‘Hoe zit het met mijn online privacy?’

Een onderzoek naar het privacybewustzijn wat betreft online privacy-kwesties onder Nederlandse jongeren die gebruikmaken van sociale media

Student naam:	Jessika Snel
Student nummer:	459673
E-mailadres:	jessika.snel@student.eur.nl

Supervisor:	Dr. M. Willekens
Tweede lezer:	Dr. B. C. M. Kester

Master Media Studies - Media & Cultuur

Erasmus School of History, Culture and Communication

Erasmus Universiteit Rotterdam

Masterthesis

Juni 2017

Aantal woorden: 28.787

‘HOE ZIT HET MET MIJN ONLINE PRIVACY?’

Een onderzoek naar het privacybewustzijn wat betreft online privacy-kwesties onder Nederlandse jongeren die gebruikmaken van sociale media

ABSTRACT

Het internet en sociale media bieden internetgebruikers de mogelijkheid om online te interacteren en content te delen. Vooral jongeren maken hier op actieve wijze gebruik van. De vormgeving en de aard van sociale media moedigen gebruikers aan om grote hoeveelheden persoonlijke gegevens weer te geven en te delen. Dit brengt echter ook privacyrisico’s met zich mee, dankzij het surveillance mechanisme waarop sociale media draaien. Sociale media en andere partijen gebruiken namelijk deze gegevens om winst te maken, maar ook om individueel gedrag te voorspellen, te beïnvloeden en zelfs te bepalen. Het behoud van (online) privacy is echter een probleem dat door velen wordt genegeerd. Men vindt privacy over het algemeen wel belangrijk, maar handelt hier nauwelijks naar, wat de privacy paradox heet. Een belangrijke reden hiervoor onder jongeren is onwetendheid; jongeren zijn zich vaak onbewust van de bewustzijnsexploitatie gedaan door bedrijven en missen digitale geletterdheid om zich hier beter tegen te beschermen. Dit onderzoek richt zich op in hoeverre het privacybewustzijn, bestaande uit de perceptie, aandacht en kennis wat betreft online privacy-kwesties, reikt onder Nederlandse jongeren vanaf 16 tot en met 29 jaar die gebruikmaken van sociale media. Via een online enquête is er data verzameld van 260 respondenten. Bevindingen toonden aan dat actief sociale mediagebruik en deels het opleidingsniveau van invloed bleken te zijn op de privacyperceptie en geslacht op de privacykennis. Leeftijd en privacykennis bleken van invloed te zijn op de kans dat respondenten van plan waren bewuste actie te ondernemen om de online privacy beter te beschermen. Aan de hand van de resultaten wordt geconcludeerd dat ook onder de onderzochte jongeren de privacy paradox aanwezig is, maar dat er een nuance noodzakelijk is, omdat de privacy paradox gedeeltelijk wordt tegengesproken; respondenten die op actievere wijze gebruikmaken van sociale media maakten zich namelijk minder zorgen over hun online privacy dan respondenten die op minder actieve wijze gebruikmaken van sociale media. Daarnaast wordt geconcludeerd dat het gebrek aan privacykennis onder de respondenten niet sociaal is gestructureerd, sinds leeftijd en opleidingsniveau hier niet van invloed op bleken te zijn. Tot slot wordt geconcludeerd dat dit onderzoek deels heeft bijgedragen aan het bijbrengen van reflectie, kennis en een kritischer bewustzijn over online privacy onder de respondenten, waarmee zij op bewustere wijze om kunnen gaan met het delen van persoonlijke gegevens op het internet en sociale media.

SLEUTELWOORDEN: *Online privacy, internet, sociale media, privacy paradox, privacybewustzijn*

Inhoudsopgave

1. Inleiding

1.1. Achtergrond

"Wat op het spel staat is geen individuele zorg van een paar privacy-voorvechters, maar een zaak die ons allemaal aangaat: we worden online gemanipuleerd zonder dat we mogen weten hoe" (Bart Jacobs, hoogleraar Computerbeveiliging aan de Radboud Universiteit Nijmegen, geciteerd in Martijn & Tokmetzis, 2016a, p. 2).

