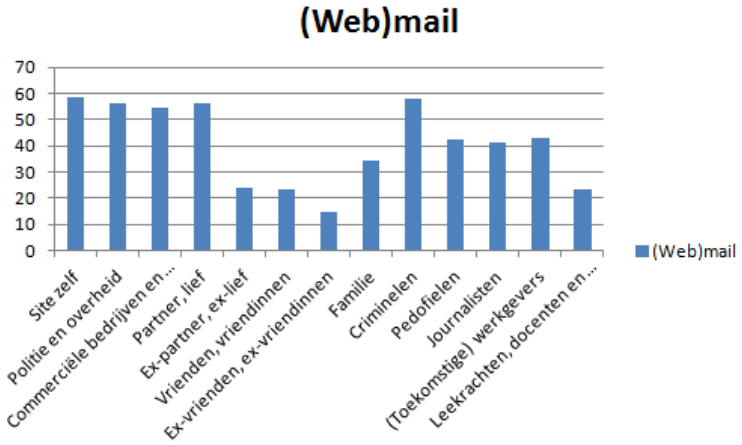
5.3.1.2 De meest frequente gepercipieerde geïnteresseerden per platform

Niet elk platform lokt volgens de respondenten dezelfde potentiële geïnteresseerden in dezelfde mate, zoals uit onderstaande resultaten blijkt[6]. Ook hier worden enkel de meest opvallende elementen besproken.



Grafiek 1. Interesse op zoekmachines

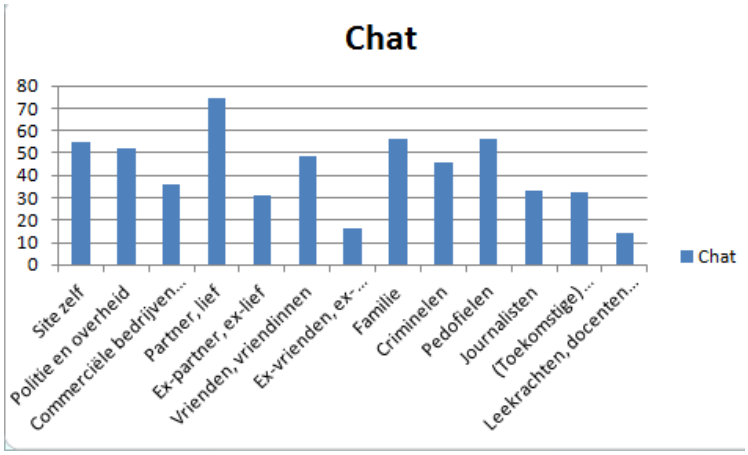
Zoekmachines zijn volgens de respondenten vooral interessant voor commerciële bedrijven en banken (82,7%), zichzelf (75,6%), (toekomstige) werkgevers (67,9%), journalisten (61,7%) en criminelen (60,7%).



Grafiek 2. Interesse op (web)mail

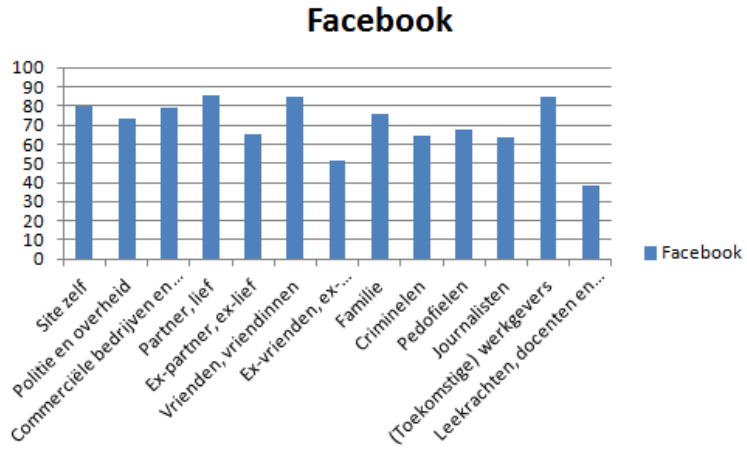
Mail is vooral nuttig voor het platform zelf (58,3%), criminelen (58,2%), de overheid (56,5%), de partner (56,2%) en de commerciële bedrijven en banken (54,3%).

[6] De procenten zijn berekend met de categorieën 'geïnteresseerd' en 'heel geïnteresseerd'.



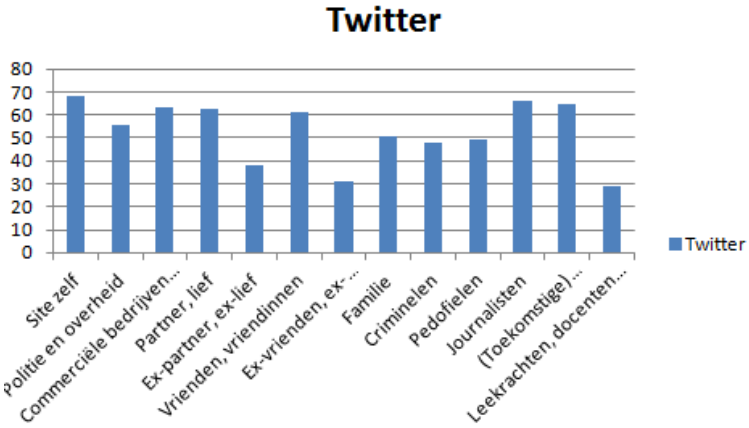
Grafiek 3. Interesse op chat

Chat wordt vooral gebruikt door de partner (74,3%), pedofielen (56,5%) en familie (56,2%).



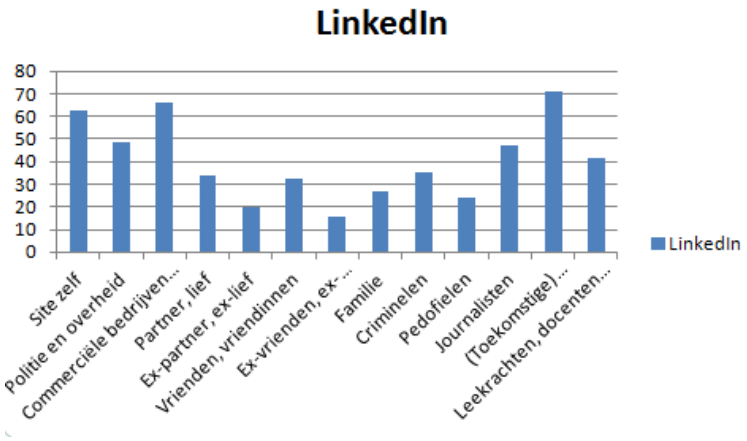
Grafiek 4. Interesse op Facebook

In **Facebook** is haast iedereen geïnteresseerd. De leerkrachten, docenten en directie scoren het laagst met 38,2% en de partners het hoogst met 85,8%. Andere grote geïnteresseerden zijn vrienden (85,0%), familie (75,6%), werkgevers (84,7%) en journalisten (63,4%).



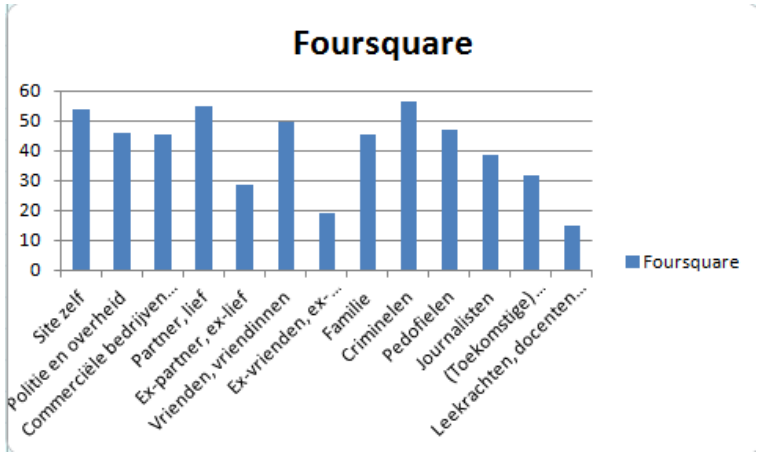
Grafiek 5. Interesse op Twitter

Twitter lokt vooral journalisten met 66,2%, (toekomstige) werkgevers met 64,5% en partners met 62,4%. Bovendien gebruikt het platform vooral zelf de gegevens (68,2%).



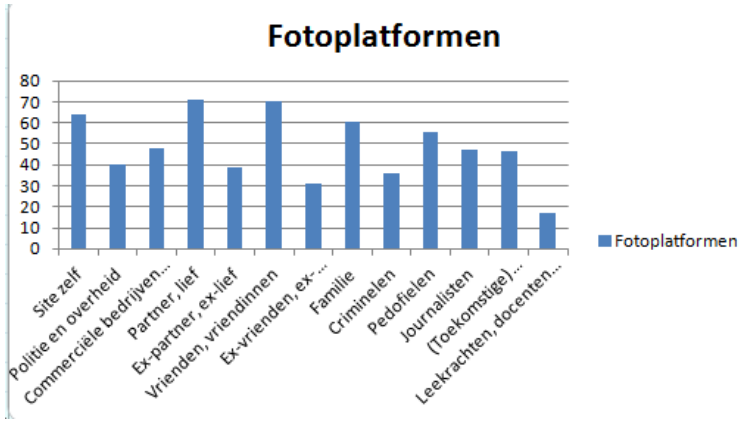
Grafiek 6. Interesse op LinkedIn

LinkedIn is een grote bron van informatie voor (toekomstige) werkgevers (70,9%) en commerciële bedrijven en banken (66,2%).



Grafiek 7. Interesse op Foursquare

Bij **Foursquare** is er maar matige interesse. Leerkrachten, docenten en directie gebruiken onder de geïnteresseerden het platform het minst voor informatie (15,0%) en criminelen het meest met 56,2%. Journalisten (38,7%) en partners (54,8%) tonen ook vrij veel interesse.

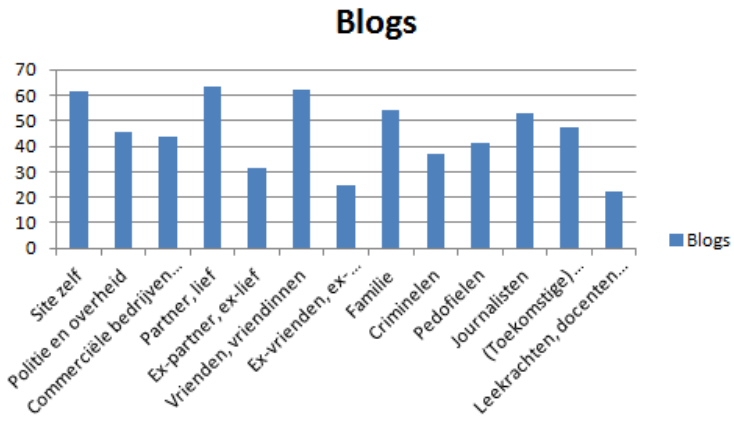


Grafiek 8. Interesse op fotoplatformen

Fotoplatformen worden dan vooral weer voor naasten gebruikt: de partner met 71,1%, vrienden met 70,3% en familie met 60,8%. Journalisten worden door 47,4% genoemd.

YouTube verzamelt vooral informatie voor zichzelf (80,5%) en is daarnaast ook voor bedrijven een informatiebron (59,4%).

Nieuwssites zijn voornamelijk een bron voor zichzelf (77,2%) en voor journalisten (68,0%). Ook commerciële bedrijven en banken maken gebruik van informatie op de sites met 53,1%.



Grafiek 9. Interesse op blogs

Blogs zijn interessant voor naasten, zoals partner (63,1%), vrienden (62,0%) en familie (54,3%). De site gebruikt met 61,3% zelf informatie en journalisten zelfs met 53,1%.

Op de **fora** zelf (65,5%) en commerciële bedrijven en banken (46,5%) na, is er matige interesse in de informatie op het onlineplatform.

Ook **koopplatformen** zijn voor zichzelf (83,1%) en commerciële bedrijven en banken (78,1%) heel interessant, maar ook de overheid (50,8%), criminelen (46,9%), partners (40,6%) en familie (39,4%) tonen interesse.

Online banking lokt verschillende instanties: criminelen (85,5%), commerciële bedrijven en banken (81,2%), overheid en politie (79,1%) en zichzelf (76,2%). Ook partners (42,2%) en familie (37,9%) tonen interesse.

Schoolsites trekken vooral leerkrachten (83,7%) en zichzelf (56,4%) aan.

Apps zijn voornamelijk nuttig voor commerciële bedrijven en banken (62,6%) en zichzelf (75,5%).

Muzieksites leveren informatie voor zichzelf (79,0%) en commerciële bedrijven en banken (63,1%). Opvallend is dat de overheid en politie maar matige interesse vertonen (29,5%) en dat de partner door 45,5% wordt genoemd.

Downloadsites verzamelen vooral zelf informatie (76,9%), maar ook de overheid (75,3%), commerciële bedrijven en banken (60,8%) en criminelen (47,5%) maken gebruik van de informatie.

De tabel voor de weergegeven grafieken:

	ZM	**Mail**	**Chat**	**FB**	**TW**	**LI**	**FQ**	**Foto**	**Blog**	**Gemiddelde over de 9 platformen**
Site zelf	75,6	58,3	54,5	80,1	68,2	62,8	53,5	64,3	61,3	64,3
Politie en overheid	52,3	56,5	52,2	73,4	55,8	48,5	45,7	39,9	45,5	52,2
Commerciële bedrijven en banken	82,7	54,3	35,6	79,0	63,4	66,2	45,5	48,1	43,9	57,6
Partner, lief	32,4	56,2	74,3	85,8	62,4	33,5	54,8	71,1	63,1	59,3
Ex-partner, ex-lief	19,2	24,1	30,9	64,9	38,3	20,0	28,6	38,8	31,6	32,9
Vrienden, vriendinnen	22,9	23,3	48,4	85,0	61,1	32,2	49,7	70,3	62,0	50,5
Ex-vrienden, ex-vriendinnen	12,1	14,5	16,6	51,6	31,1	15,9	19,0	30,9	24,6	24,0
Familie	31,5	34,5	56,2	75,6	50,3	26,6	45,2	60,8	54,3	48,3
Criminelen	60,7	58,2	46,0	64,5	47,9	35,3	56,2	36,2	37,1	49,1
Pedofielen	47,4	42,7	56,5	68,0	48,9	23,8	46,8	55,3	41,1	47,8
Journalisten	61,7	41,2	33,3	63,4	66,2	46,9	38,7	47,4	53,1	50,2
(Toekomstige) werkgevers	67,9	42,9	32,1	84,7	64,5	70,9	31,5	46,3	47,2	54,2
Leekrachten, docenten en directie	28,3	23,4	14,3	38,2	28,8	41,2	15,0	17,2	22,0	25,4

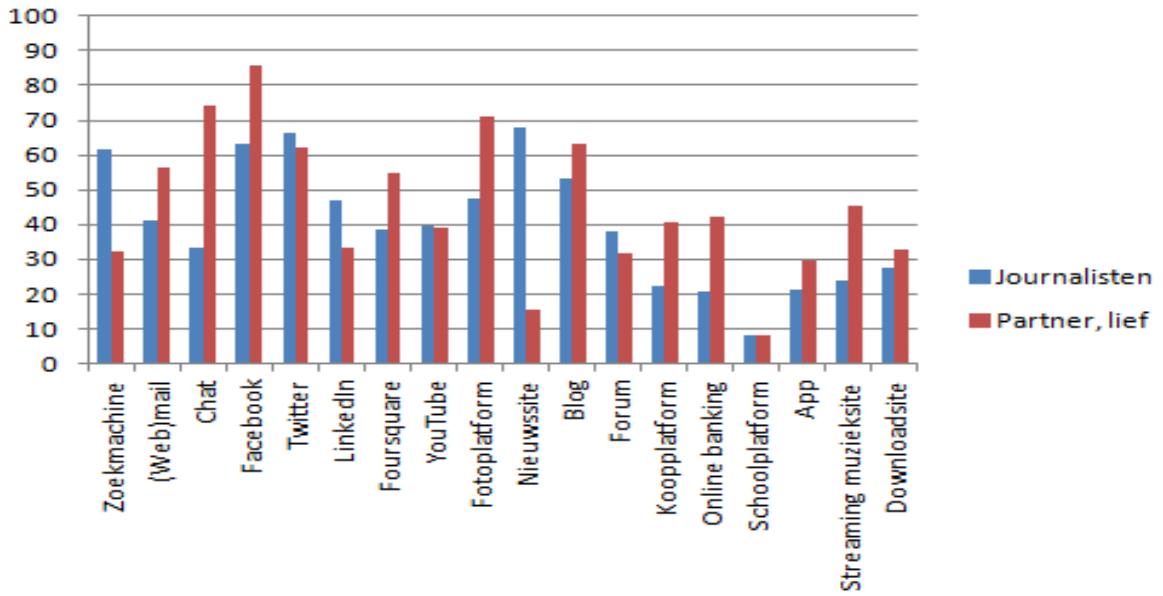
Tabel 5. Frequenties van waargenomen geïnteresseerden in platformen (in %)

De site zelf is volgens de respondenten op de negen bovengenoemde platformen de grootste geïnteresseerde, gevolgd door de partner, wat toch een opvallend resultaat is (zie tabel 5). Ook opmerkelijk is dat journalisten vrij hoog scoren, zelfs hoger dan criminelen en pedofielen. Verder hebben de evidente geïnteresseerden, zoals overheden, bedrijven en werkgevers hoge gemiddelden.