In 2013 onthulde voormalig CIA-medewerker Edward Snowden hoe de Amerikaanse nationale veiligheidsdienst (NSA) wereldwijd online communicatie in de gaten houdt zonder publiekelijk toezicht en buiten de grenzen van de Amerikaanse grondwet. Sindsdien is er veel meer aandacht voor privacy (Free Snowden, n.d.; Martijn & Tokmetzis, 2016a). Privacy zou de mogelijkheid van een persoonlijke levenssfeer moeten geven waarin het individu helemaal zichzelf kan zijn zonder de inmenging en bemoeienis van anderen (Blok, 2002; Schermer, 2007). Privacy betekent ook dat het individu zelf mag bepalen voor wie de persoonlijke levenssfeer beschermd blijft en wie daarover kennis mag verkrijgen (Blok, 2002). Echter, door de opkomst van moderne informatie- en communicatietechnologieën, zoals smartphones, tablets en vele (gratis) wifi hotspots, waarmee iedereen via het internet kan communiceren, producten kan kopen, betalingen kan regelen, informatie kan opzoeken, entertainment kan bekijken en ga zo maar door, beginnen de grenzen van de persoonlijke levenssfeer te vervagen. Ook wordt het steeds onduidelijker wie daar (onbedoelde) toegang tot heeft. Mensen worden namelijk continue gevolgd als zij online zijn, omdat bij alles wat zij doen een digitaal spoor achterlaten wat weer door verschillende digitale partijen wordt geanalyseerd en gebruikt (Martijn & Tokmetzis, 2016a). Het grote probleem daarvan is, is dat mensen niet kunnen zien door wie zij in de gaten worden gehouden (Martijn & Tokmetzis, 2016a). Volgens Martijn en Tokmetzis (2016) staat hierdoor (online) privacy onder druk.

Vorig jaar oktober trachtte de Nederlandse Publieke Omroep (NPO) meer bewustzijn over online privacy te creëren onder de Nederlandse bevolking door twee weken lang aandacht te besteden aan verscheidene onderwerpen gerelateerd aan privacy (NTR, 2016). In een van de uitgezonden programma's, *De Privacytest*, werden het publiek en de mensen thuis uitgedaagd om hun eigen privacybewustzijn onder de loep te nemen (AVROTROS, 2016a; NPO 3, 2016). In *De Privacytest* toonde ethisch hacker Wouter Slotboom aan hoe hackers toegang kunnen krijgen tot persoonlijke gegevens, via bijvoorbeeld *phishing* e-mail, waarmee hackers achter inloggegevens kunnen komen (AVROTROS, 2016a). Dit kan zelfs zo ver gaan dat wanneer er op zo'n link wordt geklikt de hardware van de computer wordt geblokkeerd en er een som geld wordt geëist om deze te deblokkeren, wat *randsomware* ofwel gijzelsoftware wordt genoemd (AVROTROS, 2016a). Op 12 mei 2017 vond een van de grootste internationale gijzelsoftware-aanvallen ooit plaats; meer dan 135.000 computers met het besturingssysteem van Windows binnen overheden, bedrijven en zelfs

ziekenhuizen in 99 verschillende landen verspreid over verschillende continenten werden geblokkeerd door *randsomware* (Houthuijs, 2017). Zo werden Spaanse telecom- en elektriciteitsbedrijven, Britse ziekenhuizen en het ministerie van Binnenlandse Zaken in Rusland getroffen (Houthuijs, 2017; "Waarschuwing voor grote internationale gijzelsoftware-campagne," 2017). Door de schaal en de snelheid van de verspreiding van de aanval wordt het ook wel een 'cyber apocalypse' genoemd (Houthuijs, 2017). De software-gijzeling had kunnen worden voorkomen als de nieuwste systeemupdate van Windows meteen was geïnstalleerd, maar veel bedrijven hadden dat niet gedaan (Houthuijs, 2017). Naast instanties zijn ook particulieren steeds meer het slachtoffer van cybercrime; in Nederland zijn vorig jaar 7.4 op de 100 personen slachtoffer geweest van een hack (CBS, 2017). Ook de Erasmus Universiteit van Rotterdam is vorig jaar november getroffen door een hackactie, waarbij persoonlijke informatie, zoals bankrekeningnummers, paspoortnummers en medische gegevens van mogelijk 17.000 medewerkers en studenten zijn buitgemaakt (Smaling, 2017). Ook deze hack was mogelijk door een veiligheidsprobleem in verouderde software (Smaling, 2017).