5.3.1.3 Voorlopig besluit

De invulvraag van de potentiële geïnteresseerden toont al een heel ander beeld dan de spontane antwoorden op de open vraag. In de open vraag vermelden jongeren ook wel minder voor de hand liggende potentiële geïnteresseerden, maar in veel mindere mate dan bij de lijst. Naast de bekende geïnteresseerden – zoals commerciële bedrijven en banken, de overheid en criminelen – komen nu ook de minder vanzelfsprekende geïnteresseerden zoals familie en journalisten meer in het vizier. Alle verschillende genoemde potentiële geïnteresseerden krijgen hoge scores. Nu is het alleen niet zo duidelijk of jongeren echt spontaan aan journalisten gaan denken als ze op Facebook surfen of dat ze het gewoon aangeduid hebben omdat de lijst hen als potentieel geïnteresseerde aangeeft. Verder onderzoek is daarom gewenst. Ook denken de jongeren dat niet alle platformen voor alle geïnteresseerden even interessant zijn. Vergeleken met Facebook, dat bijna iedereen gebruikt, worden YouTube, fora, Foursquare en apps amper gebruikt voor informatievergaring. Twee opvallende

tendensen zijn dat twee minder vanzelfsprekende potentiële geïnteresseerden vrij veel genoemd worden. Het gaat daarbij om journalisten en de partner (zie grafiek 10).



Grafiek 10. Analyse toont grote interesse van journalisten en partners

Opvallend is dat volgens de jongeren de site zelf en de commerciële bedrijven en banken vooral van zakelijke platformen zoals koopplatformen en LinkedIn gebruikmaken. Criminelen viseren online banking het meest. Sociale media zijn dan weer bij heel wat verschillende groepen populair. Zo tonen zowel naasten, zoals familie, (ex-)vrienden en (ex-)partners, als pedofielen veel interesse in de sociale netwerken. Ook lijken jongeren zich bewust te zijn van de interesse van de journalisten in de sociale media. Een laatste opvallend detail is dat werkgevers Facebook en niet LinkedIn het meest zouden gebruiken voor persoonlijke informatie.

Uit de vraagstelling is wel niet duidelijk of de jongeren denken dat de geïnteresseerden uit zijn op misbruik of gewoon geïnteresseerd zijn in de gegevens van de jongere. Bij de spontane vraag was er wel iemand die bij ‘vrienden’ expliciet ‘geen misbruik’ schreef. Maar misschien zijn de jongeren zich niet bij elke geïnteresseerde van potentieel gevaar bewust. Ook dat kan verder onderzocht worden.

5.3.2 De invloed van leeftijd en geslacht bij waargenomen geïnteresseerden

Uit analyse blijkt dat er verschillen tussen jongens en meisjes zijn. Op ‘de site zelf’ en ‘de commerciële bedrijven en banken’ na, is er bij alle potentiële geïnteresseerden een significant verschil tussen jongens en meisjes. De meisjes zien gemiddeld iemand meer als een potentieel geïnteresseerde dan de jongens doen. In bijlage vier, “Waargenomen potentiële geïnteresseerden: verschillen tussen jongens en meisjes”, zijn alle resultaten van de vergelijkende analyse gebundeld. Verder blijkt uit een regressieanalyse dat geslacht en leeftijd regelmatig als predictor fungeren. Opleiding is niet in de

analyse opgenomen, omdat het om een nominale variabele ging en omdat uit de analyses geen duidelijke invloed op te meten was.

Omdat het omslachtig werk is om alle predictoren hier op te lijsten, worden de opvallendste resultaten hieronder weergegeven. Die resultaten waren vooral opvallend voor de site zelf, bedrijven, familie, pedofielen en leerkrachten (zie tabel 6). Journalisten vertoonden op geen enkel platform een predictor, behalve op nieuwssites. Op dat platform treedt leeftijd als predictor op (β = 0,187, t = 2,070, p = 0,039). Daar geldt: hoe ouder de gebruiker, hoe meer hij zich van journalisten op nieuwssites bewust is.

	Leeftijd			**Geslacht (Man = 1, Vrouw = 2)**		
Zoekmachine	β	t	p	β	t	p
Site	0,324	3,786	0,000			
Bedrijven	0,270	3,055	0,002			
Familie	-0,348	-3,933	0,000	0,189	3,667	0,000
Pedofielen				0,128	2,376	0,018
Leerkrachten, docenten en directie				0,126	2,313	0,021
(Web)mail	β	t	p	β	t	p
Site	0,128	2,431	0,016			
Bedrijven	0,214	2,341	0,020			
Familie	-0,385	-4,217	0,000	0,132	2,470	0,014
Pedofielen	-0,188	-2,020	0,044	0,112	2,071	0,039
Leerkrachten, docenten en directie				0,126	2,303	0,022
Chat	β	t	p	β	t	p
Site						
Bedrijven				-0,105	-1,980	0,049
Familie	-0,271	-2,980	0,003	0,198	3,696	0,000
Pedofielen				0,180	3,309	0,001
Leerkrachten, docenten en directie				0,124	2,279	0,023
Facebook	β	t	p	β	t	p
Site	0,365	4,246	0,000			
Bedrijven	0,321	3,755	0,000			
Familie				0,212	3,922	0,000
Pedofielen				0,124	3,962	0,000
Leerkrachten, docenten en directie	0,227	2,422	0,016			
Twitter	β	t	p	β	t	p
Site	0,293	3,207	0,001			
Bedrijven	0,323	3,623	0,000			
Familie				0,134	2,394	0,017
Pedofielen				0,222	4,014	0,000
Leerkrachten, docenten en directie	0,312	3,304	0,001			

LinkedIn	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	0,267 0,329 0,277	2,884 3,670 2,954	0,004 0,000 0,003	 0,144	 2,513	 0,013
Foursquare	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie				 0,149 0,144	 2,548 2,479	 0,011 0,014
YouTube	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	0,220 0,214 -0,286	2,417 2,311 -3,024	0,016 0,021 0,003	 0,119 0,218	 2,143 3,959	 0,033 0,000
Fotoplatform	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie				 0,183	 3,222	 0,001
Nieuwssite	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	0,219 0,228	2,507 2,534	0,013 0,012	 0,149 0,168	 2,683 3,029	 0,008 0,003
Blog	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie				 0,165 0,212	 2,882 3,728	 0,004 0,000
Forum	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie				 0,162 0,171 0,155	 2,800 2,953 2,694	 0,005 0,003 0,007

Koopsite	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	0,285	3,092	0,002	 0,147	 2,594	 0,010
Online banking	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	0,286 0,190	3,104 1,991	0,002 0,047	 0,174 0,205 0,181	 3,080 3,639 3,198	 0,002 0,000 0,002
Schoolplatform	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	-0,221	-2,397	0,017	0,171 0,157	3,128 2,801	0,002 0,005
App	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie				-0,117 0,171	-2,123 3,011	0,035 0,003
Streaming muzieksite	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	0,207 0,193	2,202 2,069	0,028 0,039	 0,122 0,133	 2,119 2,316	 0,035 0,021
Downloadsite	β	t	p	β	t	p
Site Bedrijven Familie Pedofielen Leerkrachten, docenten en directie	0,323	3,541	0,000	 0,131 0,156	 2,324 2,766	 0,021 0,006

Tabel 6. Invloed van leeftijd en geslacht op waargenomen potentiële geïnteresseerden

Uit de resultaten blijkt dat de significante verschillen bij de mate waarin potentiële geïnteresseerden waargenomen worden door geslacht en leeftijd beïnvloed worden. Geslacht overheerst op de meeste platformen als predictor. Familie en pedofielen worden het sterkst door geslacht beïnvloed, maar ook leerkrachten worden grotendeels door die predictor beïnvloed. Leeftijd is soms een predictor, en dan voornamelijk bij de site zelf en de commerciële bedrijven en banken. Daar geldt hoe ouder de gebruiker is, hoe bewuster hij zich van die geïnteresseerde partijen is.

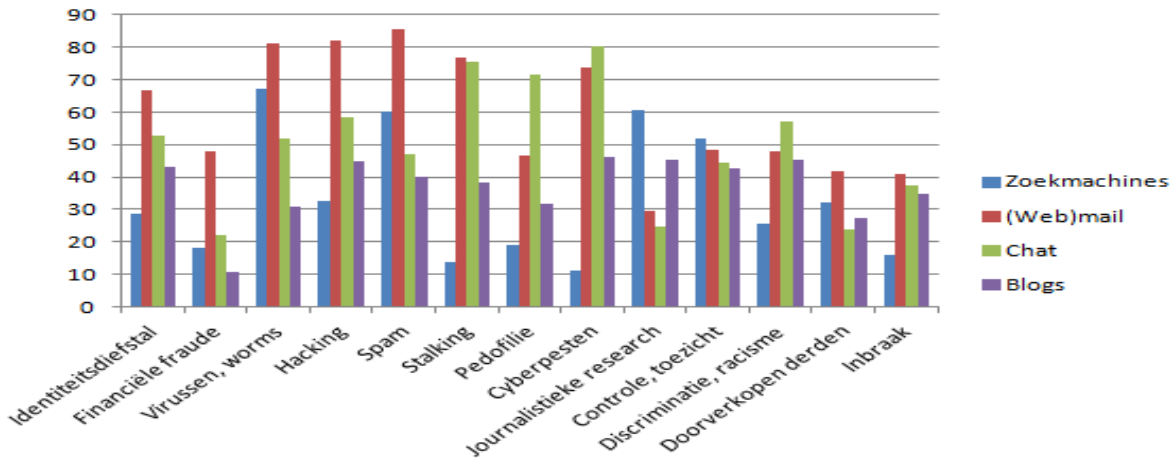
5.4 Mogelijke privacyschendingen

In deze paragraaf worden enkele opvallende elementen uit de analyse belicht. Zo gebeuren volgens de jongeren identiteitsdiefstal en journalistieke research het meest op meerdere sociale media, en discriminatie en inbraak vooral op Facebook en Twitter. Verder denken ze dat cyberpesten en stalking vooral op communicatieve platformen voorkomen, zoals chat, (web)mail, Facebook en Twitter (zie tabel 7).

Waargenomen schendingen op…	**Zoek-machine**	**(Web)-mail**	**Chat**	**Facebook**	**Twitter**	**LinkedIn**	**Foto-platform**	**Blog**
Identiteitsdiefstal	28,6	66,8	52,9	85,3	67,9	52,6	46,8	43,1
Financiële fraude, oplichting	18,2	47,7	22	32,7	19,7	20,8	6,4	10,7
Virussen, worms	67,3	81,2	52	52,9	41,6	32,9	30,6	30,9
Hacking	32,7	82,1	58,4	76,3	60,4	48	40,2	44,8
Spam	60,1	85,5	47,1	67,9	55,8	40,8	35,3	40,2
Stalking	13,6	76,6	75,4	85,3	68,8	37	39,9	38,4
Pedofilie	18,8	46,5	71,4	77,7	52,3	15,9	41,3	31,8
Cyberpesten	11	73,7	80,1	87	69,1	24,6	38,7	46,2
Journalistieke research (gebruik van gegevens en foto's)	60,4	29,5	24,6	74,3	60,1	48,8	55,8	45,4
Controle, toezicht	52	48,5	44,5	70,8	54	43,4	39,3	42,8
Discriminatie, racisme	25,7	47,7	56,9	80,9	63,9	28	40,2	45,4
Doorverkopen data aan derden	32,1	41,9	24	54,3	37,6	33,8	35,8	27,2
Inbraak (na bekendmaken vakantieplannen)	15,9	41	37,3	71,7	60,4	18,2	23,1	34,7

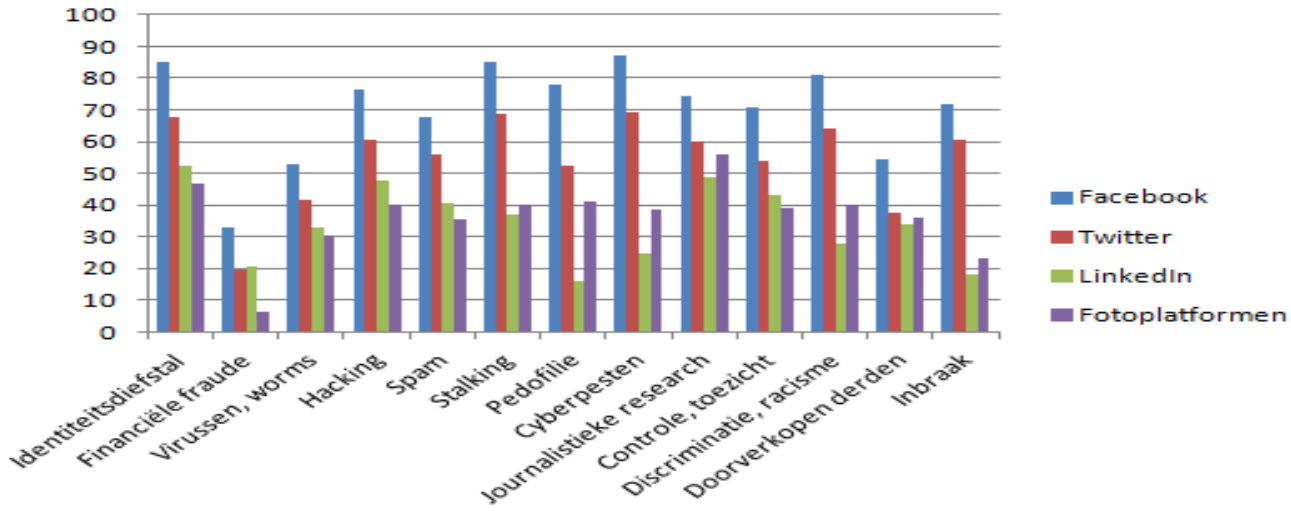
Tabel 7. Frequenties van verscheidene privacyschendingen op verschillende platformen (in %)

Bij "oudere platformen" is (web)mail volgens de jongeren nog een heel populair doelwit voor inbreuken zoals virussen en worms, hacking, spam, stalking en cyberpesten. Ook chat zou een veelgebruikt platform zijn voor stalking en cyberpesten, en voor pedofilie is dat volgens de jongeren overduidelijk het meest gebruikte platform (zie grafiek 11). Alleen Facebook scoort nog hoger (zie tabel 7). Opvallend is dat journalistieke research voornamelijk op zoekmachines en blogs zou gebeuren.



Grafiek 11. Privacyschendingen op "oudere" platformen

Bij de sociale media is volgens de respondenten Facebook het grootste doelwit voor alle inbreuken. Alle inbreuken zijn op alle platformen vrij goed vertegenwoordigd, en het valt op dat journalistieke research vrij veel genoemd wordt (zie grafiek 12).



Grafiek 12. Privacyschendingen op sociale media

In de resterende platformen met lagere scores zijn er ook enkele interessante elementen. Zo worden virussen, worms en spam bij elk platform veel genoemd. Ook journalistieke research is een veel wederkerend element (zie tabel 8). Jongeren zijn zich verrassend weinig bewust van het doorverkopen van data aan derden. Bij apps en koopplatformen, waar die praktijk toch wel regelmatig gebeurt, is de frequentie eerder aan de lage kant. Bij online banking is dat gelijkaardig. En hoewel de dreiging van hackers voldoende in het nieuws komt, denkt maar 57,2% van de jongeren aan hacking.

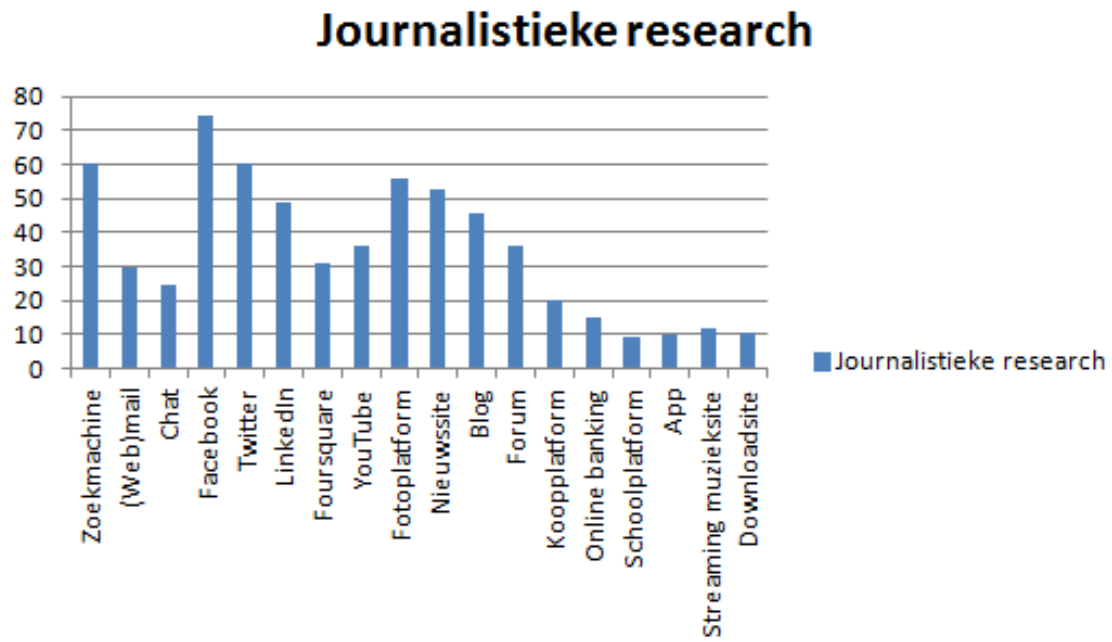
Waargenomen schendingen op…	YouTube (%)
Virussen, worms	47,4
Hacking	39,9
Spam	47,4
Journalistieke research (gebruik van gegevens en foto's)	35,8
Discriminatie, racisme	43,4
Doorverkopen data aan derden	23,4
Waargenomen schendingen op…	Foursquare (%)
Stalking	40,8
Journalistieke research (gebruik van gegevens en foto's)	31,2
Controle, toezicht	42,2
Inbraak (na bekendmaken vakantieplannen)	41,0
Waargenomen schendingen op…	Nieuwssites (%)
Journalistieke research (gebruik van gegevens en foto's)	52,6
Waargenomen schendingen op…	Fora (%)
Spam	44,2
Journalistieke research (gebruik van gegevens en foto's)	36,1
Controle, toezicht	34,7
Discriminatie, racisme	36,1
Waargenomen schendingen op…	Koopplatformen (%)
Financiële fraude, oplichting	75,1
Spam	38,7
Doorverkopen data aan derden	43,4
Waargenomen schendingen op…	Online banking (%)
Identiteitsdiefstal	55,2
Financiële fraude, oplichting	80,9
Hacking	57,2
Controle, toezicht	43,6
Waargenomen schendingen op…	Schoolplatformen (%)
Controle, toezicht	39,9
Waargenomen schendingen op…	Apps (%)
Virussen, worms	49,4
Spam	41,6
Doorverkopen data aan derden	20,5
Waargenomen schendingen op…	Streaming muzieksites (%)
Virussen, worms	46,8
Spam	40,2
Waargenomen schendingen op…	Downloadsites (%)
Virussen, worms	69,4
Hacking	47,1
Spam	56,6

Tabel 8. Privacyschendingen op de resterende platformen

Zoals eerder werd vermeld, wordt journalistieke research vaak genoemd als een mogelijke privacyinbreuk. Vooral op zoekmachines en sociale media zoals Facebook en Twitter wordt het volgens de respondenten veel toegepast (zie tabel 9 en grafiek 13). Maar ook op fotoplatformen, nieuwssites, blogs en fora zouden de journalisten informatie kunnen vergaren.

	Journalistieke research (in %)
Zoekmachine	60,4
(Web)mail	29,5
Chat	24,6
Facebook	74,3
Twitter	60,1
LinkedIn	48,8
Foursquare	31,2
YouTube	35,8
Fotoplatform	55,8
Nieuwssite	52,6
Blog	45,4
Forum	36,1
Koopplatform	19,9
Online banking	15,3
Schoolplatform	9,5
App	10,1
Streaming muzieksite	12,1
Downloadsite	10,7

Tabel 9. De bedreiging van journalistieke research op verschillende platformen



Grafiek 13. De bedreiging van journalistieke research op verschillende platformen

5.5 Privacybewustzijn bij jongeren

In de survey werd ook het privacybewustzijn op verschillende onlineplatformen bij jongeren nagegaan door de vraag "In welke mate houd jij op de volgende platformen rekening met een eventuele schending van je privacy online door bijvoorbeeld privacysettings aan te passen of *cookies* te verwijderen?". Daaruit blijkt dat de jongeren zich toch nog te weinig van eventuele privacyschendingen aantrekken. Bij zoekmachines ligt het nemen van beschermingsmaatregelen vrij laag: 56,4% houdt geen rekening met een eventuele privacyschending en slechts 29,2% een beetje, terwijl er voldoende negatieve berichten over Google in de media komen. Ook andere platformen worden blijkbaar niet als potentieel gevaar voor de privacy bekeken (zie tabel 10).

HELEMAAL NIET TOT AMPER (%)	
LinkedIn	50,9
YouTube	51,7
Fotoplatform	52,4
Downloadsite	53,2
Foursquare	54,1
Blog	55,8
Zoekmachine	56,4
Schoolsite	56,5
Forum	59,9
Streaming muzieksite	63,3
App	65,9
Nieuwssite	74,4
BEETJE TOT VEEL (%)	
Twitter	39,8
Chat	53,8
(Web)mail	59,5
VEEL TOT HEEL VEEL (%)	
Koopplatformen	43,7
Online banking	67,5
Facebook	83,7

Tabel 10. Mate waarin gebruiker met eventuele schending van de privacy rekening houdt

Bij de mail en chat is het al een stuk beter. Bij koopaccounts wordt er grotendeels rekening mee gehouden. 43,7% is zich veel tot heel veel van potentiële inbreuken bewust, en 20,5% een beetje, wat een totaal van 64,2% geeft. Bij online banking is 67,5% zich veel tot heel veel van gevaar bewust. Opvallend is het hoge cijfer bij Facebook. 83,7% is zich veel tot heel veel van het gevaar bewust, maar bij Twitter liggen de cijfers terug een stukje lager. 39,8% is zich een beetje tot veel bewust van potentiële inbreuken, en 19,3% heel veel, wat toch een cijfer van 59,1% geeft.

5.5.1 De invloed van leeftijd en geslacht op privacybewustzijn

Om eventuele verschillen tussen jongens en meisjes te vinden, werd er gebruik gemaakt van onafhankelijke T-testen en een meervoudige regressieanalyse. Op vier van de achttien verschillende onlineplatformen is een significant verschil tussen jongens en meisjes gevonden. Het gaat om de platformen zoekmachines, Facebook, blogs en online banking (zie tabel 11).

	Meisjes M	Meisjes SD	Jongens M	Jongens SD	t(…) = …	p
Zoekmachine	2,23	1,085	2,53	1,218	t(302) = 2,090	0,037
Facebook	4,28	0,910	4,00	1,080	t(298) = -2,266	0,024
Blog	2,45	1,386	2,06	1,116	t(171,428) = -2,383	0,018
Online banking	3,95	1,372	3,38	1,620	t(133,124) = -2,850	0,005

Tabel 11. Invloed van geslacht op privacybewustzijn

Jongens houden op zoekmachines meer rekening met hun privacy dan meisjes. Meisjes zijn zich dan weer bewuster van hun privacy op de platformen Facebook, blogs en online banking. Met een meervoudige regressieanalyse werd nagegaan welke eigenschappen ook als predictoren fungeren. Dat wordt in de onderstaande tabel weergegeven.

Platform	**Leeftijd**			**Geslacht (Man = 1, Vrouw = 2)**		
	β	t	p	β	t	p
Zoekmachine				-0,119	-2,050	0,041
Facebook				0,135	2,319	0,021
Twitter	-0,217	-2,146	0,033			
YouTube	-0,267	-2,715	0,007			
Fotoplatform	-0,240	-2,353	0,019			
Blog	-0,289	-2,891	0,004	0,147	2,435	0,016
Forum	-0,296	-2,930	0,004			
Online banking				0,173	2,983	0,003
App	-0,221	-2,163	0,031			

Tabel 12. Invloed van leeftijd en geslacht op privacybewustzijn op verschillende platformen

De vier platformen zoekmachines, Facebook, blogs en online banking hebben geslacht als predictor, dus ook hier speelt geslacht een rol. Voor blogs is ook leeftijd een significante voorspeller van privacybewustzijn. Samen met blogs worden ook Twitter, YouTube, fotoplatformen, fora en apps door leeftijd beïnvloed. Hier geldt hoe jonger iemand is, hoe minder die zich van zijn privacy bewust is. Maar de andere helft van de platformen (mail, chat, LinkedIn, Foursquare, nieuwssites, koopplatformen, schoolsites, muzieksites en downloadsites) heeft geen predictoren. Ook hier is opleiding in de analyse niet opgenomen omdat het een nominale variabele is. Bovendien is er geen direct meetbare invloed teruggevonden.

5.5.2 Beschermingsstrategieën

De jongeren beschermen grotendeels hun privacy op onlineplatformen, al variëren de methodes wel. In de survey werden acht mogelijkheden gegeven, waarbij de jongere moest aanduiden welke strategie hij gebruikt. Het aanpassen van de privacysettings en opletten met wat ze online plaatsen waren allebei het populairst. Opvallend is dat slechts 56,9% gebruikmaakt van een firewall en/of antivirussoftware. En de gebruikersovereenkomst scoort met amper 19,4% nog steeds heel slecht (zie tabel 13).

Beschermingsstrategieën	**Aantal in %**
Aanpassen privacysettings	80,1
Opletten met wat je online plaatst	80,1
Letten op wat je schrijft	77,7
Opletten met wie je online communiceert	72,5
Gebruikmaken van nicknames	48,0
Verwijderen van *cookies*	37,0
Gebruikmaken van een firewall en/of antivirussoftware	56,9
Lezen van de gebruikersovereenkomst	19,4

Tabel 13. Frequenties van beschermingsstrategieën

Als negende optie vulde 7,5% van de respondenten de open vraag 'andere' in, waardoor ze konden aanvullen wat ze nog gebruiken. Daarbij werden de programma's AdBlock en 'Do Not Track Me' (= een extensie die automatisch *cookies* verwijdert) genoemd. Terugkerende elementen waren incognito surfen, het verbergen van het IP-adres, het gebruik en het veranderen van verschillende wachtwoorden, het mijden van bepaalde websites en toepassingen en het negeren van onbekenden. Ook valse informatie (bv. onzin e-mailadressen) geven wordt als strategie genoemd, net zoals het antwoord 'gebruik van gezond verstand' waarmee een jongere altijd voorzichtig moet zijn en zeker niet mag zeggen dat hij van huis weggaat.

5.5.3 Correlatie tussen privacybewustzijn en gebruik

Tijdens de analyse van de resultaten leek het ook interessant om de correlatie tussen het gebruik en het privacybewustzijn na te gaan. Er blijkt namelijk een significante positieve samenhang tussen het gebruik van en het privacybewustzijn op onlineplatformen te zijn. Dus hoe meer iemand de platformen gebruikt, hoe meer die zich van zijn privacy bewust is. Wel klopt de stelling voor een paar uitzonderingen niet: zo is er geen correlatie gevonden tussen gebruik en de volgende platformen: zoekmachines, (web)mail, Facebook, nieuwssites en schoolplatformen (zie tabel 14).

Platform	r	p
Zoekmachine	0,029	0,612 (p>0,05)
(Web)mail	0,021	0,713 (p>0,05)
Chat	0,131	0,024 (p<0,05)
Facebook	0,005	0,928 (p>0,05)
Twitter	0,268	0,000 (p<0,01)
LinkedIn	0,168	0,007 (p<0,01)
Foursquare	0,144	0,019 (p<0,05)
YouTube	0,161	0,005 (p<0,01)
Fotoplatform	0,255	0,000 (p<0,01)
Nieuwssite	0,045	0,438 (p>0,05)
Blog	0,265	0,000 (p<0,01)
Forum	0,189	0,002 (p<0,01)
Koopplatform	0,140	0,018 (p<0,05)
Online banking	0,166	0,004 (p<0,01)
Schoolplatform	0,065	0,264 (p>0,05)
Apps	0,123	0,042 (p<0,05)
Muziek streaming	0,134	0,027 (p<0,05)
Downloadplatform	0,160	0,007 (p<0,01)

Tabel 14. Correlaties tussen gebruik en privacybewustzijn

5.5.4 Correlatie tussen privacybewustzijn en waargenomen potentiële geïnteresseerden

Ook de mogelijke correlatie tussen privacybewustzijn en de waargenomen potentiële geïnteresseerden leek eens de moeite waard om te onderzoeken. Zo blijkt dat jongeren het meest aan familie denken als ze meer aan hun privacy op verschillende platformen denken. De site zelf, politie en overheid, (toekomstige) werkgevers, criminelen en pedofielen hebben normale scores, maar commerciële bedrijven en banken scoren opvallend laag. Ook aan leerkrachten, docenten en directie wordt minder gedacht. Met partners, ex-partners, vrienden en ex-vrienden daarentegen wordt meer rekening gehouden als het privacybewustzijn stijgt. Journalisten scoren ook opvallend goed, wat betekent dat jongeren echt wel rekening met hen houden. Eén vreemd detail is dat het platform Facebook amper correlaties vertoont (zie bijlage 5 voor de uitgebreide tabel).

5.6 Journalisten en onlineprivacy

Bij de open vraag over waargenomen potentiële geïnteresseerden blijkt dat niet al te veel jongeren spontaan aan de media denken[7]. Slechts drie van de 346 jongeren noemen grote mediaconcerns, één iemand de pers en maar vijf personen de journalisten. Als die resultaten dan vergeleken worden met de invulvraag van de geïnteresseerden, komen er heel andere resultaten uit de bus (zie infra). Ook bij de vraag of jongeren er zich van bewust zijn dat journalisten hun gegevens zoals statusupdates, tweets en foto's kunnen gebruiken, is plots 52,3% zich er een beetje of voldoende van bewust. 15,4% zegt zelfs 'heel veel'.

Op de vraag of journalisten zulke gegevens mogen gebruiken, antwoordt bijna de helft van de respondenten dat het afhankelijk is van de context. Als die zaken vervolgens geïllustreerd worden met de case van Sierre, zegt plots 64,1% dat het niet geoorloofd is. Bij het gebruik van statusupdates en tweets van werknemers van Ford Genk [8] is slechts 26,4% tegen het gebruik ervan. 40,7% gaat ermee akkoord als het anoniem blijft. Al kan het verschil hier liggen aan het feit dat het in het eerste voorbeeld om foto's én minderjarigen gaat, terwijl de statusupdates en tweets in het tweede voorbeeld anoniem zijn en van volwassenen komen.

De vraag over het gebruik van foto met volledige naam erbij in krant of op televisie botste op heel wat weerstand. Als het om de jongere zelf ging, was 63,8% tegen het gebruik ervan. Als het om naasten ging, lag het met 66,1% zelfs nog iets hoger (zie tabel 15).

[7] Zie bijlage 3: Potentiële geïnteresseerden volgens scholieren en studenten.
[8] Eind 2012 werd besloten om in 2014 de fabriek te sluiten, met een grote staking als gevolg.

Vraag	Ja	Ja, indien anoniem	Nee	Afhankelijk van context
Mogen journalisten gegevens, foto's, statusupdates, e.d. gebruiken?	3,3	11,7	36,5	48,5
Mogen tweets en statusupdates van de werknemers van Ford Genk in de krant geplaatst worden?	8,1	40,7	26,4	24,8
	Ja		**Nee**	
Was het gebruik van foto's van de slachtoffers van Sierre deontologisch verantwoord?	13,1		64,1	
Als jou iets overkomt, zouden journalisten je dan met foto en/of volledige naam in de media mogen tonen?	16,0		63,8	
Als iemand uit jouw naaste omgeving iets overkomt, zouden journalisten die persoon dan met foto en/of volledige naam in de media mogen tonen?	12,4		66,1	

Tabel 15. Frequenties van de antwoorden op ethische vragen (in %)

5.6.1 Verschillen tussen jongens en meisjes

Om eventuele verschillen tussen jongens en meisjes te vinden, werd er gebruik gemaakt van onafhankelijke T-testen. Enkel bij de vragen over 'het algemeen gebruik van statusupdates, tweets en foto's' en 'het gebruik van tweets en statusupdates van de werknemers van Ford Genk' was er een significant verschil. Meisjes laten bij de eerste vraag het gebruik gemiddeld meer toe dan jongens. Ook bij de vraag over Ford Genk laten de meisjes het gebruik gemiddeld meer toe dan de jongens. Bij die vragen treedt geslacht ook als predictor op (zie tabel 16).