Sociale media zijn ook belangrijke spelers in het vervagen van de grenzen van de persoonlijke levenssfeer. Sociale media bieden (gratis) diensten aan in ruil voor persoonlijke informatie via de profielen die gebruikers hiervoor aan moeten maken. Daarnaast wordt er continue informatie over gebruikers verzameld wanneer deze van die diensten gebruikmaken. Ook voor sociale media geldt dat het voor de gebruikers zelf vaak onduidelijk is wie toegang heeft tot hun gegevens en wat er precies met die gegevens gebeurt. Zo stelt Facebook (2016b) bijvoorbeeld dat ze gegevens van hun gebruikers delen met groepen bedrijven die onderdeel van Facebook zijn. Facebook geeft de mogelijkheid in te zien om welke bedrijven dat gaat, maar om te weten wat deze bedrijven met de gedeelde gegevens doen moet de privacyvoorwaarden van elk bedrijf apart worden bekeken. Daarnaast verstrekt Facebook (2016b) ook gegevens aan leveranciers, serviceproviders en andere partners, die zich volgens Facebook aan een "strikte geheimhoudingsplicht [moeten houden] op een manier die in overeenstemming is met [het] gegevensbeleid [van Facebook] en de overeenkomsten die [Facebook] met hen [is] aangaan" (paragraaf Leveranciers, serviceproviders en andere partners). Wie deze partners zijn en wat de overeenkomsten zijn die Facebook met hen is aangegaan is ook onduidelijk.

Sociale media zijn wereldwijd populair en deze populariteit blijft groeien (Smeets, 2016; Van Lonkhuyzen, 2016). Ook in Nederland zijn sociale media populair; negen op de tien Nederlanders maakt gebruik van sociale media (Van der Veer, 2016). Vooral Facebook is populair waarvan meer dan 40 procent van het aantal Nederlandse gebruikers uit jongvolwassenen bestaat (Facebook, n.d.). Ook Instagram en Snapchat worden steeds populairder en met name onder jongeren; voor beide sociale media geldt dat meer dan de helft van de Nederlandse gebruikers bestaat uit jongeren (Oosterveer, 2016; Van der Veer, 2016). Door deze populariteit is er tijdens de privacy-weken van de NPO 3 ook expliciet gekeken naar de privacyvoorwaarden van het sociale medium Snapchat dat het goed doet onder Nederlandse jongeren (Oosterveer, 2016; Van der Veer, 2016). Het programma *Hunted* onthulde namelijk dat Snapchat niet zo onschuldig is als het lijkt (AVROTROS, 2016b). Via

Snapchat kunnen foto's en video's ofwel 'Snaps' naar vrienden worden gestuurd die vervolgens na bekeken te zijn weer verdwijnen. Wanneer de privacyvoorwaarden van Snapchat echter goed worden gelezen staat er dat Snapchat de locatie en alle informatie van het mobiele apparaat van de gebruiker registreert (Snap Inc., 2017). Daarnaast staat er ook in dat Snapchat niet kan voorkomen dat er screenshots van Snaps worden genomen via andere apps (Snap Inc., 2017). Ook staat er in de privacyvoorwaarden van Snapchat dat wanneer de gebruiker Snaps aan LiveStories toevoegt er toestemming wordt gegeven de content op te slaan en opnieuw kan worden uitgezonden door de zakenpartners van Snapchat zonder hierop aanspraak te kunnen maken (Snap Inc., 2017).
Ook andere instanties hebben getracht meer duidelijkheid te verkrijgen over de privacyvoorwaarden van sociale media. Naar aanleiding van informatie over de nieuwe privacyvoorwaarden van WhatsApp, uitgezocht door de groep Article 29 Working Party die bestaat uit privacy-waakhonden uit de 28 EU-landen (Sebag & Bodoni, 2016), rapporteerde de NOS dat WhatsApp, met het accepteren van de nieuwe privacyvoorwaarden, privégegevens van zijn gebruikers mag doorsturen naar Facebook, zoals het telefoonnummer en met wie er wordt geappt ("Privacy-waakhonden waarschuwen," 2016). Aan al bestaande WhatsApp-gebruikers werd door WhatsApp de mogelijkheid gegeven om binnen dertig dagen het delen van informatie aan Facebook uit te zetten via de instellingen ("Privacy-waakhonden waarschuwen," 2016), maar voor nieuwe WhatsApp-gebruikers geldt dat hun informatie automatisch wordt gedeeld met Facebook. Ook de Consumentenbond (2016) heeft aangegeven dat wanneer iemand ervaren heeft dat er slordig werd omgegaan met persoonlijke gegevens door welk bedrijf dan ook dit bij hen kan worden gemeld.