							Geslacht als predictor (Man = 1, Vrouw = 2)		
	Meisjes M	**Meisjes SD**	**Jongens M**	**Jongens SD**	**t(…) = …**	**p**	**β**	**t**	**p**
Het algemeen gebruik van statusupdates, tweets en foto's	3,25	0,739	3,01	0,800	t(304) = -2,498	0,013	0,148	2,571	0,011
Het gebruik van statusupdates en tweets van werknemers Ford Genk	2,79	0,965	2,47	0,887	t(304) = -2,627	0,009	0,150	2,610	0,010

Tabel 16. Invloed van geslacht op ethische vragen

6. Conclusies en discussie

Jongeren en privacy zijn zaken die niet altijd goed samengaan. Jongeren vertrouwen internetplatformen te veel waardoor ze kunnen *oversharen* en beschermen zichzelf te weinig tegen potentiële gevaren (Newell, 2011, p. 18-19; Walrave et al., 2012; Zansberg & Fischer, 2011, p. 30). Omdat het probleem van het niet lezen van de gebruikersovereenkomst blijft bestaan, zou het beter zijn om die voor jongeren begrijpelijker en leesvriendelijker te maken. Ook het feit dat er voor journalisten een nieuwe richtlijn ingevoerd werd, betekent dat de privacybescherming nog steeds verbeterd moet worden om potentieel misbruik tegen te gaan. Verder onderzoek naar mogelijke gevaren voor onlineprivacy is daarom wenselijk. In deze studie werden vier onderzoeksvragen gesteld, die allemaal voldoende beantwoord konden worden.

V1: Wie zien jongeren als potentiële geïnteresseerden in hun informatie op verschillende onlineplatformen?

De open vraag over waargenomen potentiële geïnteresseerden toont aan dat jongeren een heel divers beeld van geïnteresseerden hebben. Bekende instanties zoals de overheid, bedrijven, banken en criminelen worden nog steeds het vaakst genoemd, maar ook minder evidente instanties zoals familie, (ex)vrienden, (ex)partners en journalisten. Zelfs onderzoekers en auteursrechtenorganisaties zijn in de lijst terug te vinden. Wanneer de open vraag met de invulvraag vergeleken wordt, is er wel een merkbaar verschil. Amper genoemde personen zoals journalisten en partners worden in de invulvraag frequent als (heel) geïnteresseerd aangeduid. Ook hebben volgens de jongeren geïnteresseerden voorkeuren voor bepaalde platformen. Commerciële bedrijven en banken verkiezen koopplatformen en LinkedIn en criminelen online banking. Opvallend is dat werkgevers Facebook boven LinkedIn verkiezen als bron voor informatie. Familie, (ex)vrienden, (ex)partners en pedofielen gebruiken ook het liefst sociale media. Uit deze resultaten blijkt dat jongeren toch voldoende aan potentiële geïnteresseerden denken. Misschien komt dat omdat ze als *digital natives* meer ervaring hebben en vertrouwder zijn met het internet, waardoor ze weten welke gevaren er allemaal bestaan. Maar toch kan het nog steeds beter. Een derde heeft namelijk de open vraag opengelaten, en dat kan misschien komen doordat die jongeren er misschien nog niet voldoende over nagedacht hebben.

V2: Welke mogelijke privacybedreigingen zijn er volgens hen per platform mogelijk?

Ook journalisten zijn volgens de jongeren het meest geïnteresseerd in sociale media. Verder wordt journalistieke research bij haast alle platformen vaak genoemd als een privacyschending. Bijna de helft van de jongeren vermeldt in de vragen over het gebruik van persoonlijke gegevens in de media dat het afhankelijk is van de context, maar tweederde staat heel afkerig tegenover het gebruik ervan als het om henzelf of om naasten gaat. Verder denken jongeren verrassend genoeg weinig aan het doorverkopen van data aan derden op koopplatformen en apps. Ook hackers op online banking worden vrij weinig vermeld. Dat kan misschien te wijten zijn aan de overvloed van vertrouwen dat jongeren in

platformen hebben. Onderzoek heeft aangetoond dat jongeren zich vrij veilig voelen (Butler et al., 2011; Newell, 2011; Tuunainen et al., 2009; Veltsos & Veltsos, 2010; Walrave et al., 2012; Zansberg & Fischer, 2011).

V3 – 4: In welke mate zijn jongeren zich van hun onlineprivacy bewust? Welke strategieën gebruiken jongeren online om hun privacy te beschermen?

Het privacybewustzijn bij jongeren kan beter. Enkel op de platformen chat, Facebook, Twitter, online banking en koopplatformen wordt er voldoende rekening gehouden met eventuele privacyschendingen. Ook de bescherming kan beter. Firewalls en antivirusprogramma's wordt nog te weinig gebruikt, en amper één vijfde leest de gebruikersovereenkomst. Dat is nog steeds veel te weinig, wat ook in voorgaand onderzoek werd aangetoond (Butler et al., 2011; Cha, 2011; Tuunainen et al., 2009). Ook is een correlatie tussen het gebruik van onlineplatformen en privacybewustzijn aangetoond. Hoe meer iemand van de platformen gebruikmaakt, hoe meer privacybewustzijn die gebruiker heeft. Enkel voor zoekmachines, (web)mail, Facebook, nieuwssites en schoolsites klopt die stelling niet.

Ten slotte hebben geslacht en leeftijd invloed en fungeren ze soms als predictoren. Zo is er een verschil in gebruik bij jongens en meisjes, zoals eerder onderzoek al meerdere keren aangetoond heeft (Fortson et al., 2007; Jones et al., 2009; Livingstone et al., 2013). Meisjes gebruiken het internet vaker voor communicatieve (Facebook) en educatieve (schoolsites) doeleinden, terwijl jongens meer entertainment zoeken, zoals het downloaden van muziek (muzieksites, downloadsites), het bekijken van filmpjes (YouTube), het opzoeken van sportuitslagen of het spelen van spelletjes (apps). Verder speelt leeftijd een rol. Hoe ouder een internetgebruiker is, hoe meer hij zich van sites en commerciële bedrijven en banken als geïnteresseerden bewust is. Ook blijkt dat hoe jonger iemand is, hoe minder hij zich van zijn privacy bewust is.

Deze studie toont aan dat jongeren zich wel voldoende bewust zijn van hun privacy en de potentiële gevaren online, maar dat ze nog altijd te weinig doen om zich online te beschermen. Enkele mogelijke redenen die ook in voorgaand onderzoek gegeven werden, zijn dat ze zich geen zorgen maken over hun privacy (Livingstone et al., 2013) omdat ze toch eerder positieve dan negatieve online-ervaringen hebben (Madden et al., 2013) of omdat ze niet goed weten hoe ze zich moeten beschermen. Ook het gebrek aan kennis van het privacybeleid kan tot te weinig bescherming leiden, omdat jongeren dan niet goed weten wie hun persoonlijke gegevens allemaal kan inkijken. Tot slot hebben de jongeren te veel vertrouwen in onlineplatformen, waardoor ze gaan *oversharen*. En volgens recent onderzoek doen ze dat nu meer dan vroeger (Butler et al., 2011; Madden et al., 2013; Newell, 2011; Tuunainen et al., 2009; Walrave et al., 2012; Zansberg & Fischer, 2011).

Jongeren houden wel voldoende rekening met allerlei verschillende instanties die in hun gegevens geïnteresseerd zouden zijn. Opvallend daarbij is dat minder evidente personen, zoals de partner, vrienden, familie en journalisten ook als indringers gezien kunnen worden en zelfs meer genoemd worden dan criminelen en pedofielen. Misschien zijn andere bedreigingen meer een ver-van-mijn-bedshow, en heeft het ongeval in Sierre heel wat mensen wakker geschud. Een laatste reden is dat de meerderheid van de respondenten al hogere studies deed, en dat de studenten daarom pedofielen niet meer als bedreiging zien. Zo kan het gemiddelde misschien vertekend zijn door hun antwoorden samen te voegen met de antwoorden van de scholieren.

Omdat het toch belangrijk is dat de houding van de jongeren verandert en ze beter voldoende op potentieel gevaar online gewezen worden, zouden er stappen moeten worden genomen om het privacybeleid bereikbaar te maken voor jongeren. Zo zou er veel simpelere taal gebruikt moeten worden, en desnoods geïllustreerd met cartoons om de jongeren aan te spreken. Ouders zouden meer informatie moeten krijgen en die moeten meenemen in de opvoeding van hun kinderen. Tot slot kan het onderwijs al vanaf de lagere school verplichte lessen wijden aan 'veilig surfen'.

Wel zijn er nog enkele opmerkingen aan dit onderzoek. Een implicatie was de vraagstelling over de waargenomen potentiële geïnteresseerden. Voor de open vraag werd er duidelijk vermeld dat het dan om privacyschending ging, maar bij de invulvraag werd dat niet herhaald. Zo werden vrienden, partner en familie frequent als geïnteresseerden aangeduid, maar het is onduidelijk om af te leiden of de respondenten dachten dat ook die partijen persoonlijke gegevens kunnen misbruiken. Bij de open vraag noemde bijvoorbeeld iemand vrienden als geïnteresseerde, maar schreef die expliciet 'geen misbruik!' erbij en werd de partner zelfs geen enkele keer genoemd.

Een andere beperking is de representativiteit van de onlinesurvey. Het gaat namelijk maar om één secundaire school en één hogeschool in Vlaanderen. Bovendien is generalisatie niet mogelijk, omdat 70,7% van de respondenten vrouwelijk was, tegenover 29,3% dat mannelijk was.

Vervolgonderzoek kan misschien een ander licht op de kwestie werpen. Zo kunnen er bijvoorbeeld diepte-interviews afgenomen worden, waarbij er meer kan worden doorgevraagd over geïnteresseerden waar respondenten spontaan aan denken en kan er meer genuanceerd worden. Ook het verschil rond leeftijd en geslacht kan beter bestudeerd worden, gezien de grillige resultaten van nu geen veralgemenend beeld van de invloed van die factoren kan geven.

Een laatste punt van aandacht is de aandacht rond journalisten. Zo kan worden nagegaan of die blijvend is of dat die er nu tijdelijk is door het ongeval in Sierre. Onderzoek van een (aantal) jaar later kan misschien heel andere resultaten geven.

7. Bibliografie

Boeken

- Carpentier, N. (2007). Journalism, Media, and Democracy. In B. Cammaerts & N. Carpentier (Eds.), *Reclaiming the Media: Communication Rights and Democratic Media Roles* (pp. 151-156). Bristol: Intellect Books.
  Geraadpleegd 22 mei 2012 via
  http://scholar.googleusercontent.com/scholar?q=cache:a_SWgciEkzcJ:scholar.google.com/&hl=nl&as_sdt=0.
- Dannen, C. & White, C. (2011). Chapter 2: Privacy, privacy, privacy. In C. Dannen & C. White (Eds.), *Beginning iOS Apps with Facebook and Twitter APIs: for iPhone, iPad, and iPod touch* (pp. 9-14). Berkely: Apress.
- Kobayashi, M. (2012). Chapter 3: Blogging Around the Globe: Motivations, Privacy Concerns, and Social Networking. In A. Abraham (Ed.), *Computational Social Networks: Security and Privacy* (pp. 55-86). London: Springer.
- Oomen, I. & Leenes, R. (2008). Privacy Risk Perceptions and Privacy Protection Strategies. In E. De Leeuw, S. Fischer-Hübner, J. Tseng & J. Borking (Eds.), *Policies and Research in Identity Management. The International Federation for Information Processing* (Vol. 261, pp. 121-138). Boston: Springer.
- Opgenhaffen, M. & Belle, B. van (2012). *Sociale media en journalistiek*. Tielt: Uitgeverij LannooCampus.
- Trudel, P. (2009). Privacy Protection on the Internet: Risk Management and Networked Normativity. In S. Gutwirth, Y. Poullet, P. De Hert, C. De Terwangne & S. Nouwt (Eds.), *Reinventing Data Protection* (pp. 317-334). United States: Springer.

Kranten

- Ceulaer, J. de (2012, 1-2 december). ‘We zullen oprechter moeten worden’. Op naar een wereld zonder privacy?. *De Standaard*.
- Deckmyn, D. (2013, 28 februari). Cyberspionnen treffen België. *De Standaard*.
- Deckmyn, D. (2013, 16-17 maart). Er is geen ontsnappen aan Zalando. Wie klikt, wordt gestrikt: hoe bedrijven u overal op het internet kunnen volgen. *De Standaard*.
- Lemmens, K. (2013, 06 februari). ‘De naam van mijn huisdier is niet zo privé’. *De Standaard*.
- Minten, D. (2012, 30 november). Perswet splijt Brits kabinet. *De Standaard*.
- Minten, D. (2013, 19 maart). Britse pers krijgt strengere waakhond. Drie partijen sluiten politiek akkoord. *De Standaard*.

- Neyt, G. (2013, 04 januari). Heksenjacht op daders. Facebook, oplossing en ophitsing in zaak-Eindhoven. *De Standaard*.
- Sels, G. (2013, 13 maart). U bent een open Facebook. Wat u 'leuk vindt' vertelt meer dan u denkt. *De Standaard*.
- Shaer, M. (2012, 17 december). Instagram, Now Under Facebook Banner, Changes Privacy Policy. *Christian Science Monitor*.
- Vanhecke, N. (2013, 18 januari). CIA leest mee met wat u online uitvoert. *De Standaard*.
- Vanhecke, N. (2013, 29 april). Gerecht krijgt dossier datalek NMBS. NMBS zou privacywet overtreden hebben. *De Standaard*.
- X. (2012, 05 oktober). Eén miljard mensen gebruiken Facebook. *Metro*.
- X. (2012, 18 oktober). Hackers maken identiteit van pester bekend. *Metro*.

Tijdschriften

Academic journals

- Al-Jaghoub, S., Al-Yaseen, H. & Al-Hourani, M. (2010). Evaluation of Awareness and Acceptability of Using E-Government Services in Developing Countries: The Case of Jordan. *The Electronic Journal Information Systems Evaluation*, *13*, *nr. 1*, 1-8.
- Antón, A. I., Earp, J. B. & Young, J. D. (2010). How Internet Users' Privacy Concerns Have Evolved Since 2002. *Security & Privacy (IEEE)*, *8*, *nr. 1*, 21-27.
- Barrett, J. & Strongman, L. (2012). The Internet, the Law, and Privacy in New Zealand: Dignity with Liberty?. *International Journal of Communication*, *6*, 127-143.
- Beatty, P., Reay, I., Dick, S. & Miller, J. (2011). Consumer Trust in E-Commerce Web Sites. *ACM Computing Surveys*, *43*, *nr. 3*, 1-46.
- Beaubien, G. (2013). Instagram Modifies Privacy Policy After Sparking Internet Outrage. *Public Relations Tactics*, *20*, *nr. 1*, 6.
- Boyd, D. M. & Ellison, N. B. (2008). Social Network Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication*, *13*, *nr. 1*, 210-230.
- Butler, E., McCann, E. & Thomas, J. (2011). Privacy Setting Awareness on Facebook and Its Effect on User-Posted Content. *Human Communication*, *14*, *nr. 1*, 39-55.
- Cha, J. (2011). Information Privacy: A Comprehensive Analysis of Information Request and Privacy Policies of Most-Visited Web Sites. *Asian Journal of Communication*, *21*, *nr. 6*, 613-631.
- Colesca, S. E. (2009). Understanding Trust in e-Government. *Engineering Economics*, *63*, *nr. 3*, 7-15.

- Cutillo, L. A., Molva, R. & Strufe, T. (2009). Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust. *IEEE Communications Magazine, 47, nr. 12,* 94-101.
- Debatin, B., Lovejoy, J. P., Horn, A. K. & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication, 15, nr. 1,* 83-108.
- Determann, L. (2012). Social Media Privacy: A Dozen Myths and Facts. *Stanford Technology Law Review, 15, nr. 7,* 1-14.
- Fernback, J. & Papacharissi, Z. (2007). Online Privacy as Legal Safeguard: The Relationship Among Consumer, Online Portal, and Privacy Policies. *New Media & Society, 9, nr. 5,* 715-734.
- Friedman, L. M. (2002). Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History. *Hofstra Law Review, 30, nr. 4,* 1093-1132.
- Genova, G. L. (2009). No Place to Play: Current Employee Privacy Rights in Social Networking Sites. *Business Communication Quarterly, 72, nr. 1,* 97-101.
- Gibbs, J. L., Ellison, N. B. & Lai, C. H. (2011). First Comes Love, Then Comes Google: An Investigation of Uncertainty Reduction Strategies and Self-Disclosure in Online Dating. *Communication Research, 38, nr. 1,* 70-100.
- Gilbert, F. (2012). Proposed EU Data Protection Regulation: The Good, the Bad, and the Unknown. *Journal of Internet Law, 15, nr. 10,* 20-34.
- Hasib, A. A. (2009). Threats of Online Social Networks. *International Journal of Computer Science and Network Security, 9, nr. 11,* 288-293.
- Helsper, E. J. (2010). Gendered Internet Use Across Generations and Life Stages. *Communication Research, 37, nr. 3,* 352-374.
- Hong, T., McLaughlin, M. L., Pryor, L, Beaudoin, C. E. & Grabowicz, P. (2005). Internet Privacy Practices of News Media and Implications for Online Journalism. *Journalism Studies, 6, nr. 1,* 15-28.
- Hutton, G. & Fosdick, M. (2011). The Globalization of Social Media. Consumer Relationships with Brands Evolve in the Digital Space. J*ournal of Advertising Research, 51, nr. 4,* 564-570.
- Jones, S., Johnson-Yale, C., Millermaier, S. & Pérez, F. S. (2009). U.S. College Students' Internet Use: Race, Gender and Digital Divides. *Journal of Computer-Mediated Communication, 14, nr. 2,* 244-264.