Dat ook de mensen zelf (online) privacy belangrijk vinden is te zien in verscheidene opiniepeilingen. Zo gaf 79 procent van de 24.143 ondervraagde internetgebruikers uit 24 verschillende landen aan dat zij bezorgd zijn dat hun informatie wordt doorverkocht (Centre for International Governance Innovation & IPSOS, 2016). In een andere opiniepeiling, afgenomen onder 28.000 Europese burgers, gaf slechts 15 procent aan dat zij het gevoel hebben controle te hebben over hun persoonlijke gegevens en gaf 70 procent aan dat zij bang zijn dat hun gegevens voor andere doeleinden worden gebruikt dan waar het oorspronkelijk voor is bedoeld (Eurobarometer, 2015). Ondanks dat veel mensen privacy belangrijk vinden, wordt er weinig naar gehandeld. Dit wordt ook wel de privacy paradox genoemd (Martijn & Tokmetzis, 2016a). Volgens Martijn en Tokmetzis (2016a) verliest privacy het vrij snel van andere waarden, zoals veiligheid, gemak en minder betalen. Men kiest vaak voor de gemakkelijkste weg en dat is niet de weg van het beschermen van de eigen privacy (Martijn & Tokmetzis, 2016a). Vooral jongeren kiezen voor de gemakkelijkste weg. Zo kwam uit het jongerenpanel JijVandaag (2016) naar voren dat 86 procent van de 1.135 ondervraagde Nederlandse jongeren van 12 tot en met 24 jaar online privacy belangrijk vindt en dat 50 procent zich echt zorgen maakt over zijn of haar online privacy (NPO Radio 1, 2016). Ondanks dat maar een op de vijf van de ondervraagde jongeren Facebook vertrouwt met zijn persoonsgegevens, stellen jongeren gebruikersgemak toch belangrijker te vinden, omdat hun hele sociale leven verbonden is aan sociale

media (JijVandaag, 2016; NPO Radio 1, 2016).

Een belangrijke reden die voor de privacy paradox wordt gegeven is een gebrek aan kennis onder internet- en sociale mediagebruikers (Batist, 2015; Schermer, 2007). Dit gebrek aan kennis kan voor een illusie van online privacy zorgen (Batist, 2015). Dit betekent dat de kennis en ideeën over de eigen online privacy, wat de gepercipieerde (online) privacy wordt genoemd, niet aansluiten bij de daadwerkelijke (online) privacy die de gebruiker wel of niet heeft, wat weer van invloed is op het hebben van een juist privacybewustzijn (Batist, 2015). Het concept van het privacybewustzijn wordt in dit onderzoek gebruikt zoals is geformuleerd door Van der Velden en El Emam (2013), namelijk; de perceptie, aandacht en kennis wat betreft online privacy-kwesties. Met perceptie wordt in dit onderzoek bedoeld hoe er op subjectieve wijze wordt gedacht over privacy op het internet en sociale media. Met aandacht wordt in dit onderzoek bedoeld de maatregelen die worden genomen om de eigen privacy op het internet en sociale media te beschermen. Tenslotte wordt met kennis in dit onderzoek bedoeld de mate van onjuiste en juiste kennis over privacy op het internet en sociale media. Er is weinig onderzoek gedaan naar het privacybewustzijn. In het onderzoek van TNO (2015), dat in Nederland de privacy-beleving onder de Nederlandse bevolking heeft onderzocht, kwam het privacybewustzijn ook aan bod. Dit ging echter eerder over de gepercipieerde privacy; wat mensen zelf denken te weten over hun online privacy, zoals of zij wel of niet denken te weten wie er toegang heeft tot hun gegevens en niet of dit ook strookt met de werkelijke privacy die zij hebben (TNO, 2015). Ook voor onderzoeken die zich meer hebben gericht op het privacybewustzijn onder jongeren, zoals de onderzoeken van Van der Velden en El Emam (2013) en Young en Quan-Haase (2013), geldt dat er is onderzocht hoe jongeren zelf hun online privacy denken te kunnen beschermen aan de hand van verschillende maatregelen, maar niet of deze maatregelen beschermend genoeg zijn.

Het internet en sociale media worden door de meeste mensen geassocieerd met positieve ontwikkelingen, omdat ze technologische vooruitgang representeren (Siapera, 2012). Volgens Siapera (2012) signaleert technologische vooruitgang verbeteringen binnen alle aspecten van het leven en er wordt dan ook binnen de maatschappij hierin veel geld geïnvesteerd. Bart Jacobs, hoogleraar computerbeveiliging aan de Radboud Universiteit, stelt dat men naast de digitale voordelen de ogen zeker niet mag sluiten voor de risico's van het computertijdperk, zeker niet na de wereldwijde gijzelsoftware-aanval op 12 mei 2017 (Houthuijs, 2017). Mensen staan nog te weinig stil bij de gevaren die op de loer kunnen liggen op het internet en sociale media en moeten zich gaan realiseren wat die gevaren kunnen betekenen en wat voor consequenties deze gevaren kunnen hebben (Martijn & Tokmetzis, 2016a). Er zou dan gesteld kunnen worden dat de digitale geletterdheid wat betreft informatie- en communicatietechnologie (ICT) onder de bevolking nog niet voldoende is (Livingstone, 2004). Door meer kennis te creëren over online privacy leert men op kritische en bewustere wijze om te gaan met de voordelen en nadelen van het internet en sociale media. Er komen al signalen van ouders die graag een vak in omgangsvormen van sociale media verplicht willen hebben in het basisonderwijs en voortgezet onderwijs (De Vreede, 2015; "Ouders: Geef kinderen les," 2015). Van

de ruim 85.000 mensen, die de onderwijsenquête van het AD hebben ingevuld, wil 63 procent dat omgaan met sociale media als verplicht vak binnen het basisonderwijs wordt gegeven en wil 51 procent dit als verplicht vak in het voorgezet onderwijs ("De mening van Nederland," 2015). Er zou echter ook nadruk moeten worden gegeven aan het privacy-aspect en de bescherming ervan.

1.2. Doel

Het doel van dit onderzoek is het onderzoeken van het privacybewustzijn wat betreft online privacy-kwesties onder Nederlandse jongeren vanaf 16 tot en met 29 jaar die gebruikmaken van sociale media. Reden hiervoor is het significante gebruik van sociale media door Nederlandse jongeren, zoals in de inleiding is beschreven. De onderzoeksmethode die hiervoor is gebruikt is een online enquête. Daarnaast is onderzocht of de gepercipieerde privacy die jongeren hebben afwijkt van de daadwerkelijke privacy die zij hebben, wat betekent dat er is onderzocht hoe groot het gebrek aan kennis is wat betreft online privacy. Dit gebrek aan kennis is onderzocht aan de hand van quizvragen in de enquête over online privacy-kwesties. Dit onderzoek heeft zich ook gericht op het vergroten van de initiële kennis over online privacy onder de onderzochte jongeren, door informatie te geven na elke quizvraag, waardoor de gepercipieerde privacy meer zal overeenkomen met de daadwerkelijke privacy.

Dit onderzoek heeft hiermee een vorm van actieonderzoek uitgevoerd, waarbij is getracht niet alleen de inzichten van de onderzoeker zelf te vergroten, maar ook dat van de onderzoeksobjecten (Reason & Bradbury, 2007). Dit onderzoek heeft ernaar gestreefd om reflectie, kennis en een kritischer bewustzijn over online privacy bij te dragen onder de onderzochte jongeren (Reason & Bradbury, 2007), wat er hopelijk voor heeft gezorgd dat zij wellicht zelf actie zullen ondernemen om hun online privacy beter te beschermen door bewuster om te gaan met het delen van persoonlijke gegevens op het internet en sociale media. De uitkomsten van dit onderzoek kunnen maatschappelijk relevant zijn voor institutionele toepassingen van mediawijsheid (Livingstone, 2004), zoals scholen die jongeren onderwijs kunnen geven hoe om te gaan met (de gevaren van) het internet en sociale media.