- Jung, A. M. (2011). Twittering Away the Right of Publicity: Personality Rights and Celebrity Impersonation on Social Networking Websites. *Chicago-Kent Law Review, 86, nr. 1*, 381-417.
- Jurgenson, N. & Rey, P. J. (2012). Comment on Sarah Ford's 'Reconceptualization of Privacy and Publicity. *Information, Communication & Society, 15, nr. 2*, 287-293.
- Kelm, O. R. (2011). Social Media: It's What Students Do. *Business Communication Quarterly, 74, nr. 4*, 505-520.
- Kerr, I. R. & Bornfreund, M. (2005). Buddy Bots: How Turing's Fast Friends Are Undermining Consumer Privacy. *Presence: Teleoperators & Virtual Environments, 14, nr. 6*, 647-655.
- Knight, M. (2012). Journalism as Usual: The Use of Social Media as Newsgathering Tool in the Coverage of the Iranian Elections in 2009. *Journal of Media Practice, 13, nr. 1*, 61-74.
- Kuzma, J. (2011). Empirical Study of Privacy Issues Among Social Networking Sites. *Journal of International Commercial Law & Technology, 6, nr. 2*, 74-85.
- Liao, Z. & Cheung, M. T. (2001). Internet-Based E-Shopping and Consumer Attitudes: An Empirical Study. *Information & Management, 38, nr. 5*, 299-306.
- Newell, B. C. (2011). Rethinking Reasonable Expectations of Privacy in Online Social Networks. *Richmond Journal of Law and Technology, 17, nr. 4*, 1-61.
- O'Brien, M. (2008). Law, Privacy and Information Technology: A Sleepwalk Through the Surveillance Society?. *Information & Communications Technology Law, 17, nr. 1*, 25-35.
- Pierson, J. & Heyman, R. (2011). Review of Article: "Social media and cookies: challenges for online privacy". *International Journal of Metric Analysis Research, Development and Innovation Datametrics, 4, nr. 1*, s.p.
- Preneel, B. (2012). Privacy: het einde van de rit?. *Karakter, 10, nr. 37*, 18-19.
- Quinn, A. (2007). Moral Virtues for Journalists. *Journal of Mass Media Ethics, 22, nr. 2/3*, 168-186.
- Sayed, N. (2011). Towards the Egyptian Revolution: Activists' Perceptions of Social Media for Mobilization. *Journal of Arab & Muslim Media Research, 4, nr. 2/3*, 273-298.
- Smith, J. A. (2008). Moral Guardians and the Origins of the Right to Privacy. *Journalism & Communication Monographs, 10, nr. 1*, 64-110.
- Sprague, R. (2009). Rethinking Information Privacy in an Age of Online Transparency. *Labor and Employment Law Journal, 25, nr. 2*, 395-417.

- Swire, P. P. (2003). Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy. *Hastings Law Journal, 54, nr. 5,* 847-873.
- Veltsos, J. R. & Veltsos, C. (2010). Teaching Responsibly With Technology-Mediated Communication. *Business Communication Quarterly, 73, nr. 4,* 463-467.
- Vincze, H. O. (2011). Social Networking in the News (Romanian News Media Representations of Online Social Networking). *Journal of Media Research, 4, nr. 3,* 3-18.
- Volkmer, C. J. (2004). Should Adware and Spyware Prompt Congressional Action?. *Journal of Internet Law, 7, nr. 11,* 1-18.
- Walrave, M., Vanwesenbeeck, I. & Heirman, W. (2012). Connecting and Protecting? Comparing Predictors of Self-Disclosure and Privacy Settings Use Between Adolescents and Adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6, nr. 1,* s.p.
- West, A., Lewis, J. & Currie, P. (2009). Students' Facebook 'Friends': Public and Private Spheres. *Journal of Youth Studies, 12, nr. 6,* 615-627.
- Whitehouse, G. (2010). Newsgathering and Privacy: Expanding Ethics Codes to Reflect Change in the Digital Media Age. *Journal of Mass Media Ethics, 25, nr. 4,* 310-327.
- X. (2011). Protecting Youths from Online Harassment: Cyberbullying and Sexting Are Among the Risks to Be Aware Of. *Harvard Mental Health Letter, 28, nr. 3,* 4.
- X. (2012). Watchdogs Criticize New Google Privacy Policy. *Information Management Journal, 46, nr. 3,* 7.
- X. (2012). Google Continues to Come Under Fire for Privacy Issues. *Information Management Journal, 46, nr. 4,* 8.
- Yaghoubi, N. M., Kord, B. & Shakeri, R. (2010). E-Government Services and User Acceptance: The Unified Models' Perspective. *European journal of Economics, Finance & Administrative Sciences, 3, nr. 24,* 36-49.
- Zahid, N., Mujtaba, A. & Riaz, A. (2010). Consumer Acceptance of Online Banking. *European Journal of Economics, Finance and Administrative Sciences,* 3, *nr. 27,* 44-52.
- Zansberg, S. D. & Fischer, J. K. (2011). Privacy Expectations in Online Social Media – An Emerging Generational Divide?. *Communications Lawyer, 28, nr. 3,* 26-34.

Periodicals

- Bradley, T. (2009). Protect Your Privacy on Facebook and Twitter. *PC World, 27, nr. 12,* 110-112.
- Brynko, B. (2011). Trust in Social Networking. *Information Today, 28, nr. 7,* 11.
- Deschenaux, J. (2010). Europeans Demand Greater Privacy. *HR Magazine, 55, nr. 6,* 99-104.
- Luyten, A. (2010). Het einde van de privacy: we zijn gezien. *Humo, 74, nr. 3650,* 10-15.

- Ms (2011). Hoe Google ons leven controleert. *Humo, 75, nr. 3716/47,* s.p.
- Neff, J. (2011). Why Social Networks Are Cool on Sharing. *Advertising Age, 82, nr. 18,* 7.
- Rainey, M. (2012). Fired Before You're Hired? The Impact of Social Media on the Workforce. *INSIGHT into Diversity, 79, nr. 1/2,* 18-21.
- Spanbauer, S. (2008). The Right Social Network for You. *PC World, 26, nr. 4,* 105-110.
- Tochner, S. (2012). California Restricts Employer Access to Workers' Social Media. *HR Magazine, 57, nr. 12,* 18.
- Wallace, B. (2000). Who's Reading Your Mail? Feds Have Their Eye on You. *PC World, 18, nr. 5,* 66.
- X. (2007). Internet History. From ARPANET to Broadband. *Congressional Digest, 86, nr. 2,* 35-37.
- Zuallaert, J. (2012). 'Er is steeds minder vrijheid op het internet'. *Knack, 42, nr. 40,* 66-71.
- Zuallaert, J. (2012). De eeuwige wafelenbak. *Knack, 42, nr. 40,* 72.

Congres

- Cullen, R. & Reilly, P. (2007, 03-06 januari). *Information Privacy and Trust in Government: A Citizen-Based Perspective from New Zealand*. Conference Papers gepresenteerd op de 40th Hawaii International Conference on System Sciences van 03-06 januari 2007 in Big Island (Hawaii). New Zealand: University of Wellington.

- Donsbach, W., Rentsch, M. & Mende, A. M. (2009, 21-25 mei). *The Ethics Gap: Why Germans Have Little Esteem and No Trust in Journalists*. Conference Papers gepresenteerd op de 60th Annual Conference of the International Communication Association van 21-25 mei 2009 in Chicago (IL). Dresden: Technische Universität.
- Humphreys, L., Krishnamurthy, B & Gill, P. (2010, 21-26 juni). *How Much Is Too Much? Privacy Issues on Twitter*. Conference Papers gepresenteerd op het congres van International Communication Association (Annual Meeting) van 21-26 juni 2010 in Singapore. Geraadpleegd 06 maart 2013 via http://www2.research.att.com/~bala/papers/ica10.pdf.
- Jennings, J. S. (2012, 05 augustus). *Right of Publicity Law Meets Social Media*. Conference Papers gepresenteerd op het congres van American Bar Association (Annual Meeting) van 05 augustus 2012 in Chicago, Illinois. Chicago: Pattishall, McAuliffe, Newbury, Hilliard & Geraldson LLP.
- Naaman, M., Boase, J. & Lai, C. (2010, 6-10 februari). *Is it Really About Me? Message Content in Social Awareness Streams*. Conference Papers gepresenteerd op de 2010 ACM conference on Computer supported cooperative work van 6-10 februari 2010 in Savannah (GA). New York: Association for Computing Machinery.

- Nisbet, E. & Gay, G. (2007, 24 mei). *Internet Use and the Amplification of Trust and Privacy Evaluations on Support for Government Internet Monitoring*. Conference Papers gepresenteerd op de International Communication Association van 24 mei 2007 in San Francisco (CA). Ohio: The Ohio State University.
- Tuunainen, V. K., Pitkänen, O. & Hovi, M. (2009, 14-17 juni). *Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook*. Conference Papers gepresenteerd op het congres van Bled eConference (eEnablement: Facilitating an open, effective and representative eSociety) van 14-17 juni 2009 in Bled (Slovenië). Bled: Univerza v Mariboru.
- Walrave, M. (2003, 27 mei). *E-Privacy Research: A New Disciplinary Borderland*. Conference Papers gepresenteerd op het congres van International Communication Association (Annual Meeting) van 27 mei 2003 in San Diego (CA). Antwerpen: Universiteit Antwerpen.
- Walrave, M. & Heirman, W. (2011, 25 mei). *Cyberteens: Balancing Between Self-Disclosure and Privacy Concerns?*. Conference Papers gepresenteerd op het congres van International Communication Association (Annual Meeting) van 25 mei 2011 in Boston (MA). Antwerpen: Universiteit Antwerpen.
- Zwarun, L., Yao, M. (2007, mei). *Intrusion, Threats, Rights, and Strategies: Using Multidimensional Scaling to Identify People's Perception of Internet Privacy*. Conference Papers gepresenteerd op het congres van International Communication Association (Annual Meeting) van mei 2007 in San Francisco (CA). Hong Kong: City University.

Rapport

- Boyles, J. L., Smith, A. & Madden, M. (2012). *Privacy and Data Management on Mobile Devices*.
  Geraadpleegd 28 februari 2013 via
  http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.
- Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T. & Carter, C. (2000). *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*.
  Geraadpleegd 28 februari 2013 via
  http://www.pewinternet.org/~/media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf.
- Gibson, D. (2002). *Email Security Risks and How To Reduce Them*.
  Geraadpleegd 04 februari 2013 (laatste consultatie 17 februari 2013) via
  http://www.davidgibson.com/Email%20Security%20Risks%20and%20How%20To%20Reduce%20Them.pdf.
- Livingstone, S., Kirwil, L., Ponte, C. & Staksrud, E. (2013). *In Their Own Words: What Bothers Children Online? With the EU Kids Online Network*.

Geraadpleegd 11 mei 2013 via http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf.

- Madden, M. (2012). *Privacy management on social media sites*. Geraadpleegd 22 februari 2013 via http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx.
- Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A. & Beaton, M. (2013). *Teens, Social Media, and Privacy*. Geraadpleegd 28 mei 2013 via http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_TeensSocialMediaandPrivacy_FINAL.pdf.
- Maurer, H., Balke, T., Kappe, F., Kulathuramaiyer, N., Weber, S. & Zaka, B. (2007). *Report on Dangers and Opportunities Posed By Large Search Engines, Particularly Google*. Geraadpleegd 04 februari 2013 (laatste consultatie 17 februari 2013) via http://www.iicm.tugraz.at/iicm_papers/dangers_google.pdf.
- TRUSTe (2012, 16 juli). *U.S. Consumer Findings from 2012 Online and Mobile Privacy Perceptions Report*. Geraadpleegd 01 maart 2013 via http://www.truste.com/about-TRUSTe/press-room/news_truste_releases_us_customer_findings_report.
- TRUSTe (2012, 12 september). *Online Behavioural Advertising, Self Regulation and Consumer Perceptions*. Geraadpleegd 01 maart 2013 via http://www.iabeurope.eu/media/106886/iab_europe_truste_webinar_9-12-2012.pdf.
- Walrave, M., Heirman, W., Jacquemin, H., Feld, J. & Coppens, F. (2011). *E-marketing & minderjarigen* (*Observatorium van de Rechten op het Internet*). Geraadpleegd 01 februari 2013 (laatste consultatie 17 februari 2013) via http://www.internet-observatory.be/internet_observatory/pdf/E-marketing_report_nl.pdf.
- Wüeest, C. (2005). *Threats to Online Banking (Virus Bulletin & Symantec)*. Geraadpleegd 04 februari 2013 (laatste consultatie 17 februari 2013) via https://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf.

Powerpointpresentatie

- Schneider, K. (2002). Threats to Email Security. Californië: Symantec Corporation.

Thesissen en doctoraten

- Spoel, I. van der (2012, 15 augustus). *Privacy zat. Informationele privacy herzien met de kritische blik van Foucault*. Utrecht: Universiteit Utrecht.

Internet

- Belle, B. van (2013, 01 januari). Controleer of uw gegevens ook gelekt werden door de NMBS.
  Geraadpleegd 02 januari 2013 (laatste consultatie 17 februari 2013) via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20130101_017&utm_source=facebook&utm_medium=social&utm_term=biz&utm_content=article&utm_campaign=seeding.
- Brenner, J. (2013, 14 februari). Pew Internet: Social Networking (full detail).
  Geraadpleegd 28 februari 2013 via http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx.
- Bvb (2012, 16 april). Klacht bij Raad voor de Journalistiek over berichtgeving Zwitserland.
  Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20120416_141.
- Cochez, T. (2012, 17 april). Klacht bij Raad voor de Journalistiek na busdrama in Sierre.
  Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.mediakritiek.be/index.php?page=7&detail=1465&7addda05552ee45fa3404584daaa7faa2c51c9f2=n1d2gk1ube5e5a309loq837a64.
- Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL).
  Geraadpleegd 28 februari 2013 via http://www.privacycommission.be/nl.
- Deltour, P. (2003). Incognito of met een alias naar de waarheid: over undercoverjournalistiek.
  Geraadpleegd 01 september 2012 (laatste consultatie 17 februari 2013) via http://www.journalist.be/sites/default/files/pdf/undercover.pdf.
- Deltour, P. (2003, augustus). Discussietekst: Naar een moderne journalistieke code ?.
  Geraadpleegd 01 september 2012 (laatste consultatie 17 februari 2013) via http://www.journalist.be/sites/default/files/pdf/nieuwe_deontologische_code.pdf.
- Demeyer, P. (2012, 27 september). Vergeet uw Facebookpagina niet op te nemen in uw testament.
  Geraadpleegd 27 september 2012 (laatste consultatie 17 februari 2013) via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20120926_00312840.
- Desmyttere, P. (2012, 18 februari). Is onze privacy in goede handen op sociale media?.
  Geraadpleegd 31 augustus 2012 (laatste consultatie 17 februari 2013) via

http://www.desmyttere.be/nl/nieuws/is-onze-privacy-in-goede-handen-op-sociale-media/.