1.3. Onderzoeksvraag

De onderzoeksvraag luidt als volgt: in hoeverre reikt het privacybewustzijn, bestaande uit de perceptie, aandacht en kennis wat betreft online privacy-kwesties, onder Nederlandse jongeren vanaf 16 tot en met 29 jaar die gebruikmaken van sociale media? De subvragen die hierbij horen zijn:

- Wat is de perceptie onder de onderzochte jongeren aangaande privacy op het internet en sociale media?
- Wat is de aandacht in de vorm van maatregelen die onderzochte jongeren nemen om hun eigen privacy te beschermen op het internet en sociale media?

- Wat voor kennis hebben de onderzochte jongeren aangaande privacy op het internet en sociale media?
- Wat is van invloed op het privacybewustzijn wat betreft online privacy-kwesties onder de onderzochte jongeren?
- Wijkt de gepercipieerde privacy, die de onderzochte jongeren hebben, af van de daadwerkelijke privacy? (Hoe groot is het gebrek aan kennis over online privacy?)
- Zijn de onderzochte jongeren van plan bewuste actie te ondernemen om hun online privacy beter te beschermen, wanneer hun initiële kennis over online privacy is vergroot?

1.4. Thesisoverzicht

De volgende hoofdstukken betreffen het theoretisch kader, de methodologie, de resultaten en als laatste de conclusie. De thesis eindigt met de literatuurlijst en de appendices.

- Het theoretisch kader is opgedeeld in negen subhoofdstukken. Het eerste subhoofdstuk betreft het sociale mediagebruik onder jongeren. Het tweede subhoofdstuk past het concept van het panopticum op de huidige maatschappij toe. Het derde subhoofdstuk bespreekt de exploitatie van het bewustzijn dat het gevolg is van de digitale variant van het panopticum. Het vierde subhoofdstuk betreft de eendimensionalisering van de geest wat een gevolg is van de exploitatie van het bewustzijn. Het vijfde subhoofdstuk behandelt de verandering van het concept van privacy dankzij het digitale tijdperk. Het zesde subhoofdstuk belicht het concept van de privacy paradox. Het zevende subhoofdstuk bespreekt het concept van het privacybewustzijn. Het achtste subhoofdstuk licht de nieuwe digitale kloof toe en het negende subhoofdstuk bespreekt de hypotheses.
- In de methodologie komen achtereenvolgens de volgende onderdelen aan bod: de onderzoeksmethode; de dataverzamelingsmethode; de onderzoekspopulatie; het aantal eenheden van de steekproef; de operationalisering en tot slot de statistische testen die zijn gebruikt om de data te analyseren.
- In de resultaten worden allereerst de descriptieve resultaten besproken en vervolgens de afzonderlijke resultaten van de statistische testen.
- In de conclusie wordt er antwoord gegeven op de onderzoeksvraag en de bijbehorende subvragen door betekenis te geven aan de resultaten en worden de beperkingen van het onderzoek en aanbevelingen voor vervolgonderzoek besproken.

2. Theoretisch kader

Deze thesis onderzoekt in hoeverre het privacybewustzijn reikt onder jongeren vanaf 16 tot en met 29 jaar die gebruikmaken van sociale media. Zoals omschreven in de inleiding van dit onderzoek, bestaat het privacybewustzijn uit de perceptie, aandacht en kennis wat betreft online privacy-kwesties. Om het privacybewustzijn van de doelgroep te onderzoeken, gaat dit theoretische hoofdstuk allereerst in op het sociale mediagebruik onder jongeren. Vervolgens wordt het concept van het panopticum toegepast op de huidige maatschappij en wordt toegelicht hoe de digitale variant daarvan heeft gezorgd voor een steeds grotere exploitatie van het bewustzijn. Hierna wordt besproken hoever bewustzijnsexploitatie gaat en kan gaan en wat voor negatieve gevolgen dit kan hebben die betrekking hebben op de gehele maatschappij. Daarna wordt het concept van privacy belicht en hoe dit onderhevig is aan veranderingen in het digitale tijdperk. Vervolgens wordt het concept van de privacy paradox toegelicht, sinds het vooral jongeren zijn die privacy wel degelijk belangrijk vinden, maar weinig actie ondernemen om deze daadwerkelijk te beschermen. Daarna wordt het concept van het privacybewustzijn, aangaande het internet en sociale media, besproken. Hierna wordt de nieuwe digitale kloof toegelicht. Het theoretisch kader eindigt met een bespreking van de hypotheses.