- Dka & Hmp (2012, 05 november). Veerle Baetens zorgt voor deining op Twitter. Geraadpleegd 06 maart 2013 via http://www.nieuwsblad.be/article/detail.aspx?articleid=DMF20121104_00357437.
- Domi (2012, 19 september). Franse rechter geeft prinses Kate gelijk. Geraadpleegd 28 februari 2013 via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20120918_00301149.
- Gordon, W. (2012, 21 november). AdjustYourPrivacy Locks Down Your Entire Internet Life from One Page. Geraadpleegd 17 februari 2013 (laatste consultatie 17 februari 2013) via http://lifehacker.com/5962369/adjustyourprivacy-locks-down-your-entire-internet-life-from-one-page.
- Gordon, W. (2013, 03 januari). The Always Up-to-Date Guide to Managing Your Facebook Privacy. Geraadpleegd 17 februari 2013 (laatste consultatie 17 februari 2013) via http://lifehacker.com/5813990/the-always-up+to+date-guide-to-managing-your-facebook-privacy.
- Haegen, K. van der (2012, 05 december). Cookies: wat je moet weten over de nieuwe cookiewet. Geraadpleegd 28 februari 2013 via http://wijs.be/nl/trends-inzichten/blog/detail/cookies-wat-je-moet-weten-over-de-nieuwe-cookiewet.
- Haney, D. (2012, 24 oktober). Crime Online: Internet Dating Dangers. Geraadpleegd 15 februari 2013 (laatste consultatie 17 februari 2013) via http://www.hispanicbusiness.com/2012/10/24/crime_online_internet_dating_dangers.htm.
- Henry, A. (2012, 13 april). Collusion for Chrome Shows You Who's Tracking You on the Web, As You Browse. Geraadpleegd 17 februari 2013 (laatste consultatie 17 februari 2013) via http://lifehacker.com/5901674/collusion-for-chrome-shows-you-where-your-personal-data-is-going-on-the-web-as-you-browse.
- Holahan, C. (2008, 03 juli). Viacom vs. YouTube: Beyond Privacy (Business Week Online). Geraadpleegd 17 februari 2013 (laatste consultatie 17 februari 2013) via http://www.businessweek.com/stories/2008-07-03/viacom-vs-dot-youtube-beyond-privacybusinessweek-business-news-stock-market-and-financial-advice.
- Karch, M. (2013). Google Bomb. Geraadpleegd 28 februari 2013 via

http://google.about.com/od/g/g/googlebombdef.htm.

- Keymeulen, T. van (2001, 16 maart). Deontologische twijfels over online journalistiek. Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.standaard.be/artikel/detail.aspx?artikelid=DMA14032001_004.
- Leemputten, P. van (2009, 20 juli). Fiscus checkt Facebook en Netlog. Geraadpleegd 01 maart 2013 via http://www.zdnet.be/news/105328/fiscus-checkt-facebook-en-netlog/.
- Leemputten, P. van (2012, 18 september). Wat is zichtbaar voor wie?. Geraadpleegd 25 september 2012 (laatste consultatie 17 februari 2013) via http://www.zdnet.be/news/143368/facebookbericht-zaait-nutteloze-paniek/?utm_source=standaard&utm_medium=artikel&utm_term=hp-oranje&utm_campaign=crosspromo.
- Loa (2012, 24 september). Facebook ontkent dat bug privéberichten publiek maakt. Geraadpleegd 25 september 2012 (laatste consultatie 17 februari 2013) via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20120924_178.
- Mg (2012, 23 februari). Online privacy in America. Rights and wrongs. Geraadpleegd 28 februari 2013 via http://www.economist.com/blogs/schumpeter/2012/02/online-privacy-america.
- Mtm (2013, 04 januari). Burgemeester en politiechef dienen klacht in tegen Facebookpagina ‘Zelzaatse hoertjes'. Geraadpleegd 28 februari 2013 via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20130104_00421849.
- Nijs, Y. (2011, 28 september). Facebook wist deel van 'tracking cookies' na uitloggen. Geraadpleegd 06 maart 2013 via http://tweakers.net/nieuws/77058/facebook-wist-deel-van-tracking-cookies-na-uitloggen.html.
- Opgenhaffen, M. (2012, 25 september). Partycrashen, met of zonder Facebook. Geraadpleegd 26 september 2012 (laatste consultatie 17 februari 2013) via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20120924_00309315.
- Palis, C. (2012, 07 april). 7 Creepy Apps That Will Make You Paranoid About Your Privacy. Geraadpleegd 17 februari 2013 (laatste consultatie 17 februari 2013) via http://www.huffingtonpost.com/2012/04/06/creepy-apps_n_1403268.html.
- Pardoen, T. (2011). Undercover bij de belspelletjes: Maxime De Winne, de infiltrant van 'Basta'. Geraadpleegd 10 september 2012 (laatste consultatie 17 februari 2013) via http://www.humo.be/humo-archief/30686/undercover-bij-de-belspelletjes-maxime-de-winne-de-infiltrant-van-basta.

- Privacy Rights Clearinghouse (2012, augustus). Fact sheet 35: Social Networking Privacy: How to be Safe, Secure and Social.
  Geraadpleegd 31 augustus 2012 (laatste consultatie 17 februari 2013) via https://www.privacyrights.org/social-networking-privacy.
- Raad van de Journalistiek (RVDJ).
  Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.rvdj.be.
- Raad van de Journalistiek. Journalistieke code.
  Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.rvdj.be/journalistieke-code.
- RVDJ (2012, 12 april). Code wordt uitgebreid met richtlijn over het gebruik van informatie uit persoonlijke websites.
  Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.rvdj.be/nieuws/code-wordt-uitgebreid-met-richtlijn-over-het-gebruik-van-informatie-uit-persoonlijke-websites.
- RVDJ (2012, 12 april). Richtlijn over het gebruik van informatie en beeldmateriaal van persoonlijke websites en sociale netwerksites.
  Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.rvdj.be/uitspraak/richtlijn-over-het-gebruik-van-informatie-en-beeldmateriaal-van-persoonlijke-websites-en-s.
- Rdc (2013, 08 januari). ‘Facebookpagina met foto's dronken Leuvense studenten is inbreuk op privacy'.
  Geraadpleegd 28 februari 2013 via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20130108_00425984.
- Redactie HLN (2012, 23 maart). Raad voor de Journalistiek wil overleg met hoofdredacties na busramp.
  Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.hln.be/hln/nl/957/Binnenland/article/detail/1413344/2012/03/23/Raad-voor-de-Journalistiek-wil-overleg-met-hoofdredacties-na-busramp.dhtml.
- Rvs (2012, 31 oktober). Koningskwesties: Paleis trekt naar Journalistieke Raad.
  Geraadpleegd 01 november 2012 (laatste consultatie 17 februari 2013) via http://www.destandaard.be/artikel/detail.aspx?artikelid=DMF20121031_00353891.
- Sels, G. (2013, 13 maart). U bent een open Facebook. Wat u ‘leuk vindt' vertelt meer dan u denkt.
  Geraadpleegd 14 maart 2013 via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20130312_00501827.

- Simmons, A. (2012, 12 juni). What Are the Dangers of Skype?. Geraadpleegd 15 februari 2013 (laatste consultatie 17 februari 2013) via http://www.ehow.com/list_5925719_dangers-skype_.html.
- Stevens, A. (2013, 05 februari). Facebook vertelt waar je vrienden zijn. Geraadpleegd 15 februari 2013 (laatste consultatie 17 februari 2013) via http://www.standaard.be/mobilia/cnt/DMF20130205_059.
- Tib (2013, 05 februari). Peter Van De Veire bezorgt BV's schrik van hun leven. Geraadpleegd 15 februari 2013 (laatste consultatie 17 februari 2013) via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF20130205_035.
- Voorhoof, D. (2011, 26 januari). Facebook en de Raad voor de Journalistiek. Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.legalworld.be/legalworld/facebook-en-de-raad-voor-de-journalistiek.html?LangType=2067.
- VRT (2012, 25 april). Uitzending Terzake: Sociale media: een gevaar voor onze privacy?. Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.deredactie.be/cm/vrtnieuws/mediatheek/programmas/terzake/2.20873/2.20874/1.1283629.
- Wassom, B. (2012, 05 januari). 5 Predictions for Social Media Law in 2012. Geraadpleegd 11 november 2012 (laatste consultatie 17 februari 2013) via http://mashable.com/2012/01/05/social-media-legal-predictions/.
- Wlr (1991, 24 april). Practice; evidence -- Marcel and others v Commissioner of Police for the Metropolis and others. Geraadpleegd 28 februari 2013 via http://www.lawgazette.co.uk/news/practice-evidence-marcel-and-others-v-commissioner-police-metropolis-and-others.
- X. (1994, 17 februari). De Belgische Grondwet. Geraadpleegd 01 september 2012 (laatste consultatie 17 februari 2013) via http://www.senate.be/doc/const_nl.html.
- X. (1998, 30 januari). Standaard-journalisten nemen deontologische code aan. Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via http://www.standaard.be/info.aspx?topic=info.code.
- X. (1999, 19 april). International Safe Harbor Privacy Principles. Geraadpleegd 28 februari 2013 via http://ita.doc.gov/td/ecom/shprin.html.
- X. (2012, 16 april). Klacht bij Raad voor de Journalistiek na busramp. Geraadpleegd 22 mei 2012 (laatste consultatie 17 februari 2013) via

http://www.hbvl.be/nieuws/media-en-cultuur/aid1155109/klacht-bij-raad-voor-de-journalistiek-na-busramp.aspx.

- X. (2012, 27 augustus). Busongeval Sierre.
  Geraadpleegd 01 september 2012 (laatste consultatie 17 februari 2013) via http://nl.wikipedia.org/wiki/Busongeval_Sierre.

8. Bijlagen

BIJLAGE 1: DE NIEUWE RICHTLIJN NA DE BUSRAMP IN ZWITSERLAND

Richtlijn over het gebruik van informatie en beeldmateriaal van persoonlijke websites en sociale netwerksites

Het internet, meer bepaald persoonlijke websites en blogs, internetfora en sociale netwerksites, maakt het mogelijk dat persoonlijke gegevens, meningen en afbeeldingen worden gedeeld met een groot publiek.

Persoonlijke websites en sociale netwerksites kunnen voor de media een bron van informatie zijn. Het feit dat iemand persoonlijke gegevens, informatie of beeldmateriaal op het internet of op een sociale netwerksite plaatst, zelfs als het om publiek toegankelijke pagina's gaat, betekent evenwel niet automatisch dat dit materiaal zonder meer mag worden overgenomen in andere media.

Om dit materiaal toch te kunnen gebruiken, moeten een aantal afwegingen worden gemaakt.

1. Context van de informatie

1. De journalist houdt rekening met de aard en de doelstelling van de site, zelfs wanneer het gaat om publiek toegankelijke pagina's. Een site die zich vooral richt tot een specifieke groep of omgeving wordt anders behandeld dan een site of informatie die duidelijk bedoeld is voor het algemene publiek.

2. Wanneer de betrokkene zelf de toegang tot de informatie heeft beperkt, is gebruik in principe niet geoorloofd. De journalist moet aantonen dat er sprake is van een gewichtig maatschappelijk belang om het eventuele gebruik toch te rechtvaardigen.

3. Er is bijzondere terughoudendheid vereist wanneer informatie of beeldmateriaal wordt gebruikt dat in een totaal andere context of met een totaal andere bedoeling op het net werd geplaatst dan die van de nieuwsfeiten waarover bericht wordt. Verspreiding in de ene context betekent niet dat de informatie of het beeldmateriaal zomaar in een andere context mag worden gebruikt.

2. Maatschappelijk belang

4. De aantasting van het privéleven mag niet verder gaan dan noodzakelijk in het maatschappelijk belang van de berichtgeving. Het maatschappelijk belang moet van die aard zijn dat het recht op informatie het recht op privacy overstijgt.

5. Het gebruik zonder toestemming van herkenbaar beeldmateriaal kan enkel verantwoord worden in het licht van het maatschappelijk belang van de berichtgeving. De journalist moet dit maatschappelijk belang kunnen aantonen.

6. Hoewel ook bekende of publieke figuren recht hebben op respect voor hun privéleven, moeten zij meer dan anderen aanvaarden dat bepaalde privégegevens die door hen op het internet zijn geplaatst en die voor het publiek toegankelijk zijn, openbaar worden gemaakt in het kader van verslaggeving. Ook hier mag de aantasting van het privéleven evenwel niet verder gaan dan noodzakelijk in het maatschappelijk belang van de berichtgeving.

3. Personen in een maatschappelijk kwetsbare positie

7. Bijzondere terughoudendheid is vereist bij het bekend maken van gegevens of afbeeldingen die de identificatie mogelijk maken van mensen in een maatschappelijk kwetsbare positie, zoals minderjarigen, slachtoffers van criminaliteit, rampen en ongevallen, en hun familie.

8. Over zwaar gewonde en overleden slachtoffers die geen publieke figuren zijn, worden geen persoonlijke details vrijgegeven zo lang er geen zekerheid is dat de directe naasten werden ingelicht.

9. Bij slachtoffers die geen publieke figuren zijn, vergewist de journalist zich ervan dat hij informatie en beeldmateriaal, afkomstig van persoonlijke websites en sociale netwerksites, kan overnemen. Wanneer blijkt dat nabestaanden of slachtoffers zelf zich verzetten tegen de openbaarmaking, leeft de journalist dit verbod na.

4. Behandeling van de informatie

10. De journalist checkt de waarachtigheid van de informatie of de beelden. Hij gaat na of de informatie door de betrokkene zelf op het net werd geplaatst, dan wel door anderen zonder toestemming. In het laatste geval kan de informatie enkel gebracht worden indien er een gewichtig maatschappelijk belang mee gemoeid is.

11. Bij de selectie en de publicatie van de informatie, in het bijzonder van beelden, draagt de journalist er zorg voor dat deze aangepast is aan de omstandigheden van de berichtgeving. De journalist vermijdt overdrijving bij het vrijgeven van beelden en/of details, ook wanneer de feiten de publieke opinie sterk beroeren.

Brussel, 12 april 2012

BIJLAGE 2: SURVEY BIJ SCHOLIEREN EN STUDENTEN

Wat is je geslacht? (M/V)

Wat is jouw leeftijd? (jonger dan 10, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, ouder dan 26)

Welke opleiding volg je op dit moment?

- Secundair onderwijs (middelbare school)
- Hoger onderwijs - professionele bachelor
- Hoger onderwijs - academische bachelor
- Hoger onderwijs - masteropleiding
- Afgestudeerd en aan het werk
- Afgestudeerd en werkzoekende

In de volgende reeks vragen willen we meer weten over jouw online mediagebruik. Je krijgt nu een aantal mediaplatformen of toepassingen te zien. Het is de bedoeling dat je aangeeft hoe vaak je deze platformen of toepassingen gebruikt, dit op een schaal van 'nooit' tot 'de hele dag door'.

Gelieve per online platform of toepassing het juiste bolletje aan te vinken

	Nooit	Enkele keren per jaar	Enkele keren per maand	Enkele keren per week	Dagelijks (1X per dag)	Meerdere keren per dag	De hele dag door
Zoekmachine (vb. Google, Yahoo)							
(Web)mail (vb. Gmail, Hotmail)							
Chat (vb. Skype of Facetime)							
Facebook							
Twitter							
LinkedIn							
Foursquare							
YouTube							
Fotoplatform (vb. Instagram, Flickr)							
Nieuwssite (vb. hln.be, Standaard.be)							
Blog (vb. Wordpress, Tumblr)							
Forum (vb. hobbyforum, nieuwsforum)							
Koopplatform (vb. eBay, Groupon, iTunes)							
Online banking							
Schoolplatform (vb. Smartschool, Toledo, Blackboard)							
Apps (vb. Angry Birds, FarmVille, Weer-App)							
Streaming muzieksite (vb. Spotify, Deezer)							
Downloadplatform (vb. Torrent-sites)							

Als er gesproken wordt over schending van privacy, aan welke soort van mensen of instanties denk je dan? Met andere woorden: wie denk jij dat er geïnteresseerd kan zijn in wat je online doet of welke data je achterlaat om er gebruik of zelfs misbruik van te maken? Je mag deze in onderstaande tekstvak ingeven, gescheiden door een komma.

In dit deel van de vragenlijst gaan we per platform/online toepassing na in welke mate je denkt dat de volgende personen of instanties geïnteresseerd zijn in wat je op die platformen doet en/of welke data je er achterlaat. Gelieve dit aan te geven op een schaal van 'helemaal niet geïnteresseerd' tot 'heel geïnteresseerd'.

In welke mate denk je dat de onderstaande groepen geïnteresseerd zijn in wat je doet op **Zoekmachines (vb. Google, Yahoo)?**

	Helemaal niet geïnteresseerd	Niet geïnteresseerd	Neutraal	Geïnteresseerd	Heel geïnteresseerd
De site of het platform zelf	○	○	○	○	○
Politie, overheid	○	○	○	○	○
Commerciële bedrijven en banken	○	○	○	○	○
Partner, lief	○	○	○	○	○
Ex-partners, ex-lieven	○	○	○	○	○
Vrienden	○	○	○	○	○
Ex-vrienden/ex-vriendinnen	○	○	○	○	○
Familie (vb. ouders, broers, zussen)	○	○	○	○	○
Criminelen	○	○	○	○	○
Pedofielen	○	○	○	○	○
Journalisten	○	○	○	○	○
(Potentiële) werkgevers	○	○	○	○	○
Leerkrachten, docenten, directie	○	○	○	○	○

Idem voor: (web)mail, chat, Facebook, Twitter, LinkedIn, Foursquare, YouTube, fotoplatformen, nieuwssites, blogs, fora, koopplatformen, online banking, schoolplatformen, apps, streaming muzieksites en downloadplatformen.

Je bent nu halverwege!

In de volgende reeks vragen willen we graag weten welke mogelijke inbreuken/overtredingen op de volgende platformen kunnen worden begaan. Je mag per platform meerdere vakjes aanvinken. Telkens je denkt dat een bepaalde overtreding kan plaatsvinden op dat platform, vink je het vierkantje voor de beschrijving aan. Je kan dus per vraag meerdere opties aanduiden.

Welke mogelijke inbreuken/overtredingen kunnen plaatsvinden op Zoekmachines (vb. Google, Yahoo)?

- ☐ Identiteitsdiefstal
- ☐ Financiële fraude, oplichting
- ☐ Virussen, worms
- ☐ Hacking
- ☐ Spam
- ☐ Stalking
- ☐ Pedofilie
- ☐ Cyberpesten
- ☐ Journalistieke research (gebruik van gegevens en foto's)
- ☐ Controle, toezicht
- ☐ Discriminatie, racisme
- ☐ Doorverkopen van data aan derde partijen
- ☐ Inbraak (vb. na kenbaar maken van reisplannen)

Idem voor: (web)mail, chat, Facebook, Twitter, LinkedIn, Foursquare, YouTube, fotoplatformen, nieuwssites, blogs, fora, koopplatformen, online banking, schoolplatformen, apps, streaming muzieksites en downloadplatformen.

De enquête is bijna afgelopen! Bij de volgende twee vragen willen we nagaan hoeveel rekening je houdt met jouw privacy.

In welke mate hou jij op de volgende platformen rekening met een eventuele schending van je privacy online door bijvoorbeeld privacy-settings aan te passen of cookies te verwijderen? Gelieve dit aan te duiden om een schaal van 'helemaal niet' tot 'heel veel'.

	Helemaal niet	Amper	Een beetje	Veel	Heel veel
Zoekmachine (vb. Google, Yahoo)	○	○	○	○	○
(Web)Mail (vb. Gmail, Hotmail)	○	○	○	○	○
Chat (vb. Skype of Facetime)	○	○	○	○	○
Facebook	○	○	○	○	○
Twitter	○	○	○	○	○
LinkedIn	○	○	○	○	○
Foursquare	○	○	○	○	○
YouTube	○	○	○	○	○
Fotoplatform (vb. Instagram, Flickr)	○	○	○	○	○
Nieuwssite (vb. hln.be, Standaard.be)	○	○	○	○	○
Blog (vb. Wordpress, Tumblr)	○	○	○	○	○
Forum (vb. hobbyforum, nieuwsforum)	○	○	○	○	○
Koopaccount (vb. eBay, Groupon, iTunes)	○	○	○	○	○
Online Banking	○	○	○	○	○
Schoolplatform (vb. Smartschool, Toledo)	○	○	○	○	○
Apps (vb. Angry Birds, FarmVille, Weer-App)	○	○	○	○	○
Streaming muzieksite (vb. Spotify, Deezer)	○	○	○	○	○
Downloadplatform (vb. Torrent-sites)	○	○	○	○	○

Welke strategieën gebruik jij om jouw privacy online te beschermen? Je mag meerdere opties aanvinken en indien nodig bij 'andere' nog een eigen manier vermelden.

- ☐ Privacy-settings aanpassen
- ☐ Gebruikersovereenkomst op het platform lezen
- ☐ Nicknames gebruiken
- ☐ Cookies verwijderen
- ☐ Letten op wat je schrijft
- ☐ Letten op wat je online plaatst
- ☐ Opletten met wie je online communiceert
- ☐ Gebruik van specifieke firewall en/of anti-virussoftware
- ☐ Andere:

In deze allerlaatste vragen willen we jou een paar vragen stellen over je houding tegenover journalistiek en privacy.

Ben jij je ervan bewust dat journalisten jouw statusupdates, tweets, foto's en dergelijke kunnen gebruiken in bv. een krant om hun artikel op te smukken?

- Helemaal niet
- Amper
- Een beetje
- Voldoende
- Heel veel

Vind je dat journalisten dat mogen doen?

- Ja
- Ja, als het anoniem is
- Afhankelijk van context
- Nee

Vind je het geoorloofd dat journalisten met het busongeval in Sierre de foto's van de slachtoffertjes in de krant geplaatst hebben?

- Ja
- Nee
- Ik weet het niet

Vind je dat tweets/statusupdates van werknemers van Ford Genk in de krant geplaatst mogen worden?

- Ja
- Ja, als het anoniem is
- Afhankelijk van context
- Nee

Als iemand uit jouw naaste omgeving (familie, vrienden) iets zou overkomen (bv. ongeval), zou je het dan correct vinden dat zijn/haar foto met volledige naam in een krant geplaatst wordt of op televisie wordt getoond?

- Ja
- Nee
- Ik weet het niet

Als jou iets zou overkomen (bv. ongeval), zou je het dan correct vinden dat jouw foto met volledige naam in een krant geplaatst wordt of op televisie wordt getoond?

- Ja
- Nee
- Ik weet het niet

De enquête is afgelopen. Alvast bedankt voor je deelname! Als je kans wil maken op een waardebon, geef dan hieronder je e-mailadres zodat we contact met jou kunnen opnemen als je bij de winnaars bent. Gelieve daarna nog 1 maal op het pijltje te klikken om de enquête af te sluiten.

BIJLAGE 3: POTENTIËLE GEÏNTERESSEERDEN VOLGENS SCHOLIEREN EN STUDENTEN

Van de 346 respondenten hebben er 99 de vraag opengelaten (waardoor er maar 247 respondenten overblijven). Daarom is er een procent van antwoorden op 346 respondenten berekend en een op 247 respondenten:

Websites

1. Websites zelf (al dan niet gebruik makend van cookies): 3 (0,87% op 346 respondenten, 1,22% op 247 respondenten)
2. De oprichter(s)/beheerder(s) van de site: 7 (2,02% op 346 respondenten, 2,83% op 247 respondenten)
3. Sociale media (die informatie kunnen doorverkopen aan adverteerders): 5 (1,45% op 346 respondenten, 2,02% op 247 respondenten)
    a. **Facebook: 27 (7,80% op 346 respondenten, 10,93% op 247 respondenten)**
    b. Foursquare: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    c. **Geen Twitter, LinkedIn, Instagram…**
4. Zoekmachines: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    a. **Google: 12 (3,47%, 4,86% op 247)**
5. YouTube: 3 (0,87% op 346 respondenten, 1,22% op 247 respondenten)
6. Datingsites: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
7. **E-commerce (online shops, (online) verkopers, kledingsites zoals Zalando…): 18 (5,20% op 346 respondenten, 7,29% op 247 respondenten)**
8. Goksites: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
9. Pornosites: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

(Internet)criminelen

1. **(Internet)criminelen zelf: 15 (4,34% op 346 respondenten, 6,07% op 247 respondenten)**
    a. **Hackers (bv. *phishers*): 69 (19,94% op 346 respondenten, 27,94% op 247 respondenten)**
    b. **Dieven: 12 (3,47% op 346 respondenten, 4,86% op 247 respondenten)**
    c. Inbrekers (1 vermeldde na het aankondigen vakantie): 3 (0,87% op 346 respondenten, 1,22% op 247 respondenten)
    d. **Stalkers: 10 (2,89% op 346 respondenten, 4,05% op 247 respondenten)**
    e. **Pedofielen: 10 (2,89% op 346 respondenten, 4,05% op 247 respondenten)**
    f. **Mensen met kwade bedoelingen: 17 (4,91% op 346 respondenten, 6,88% op 247 respondenten)**
    Eén iemand vernoemde daarbij alleen jongens en mannen, een ander alleen oudere mensen. Twee noemden daarbij al meteen het kopiëren en misbruiken van foto's die personen van Facebook, Twitter, Instagram en andere websites kunnen halen.
    g. **Oplichters, fraudeurs, scammers (bijvoorbeeld bij online banking): 20 (5,78% op 346 respondenten, 8,10% op 247 respondenten)**
    h. Spammers (bijvoorbeeld door illegale bedrijven): 4 (1,16% op 346 respondenten, 1,62% op 247 respondenten)
    i. Shouldersurfers: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    j. Identiteitsdieven: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    k. Kidnappers: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    l. Psychisch gestoorde mensen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

Overheid

1. **De overheid zelf, overheidsbedrijven (1x genoemd): 45 (13,01% op 346 respondenten, 18,22% op 247 respondenten)**
    a. **Politie: 16 (4,62% op 346 respondenten, 6,48% op 247 respondenten)**
    b. Verzekeringen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    c. Belastingendienst, fiscus: 4 (1,16% op 346 respondenten, 1,62% op 247 respondenten)
    d. Justitie, de juridische tak: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
        i. Advocaten: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

    e. Veiligheidsdiensten, Staatsveiligheid: 5 (1,45% op 346 respondenten, 2,02% op 247 respondenten)
        i. CIA: 3 (0,87% op 346 respondenten, 1,22% op 247 respondenten)
        ii. FBI: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
        iii. Geheim agenten: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
2. Regering: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
    a. Politici: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
3. Buitenland
    a. USA: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
    b. China: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    c. EU: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

Economie

1. Banken: 3 (0,87% op 346 respondenten, 1,22% op 247 respondenten)
    a. Online banking, homebanking: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
2. **Grote (commerciële) bedrijven (al dan niet met gerichte reclame en/of die al dan niet cookies gebruiken) (vb. Telenet, Belgacom: 1x genoemd): 51 (14,74% op 346 respondenten, 20,65% op 247 respondenten)**
    a. Webbedrijven, grote internetbedrijven (die informatie doorverkopen aan adverteerders): 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
        i. Apple: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
        ii. Microsoft: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
        iii. Apps: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
        iv. Programma's: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    b. Bedrijfsleider: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    c. Vliegtuigmaatschappijen die na meerdere online bezoeken de prijs opdrijven: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    d. Fabrikanten, producenten: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
    e. Privébedrijven: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    f. Multinationals: 5 (1,45% op 346 respondenten, 2,02% op 247 respondenten)
    g. Grote ketens (en hun sites): 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
        i. Supermarkten: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
        ii. Winkels: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
3. E-commerce (zie websites)
4. Consumentenorganisaties: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
5. **Marketeers en marktonderzoekers, reclamebureaus, adverteerders: 74 (21,39% op 346 respondenten, 29,96% op 247 respondenten)**

(Academisch) onderzoek

1. Onderzoeksbureaus, onderzoekers: 6 (1,73% op 346 respondenten, 2,43% op 247 respondenten) (bijvoorbeeld voor interesses, of voor het aantal Facebookgebruikers per dag te berekenen, of het Nationaal Instituut voor de Statistiek)
2. (Communicatie)wetenschappers: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
3. Informatici: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
4. Scholen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    ➔ **Interessant! Zelf niet aan gedacht!**

Media

1. Grote mediaconcerns, grote productiebedrijven voor tv en audio: 3 (0,87% op 346 respondenten, 1,22% op 247 respondenten)
2. Journalisten: 5 (1,45% op 346 respondenten, 2,02% op 247 respondenten) (Iemand zegt specifiek voor bekende personen)
3. Mediaspecialisten: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

4. Twitterazzo's: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
5. Persfotografen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
6. Pers: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
7. Pr: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

Vrienden, familie, kennissen en schoolgenoten

1. Familie: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    a. (Overbezorgde) ouders: 4 (1,16% op 346 respondenten, 1,62% op 247 respondenten)
2. Vrienden (iemand zegt expliciet: geen misbruik!): 6 (1,73% op 346 respondenten, 2,43% op 247 respondenten)
    a. Ex-vrienden: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
        i. Mensen die boos op je zijn, waarmee je ruzie hebt: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
    b. Té verre zogezegde vrienden: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    c. Ex-lieven: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
3. Pestkoppen, cyberpesters: 5 (1,45% op 346 respondenten, 2,02% op 247 respondenten)
    a. Grappenmakers: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
        i. Mensen die anderen voor schut willen zetten: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
4. Roddelaars: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
5. Medeleerlingen: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
6. Leeftijdsgenoten: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
7. Kennissen: 2 (0,58% op 346 respondenten, 0,81% op 247 respondenten)
8. Buren: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

Werkgevers en leerkrachten

1. **(Toekomstige) werkgevers, werkgevers die controle uitoefenen: 34 (9,83% op 346 respondenten, 13,77% op 247 respondenten)**
2. Werknemers: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
3. Leerkrachten: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

Auteursrechtenorganisaties

1. SABAM: 4 (1,16% op 346 respondenten, 1,62% op 247 respondenten)
2. Muziek- en filmindustrie (waaronder artiesten) die het illegale downloaden willen tegengaan: 5 (1,45% op 346 respondenten, 2,02% op 247 respondenten)
3. Bioscopen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
4. Auteurs, beheerders van de data: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
5. Auteurs, artiesten zelf: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
6. Concurrenten: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
7. Concurrerende artiesten: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
    ➔ **Interessant! Zelf niet aan gedacht!**

Allerlei (te vaag)

1. Iedereen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
2. Willekeurige mensen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
3. Geïnteresseerden: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)
4. Gewone mensen: 1 (0,29% op 346 respondenten, 0,41% op 247 respondenten)

BIJLAGE 4: WAARGENOMEN POTENTIËLE GEÏNTERESSEERDEN: VERSCHILLEN TUSSEN JONGENS EN MEISJES

Onafhankelijke T-testen:

Zoekmachines:

1. Familie: t(173,768) = -2,841, p = 0,005
    a. Jongens: M = 2,64; SD = 1,110
    b. Meisjes: M = 3,01; SD = 1,022
2. Leerkrachten, docenten en directie: t(170,075) = -2,284, p = 0,024
    a. Jongens: M = 2,66; SD = 1,080
    b. Meisjes: M = 2,95; SD = 0,969

(Web)mail:

1. Ex-partner, ex-lief: t(336) = -2,867, p = 0,004
    a. Jongens: M = 2,30; SD = 1,106
    b. Meisjes: M = 2,68; SD = 1,135
2. Vrienden, vriendinnen: t(336) = -2,346, p = 0,020
    a. Jongens: M = 2,51; SD = 1,068
    b. Meisjes: M = 2,80; SD = 1,015
3. Ex-vrienden, ex-vriendinnen: t(335) = -3,704, p = 0,000
    a. Jongens: M = 1,97; SD = 0,958
    b. Meisjes: M = 2,24; SD = 1,049
4. Familie: t(336) = -2,290, p = 0,023
    a. Jongens: M = 2,78; SD = 1,069
    b. Meisjes: M = 3,07; SD = 1,045
5. Leerkrachten docenten en directie: t(164,788) = -2,411, p = 0,017
    a. Jongens: M = 2,45, SD = 1,149
    b. Meisjes: M = 2,77; SD = 0,996

Chat:

1. Partner, lief: t(146,014) = -2,566, p = 0,011
    a. Jongens: M = 3,58; SD = 1,135
    b. Meisjes: M = 3,90; SD = 0,858
2. Ex-partner, ex-lief: t(340) = -3,274, p = 0,001
    a. Jongens: M = 2,46; SD = 1,155
    b. Meisjes: M = 2,91; SD = 1,148
3. Vrienden, vriendinnen: t(340) = -3,682, p = 0,000
    a. Jongens: M = 2,96; SD = 1,142
    b. Meisjes: M = 3,42; SD = 0,994
4. Ex-vrienden, ex-vriendinnen: t(340) = -3,442, p = 0,001
    a. Jongens: M = 2,15; SD = 0,983
    b. Meisjes: M = 2,58; SD = 1,055
5. Familie: t(337) = -3,527, p = 0,000
    a. Jongens: M = 3,12; SD = 1,115
    b. Meisjes: M = 3,55; SD = 0,974
6. Pedofielen: t(340) = -3,233, p = 0,001
    a. Jongens: M = 3,04; SD = 1,435
    b. Meisjes: M = 3,55; SD = 1,263
7. Leerkrachten docenten en directie: t(163,428) = -2,429, p = 0,016
    a. Jongens: M = 2,26; SD = 1,075
    b. Meisjes: M = 2,56; SD = 0,949

Facebook:

1. Partner, lief: t(335) = -2,740, p = 0,006
    a. Jongens: M = 3,98; SD = 1,020
    b. Meisjes: M = 4,26; SD = 0,779

2. Ex-partner, ex-lief: t(164,018) = -3,923, p = 0,000
    a. Jongens: M = 3,23; SD = 1,168
    b. Meisjes: M = 3,76; SD = 1,028
3. Vrienden, vriendinnen: t(336) = -4,103, p = 0,000
    a. Jongens: M = 3,78; SD = 0,910
    b. Meisjes: M = 4,16; SD = 0,716
4. Ex-vrienden, ex-vriendinnen: t(336) = -3,627, p = 0,000
    a. Jongens: M = 2,95; SD = 1,190
    b. Meisjes: M = 3,45; SD = 1,132
5. Familie: t(155,487) = -3,795, p = 0,000
    a. Jongens: M = 3,58; SD = 0,982
    b. Meisjes: M = 3,98; SD = 0,807
6. Pedofielen: t(156,497) = -3,471, p = 0,001
    a. Jongens: M = 3,28; SD = 1,398
    b. Meisjes: M = 3,83; SD = 1,180

Twitter:

1. Partner, lief: t(142,860) = -2,325, p = 0,021
    a. Jongens: M = 3,26; SD = 1,326
    b. Meisjes: M = 3,62; SD = 1,070
2. Ex-partner, ex-lief: t(321) = -2,349, p = 0,019
    a. Jongens: M = 2,78; SD = 1,214
    b. Meisjes: M = 3,11; SD = 1,104
3. Vrienden, vriendinnen: t(144,404) = -2,675, p = 0,008
    a. Jongens: M = 3,18; SD = 1,251
    b. Meisjes: M = 3,57; SD = 1,024
4. Ex-vrienden, ex-vriendinnen: t(321) = -2,129, p = 0,034
    a. Jongens: M = 2,61; SD = 1,198
    b. Meisjes: M = 2,91; SD = 1,126
5. Familie: t(148,189) = -2,326, p = 0,021
    a. Jongens: M = 2,99; SD = 1,229
    b. Meisjes: M = 3,33; SD = 1,042
6. Criminelen: t(319) = -2,788, p = 0,006
    a. Jongens: M = 2,91; SD = 1,331
    b. Meisjes: M = 3,34; SD = 1,187
7. Pedofielen: t(150,496) = -3,697, p = 0,000
    a. Jongens: M = 2,78; SD = 1,389
    b. Meisjes: M = 3,40; SD = 1,224

LinkedIn:

1. Overheid en politie: t(302) = -2,669, p = 0,008
    a. Jongens: M = 2,99; SD = 1,156
    b. Meisjes: M = 3,36; SD = 1,089
2. Ex-partner, ex-lief: t(302) = -2,594, p = 0,010
    a. Jongens: M = 2,33; SD = 1,107
    b. Meisjes: M = 2,69; SD = 1,060
3. Ex-vrienden, ex-vriendinnen: t(299) = -2,156, p = 0,032
    a. Jongens: M = 2,30; SD = 1,062
    b. Meisjes: M = 2,59; SD = 1,029
4. Pedofielen: t(138,325) = -2,209, p = 0,029
    a. Jongens: M = 2,39; SD = 1,355
    b. Meisjes: M = 2,76; SD = 1,196

Foursquare:

1. Pedofielen: t(297) = -2,622, p = 0,009
    a. Jongens: M = 2,89; SD = 1,414
    b. Meisjes: M = 3,33; SD = 1,268
2. (Toekomstige) werkgevers: t(297) = -2,315, p = 0,021

    a. Jongens: M = 2,67; SD = 1,159
    b. Meisjes: M = 3,01; SD = 1,134
3. Leerkrachten, docenten en directie: t(297) = -2,697, p = 0,007
    a. Jongens: M = 2,32; SD = 1,071
    b. Meisjes: M = 2,67; SD = 1,010

YouTube:

1. Criminelen: t(324) = -2,353, p = 0,019
    a. Jongens: M = 2,18; SD = 1,152
    b. Meisjes: M = 2,47; SD = 0,988
2. Pedofielen: t(323) = -3,925, p = 0,000
    a. Jongens: M = 2,15; SD = 1,182
    b. Meisjes: M = 2,70; SD = 1,124

Fotoplatformen:

1. Ex-partner, ex-lief: t(306) = -3,025, p = 0,003
    a. Jongens: M = 2,73; SD = 1,149
    b. Meisjes: M = 3,16; SD = 1,074
2. Ex-vrienden, ex-vriendinnen: t(304) = -2,107, p = 0,036
    a. Jongens: M = 2,65; SD = 1,137
    b. Meisjes: M = 2,95; SD = 1,113
3. Familie: t(306) = -3,425, p = 0,001
    a. Jongens: M = 3,16; SD = 1,087
    b. Meisjes: M = 3,60; SD = 0,977
4. Criminelen: t(306) = -2,502, p = 0,013
    a. Jongens: M = 2,66; SD = 1,309
    b. Meisjes: M = 3,06; SD = 1,199

Nieuwssites:

1. Overheid en politie: t(324) = -2,822, p = 0,005
    a. Jongens: M = 2,53; SD = 1,129
    b. Meisjes: M = 2,92; SD = 1,132
2. Partner, lief: t(324) = -2,199, p = 0,029
    a. Jongens: M = 2,29; SD = 0,951
    b. Meisjes: M = 2,55; SD = 0,986
3. Ex-partner, ex-lief: t(325) = -2,679, p = 0,008
    a. Jongens: M = 1,82; SD = 0,859
    b. Meisjes: M = 2,10; SD = 0,873
4. Ex-vrienden, ex-vriendinnen: t(324) = -2,485, p = 0,013
    a. Jongens: M = 1,77; SD = 0,809
    b. Meisjes: M = 2,03; SD = 0,870
5. Familie: t(324) = -2,851, p = 0,005
    a. Jongens: M = 2,25; SD = 1,034
    b. Meisjes: M = 2,60; SD = 0,994
6. Criminelen: t(189,330) = -3,957, p = 0,000
    a. Jongens: M = 1,77; SD = 0,898
    b. Meisjes: M = 2,23; SD = 1,013
7. Pedofielen: t(324) = -3,155, p = 0,002
    a. Jongens: M = 1,78; SD = 0,900
    b. Meisjes: M = 2,15; SD = 0,962
8. Journalisten: t(150,974) = -2,324, p = 0,021
    a. Jongens: M = 3,45; SD = 1,433
    b. Meisjes: M = 3,85; SD = 1,254
9. (Toekomstige) werkgevers: t(324) = -2,521, p = 0,012
    a. Jongens: M = 2,52; SD = 1,203
    b. Meisjes: M = 2,87; SD = 1,126
10. Leerkrachten, docenten en directie: t(324) = -2,027, p = 0,043
    a. Jongens: M = 2,60; SD = 1,208

b. Meisjes: M = 2,89; SD = 1,128

Blogs:

1. Partner, lief: t(306) = -2,263, p = 0,024
    a. Jongens: M = 3,24; SD = 1,143
    b. Meisjes: M = 3,56; SD = 1,080
2. Ex-partner, ex-lief: t(132,895) = -2,039, p = 0,043
    a. Jongens: M = 2,59; SD = 1,210
    b. Meisjes: M = 2,90; SD = 1,080
3. Familie: t(305) = -3,119, p = 0,002
    a. Jongens: M = 2,99; SD = 1,171
    b. Meisjes: M = 3,43; SD = 1,076
4. Criminelen: t(307) = -3,204, p = 0,001
    a. Jongens: M = 2,53; SD = 1,300
    b. Meisjes: M = 3,03; SD = 1,187
5. Pedofielen: t(306) = -3,803, p = 0,000
    a. Jongens: M = 2,58; SD = 1,251
    b. Meisjes: M = 3,18; SD = 1,231

Fora:

1. Ex-vrienden, ex-vriendinnen: t(300) = -2,076, p = 0,039
    a. Jongens: M = 2,01; SD = 0,917
    b. Meisjes: M = 2,26; SD = 0,955
2. Familie: t(298) = -2,572, p = 0,011
    a. Jongens: M = 2,54; SD = 1,056
    b. Meisjes: M = 2,89; SD = 1,043
3. Criminelen: t(300) = -2,384, p = 0,018
    a. Jongens: M = 2,30; SD = 1,207
    b. Meisjes: M = 2,65; SD = 1,120
4. Pedofielen: t(299) = -3,036, p = 0,003
    a. Jongens: M = 2,28; SD = 1,179
    b. Meisjes: M = 2,74; SD = 1,180
5. Leerkrachten, docenten en directie: t(300) = -2,794, p = 0,006
    a. Jongens: M = 2,11; SD = 1,012
    b. Meisjes: M = 2,46; SD = 0,949

Koopplatformen:

1. Familie: t(312) = -2,318, p = 0,021
    a. Jongens: M = 2,80; SD = 1,156
    b. Meisjes: M = 3,12; SD = 1,095

Online banking

1. Vrienden, vriendinnen: t(313) = -3,182, p = 0,002
    a. Jongens: M = 1,92; SD = 0,932
    b. Meisjes: M = 2,29; SD = 0,915
2. Ex-vrienden, ex-vriendinnen: t(310) = -2,475, p = 0,014
    a. Jongens: M = 1,74; SD = 1,011
    b. Meisjes: M = 2,03; SD = 0,910
3. Familie: t(313) = -2,967, p = 0,003
    a. Jongens: M = 2,72; SD = 1,196
    b. Meisjes: M = 3,14; SD = 1,097
4. Pedofielen: t(311) = -3,633, p = 0,000
    a. Jongens: M = 1,83; SD = 1,120
    b. Meisjes: M = 2,33; SD = 1,100
5. (Toekomstige) werkgevers: t(139,176) = -2,081, p = 0,039
    a. Jongens: M = 2,37; SD = 1,231
    b. Meisjes: M = 2,68; SD = 1,071

6. Leerkrachten, docenten en directie: t(310) = -3,359, p= 0,001
    a. Jongens: M = 1,77; SD = 0,919
    b. Meisjes: M = 2,15; SD = 0,873

Schoolplatform

1. Overheid en politie: t(186,568) = -2,401, p = 0,017
    a. Jongens: M = 1,96; SD = 0,918
    b. Meisjes: M = 2,24; SD = 1,042
2. Partner, lief: t(321) = -2,364, p = 0,019
    a. Jongens: M= 1,91; SD = 0,934
    b. Meisjes: M = 2,19; SD = 0,959
3. Vrienden, vriendinnen: t(321) = -2,699, p = 0,007
    a. Jongens: M = 1,97; SD = 1,143
    b. Meisjes: M = 2,32; SD = 1,026
4. Familie: t(320) = -2,646, p = 0,009
    a. Jongens: M = 2,21; SD = 1,172
    b. Meisjes: M = 2,57; SD = 1,106
5. Criminelen: t(316) = -1,970, p = 0,050
    a. Jongens: M = 1,59; SD = 0,931
    b. Meisjes: M = 1,81; SD = 0,845
6. Pedofielen: t(321) = -2,812, p = 0,005
    a. Jongens: M = 1,57; SD = 0,918
    b. Meisjes: M = 1,89; SD = 0,952
7. (Toekomstige) werkgevers: t(320) = -3,191, p = 0,002
    a. Jongens: M = 1,87; SD = 1,092
    b. Meisjes: M = 2,32; SD = 1,156

Apps:

1. Familie: t(143,767) = -2,684, p = 0,008
    a. Jongens: M = 2,28; SD = 1,164
    b. Meisjes: M = 2,67; SD = 1,033
2. Pedofielen: t(310) = -2,178, p = 0,030
    a. Jongens: M = 1,85; SD = 1,099
    b. Meisjes: M = 2,14; SD = 1,045
3. (Toekomstige) werkgevers: t(310) = -2,358, p = 0,019
    a. Jongens: M = 1,98; SD = 1,093
    b. Meisjes: M = 2,30; SD = 1,082

Streaming muzieksites:

1. Overheid en politie: t(306) = -3,117, p = 0,002
    a. Jongens: M = 2,38; SD = 1,222
    b. Meisjes: M = 2,86; SD = 1,232
2. Criminelen: t(306) = -3,245, p = 0,001
    a. Jongens: M = 1,87; SD = 1,043
    b. Meisjes: M = 2,33; SD = 1,138
3. Pedofielen: t(306) = -2,264, p = 0,024
    a. Jongens: M = 1,82; SD = 1,006
    b. Meisjes: M = 2,10; SD = 0,961
4. (Toekomstige) werkgevers: t(306) = -2,083, p = 0,038
    a. Jongens: M = 1,99; SD = 0,994
    b. Meisjes: M = 2,25; SD = 1,009
5. Leerkrachten, docenten en directie: t(306) = -2,330, p = 0,020
    a. Jongens: M = 1,83; SD = 0,967
    b. Meisjes: M = 2,10; SD = 0,926

Downloadplatformen:

1. Partner, lief: t(151,211) = -2,127, p = 0,035

    a. Jongens: M = 2,60; SD = 1,194
    b. Meisjes: M = 2,91; SD = 1,110
2. Familie: t(313) = -2,196, p = 0,029
    a. Jongens: M = 2,46; SD = 1,168
    b. Meisjes: M = 2,77; SD = 1,130
3. (Toekomstige) werkgevers: t(312) = -2,198, p = 0,029
    a. Jongens: M = 2,15; SD = 1,040
    b. Meisjes: M = 2,44; SD = 1,101
4. Leerkrachten, docenten en directie: t(311) = -2,905, p = 0,004
    a. Jongens: M = 1,92; SD = 1,014
    b. Meisjes: M = 2,29; SD = 1,017

BIJLAGE 5: CORRELATIE TUSSEN PRIVACYBEWUSTZIJN EN WAARGENOMEN POTENTIËLE GEÏNTERESSEERDEN

	ZM	Mail	Chat	FB	TW	LI	FQ	YT	Foto	Nieuws	Blog	Forum	Koop	Bank	School	App	Muziek	Down-load	Aantal correlaties
Site zelf					0,132 0,030	0,206 0,001	0,172 0,006		0,166 0,008		0,191 0,002	0,128 0,039	0,258 0,000	0,133 0,025		0,148 0,016	0,144 0,019	0,231 0,000	11
Politie en overheid	0,114 0,048					0,186 0,003	0,148 0,019	0,129 0,027		0,156 0,008			0,232 0,000	0,256 0,000	0,187 0,001	0,248 0,000	0,210 0,001	0,191 0,001	11
Commerciële bedrijven en banken							0,132 0,037				0,141 0,022		0,135 0,025	0,266 0,000	0,150 0,011		0,230 0,000		6
Partner, lief	0,132 0,021				0,198 0,001	0,189 0,003	0,191 0,002		0,194 0,002	0,136 0,020	0,215 0,000	0,216 0,000	0,170 0,005	0,160 0,007	0,130 0,027	0,177 0,004			12
Ex-partner, ex-lief						0,168 0,008	0,126 0,047	0,195 0,001			0,189 0,002	0,162 0,009			0,233 0,000	0,198 0,001			7
Vrienden, vriendinnen		0,166 0,004			0,182 0,003	0,231 0,000		0,195 0,001	0,148 0,017		0,183 0,003	0,156 0,012	0,168 0,005		0,128 0,030	0,210 0,001		0,125 0,039	11
Ex-vrienden, ex-vriendinnen		0,171 0,003				0,153 0,016	0,179 0,002	0,179 0,002	0,145 0,020		0,146 0,018	0,131 0,034			0,233 0,000	0,214 0,000			8
Familie		0,214 0,000	0,119 0,041		0,266 0,000	0,201 0,001		0,151 0,009	0,127 0,000	0,152 0,009	0,225 0,000	0,225 0,000	0,215 0,000	0,178 0,003	0,136 0,021	0,207 0,001	0,174 0,004	0,166 0,006	15
Criminelen				0,130 0,024	0,136 0,026	0,151 0,017	0,144 0,022	0,179 0,002		0,130 0,026	0,235 0,000	0,261 0,000	0,167 0,005	0,256 0,000	0,208 0,000	0,252 0,000	0,205 0,001	0,245 0,000	14
Pedofielen		0,139 0,016		0,150 0,009	0,156 0,010		0,177 0,005	0,166 0,004	0,168 0,007	0,140 0,016	0,246 0,000	0,224 0,000	0,168 0,005		0,195 0,001	0,272 0,000	0,169 0,006	0,180 0,003	14
Journalisten		0,117 0,042				0,211 0,001	0,229 0,000	0,124 0,032	0,134 0,031			0,178 0,004			0,204 0,001	0,304 0,000	0,185 0,002		9
(Toekomstige) werkgevers		0,115 0,048	0,167 0,004		0,126 0,039		0,245 0,000			0,119 0,042	0,147 0,017	0,185 0,003	0,134 0,026		0,172 0,003	0,234 0,000	0,187 0,002	0,196 0,001	12
Leerkrachten, docenten en directie										0,148 0,011	0,139 0,024	0,177 0,004				0,232 0,000	0,234 0,000	0,184 0,002	6

Correlatie tussen privacybewustzijn en waargenomen potentiële geïnteresseerden (bovenste cijfer is ‘r’, het onderste het significantiegetal ‘p’)