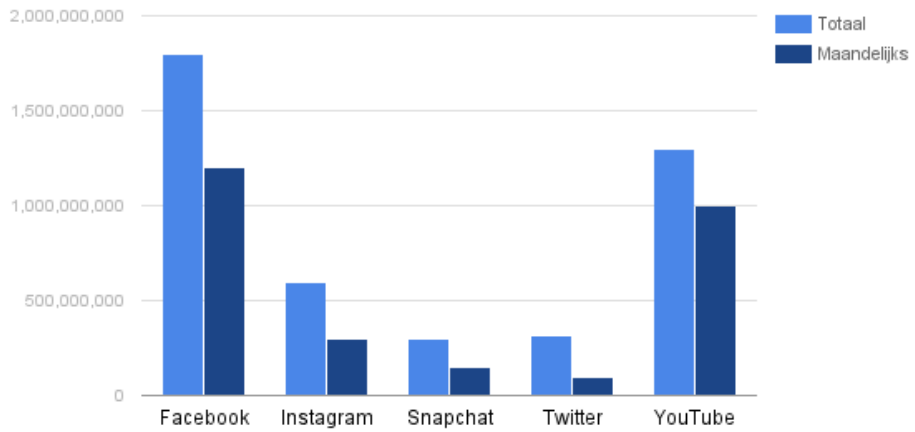
2.1. Sociale mediagebruik onder jongeren

Alle generaties verschuiven van traditionele naar digitale media (Sitompoel, 2015). De jongere generaties, die ook wel de *technoholics* en *digital natives* worden genoemd, zijn al heel erg digitaal in hun mediagebruik; de meerderheid van hun media-activiteiten vindt online plaats en dit zal de komende tijd alleen maar blijven groeien (Sitompoel, 2015). Het einde van het jaar 2013 markeerde het punt waarbij het aantal mensen die met digitale technologie opgroeien het aantal mensen die zich aan digitale technologie hebben moeten aanpassen overtrof (Van Eeden, 2014). Deze digitale generatie is gewapend met smartphones, tablets en laptops en verwacht te kunnen browsen, kijken, bloggen, luisteren, kopen en communiceren waar en wanneer dan ook en doen dit veelal via sociale media (Van Eeden, 2014).

Het internet en sociale media bieden nieuwe mogelijkheden voor het uitwisselen van informatie, kennis en cultuur (OECD, 2007). Het internet is de nieuwe afzetmarkt geworden voor creativiteit en heeft de aard van contentproductie veranderd, omdat de toetredingsbarrières voor het creëren van content zijn afgenomen of zijn verdwenen en de distributiekosten en kosten om content te produceren en te consumeren lager zijn (OECD, 2007). Dit heeft geleid tot een democratisering van mediaproductie; iemand hoeft geen professional meer te zijn om content te kunnen creëren (OECD, 2007). Vooral sociale media in de vorm van sociale netwerksites hebben internetgebruikers de mogelijkheid gegeven om aan de hand van een publiek of semipubliek profiel dat bestaat uit persoonlijke gegevens, zoals naam, leeftijd, foto en e-mailadres, online een persoonlijk netwerk te creëren dat in de meeste gevallen is bedoeld om mee te interacteren en content mee te delen (Boyd &

Ellison, 2007; Young & Quan-Haase, 2013).

Deze mogelijkheden hebben velen met beide handen aangepakt, waarmee sociale media zich zeer populair hebben gemaakt. Dit komt in meerdere cijfers naar voren (Figuur 1). Zo kwam uit de kwartaalcijfers van Facebook van maart 2016 naar voren dat er wereldwijd meer dan een miljard mensen dagelijks inloggen op Facebook, wat 16 procent meer is dan het jaar ervoor (Van Lonkhuyzen, 2016). Ook in mobielgebruik steeg het aantal actieve Facebookgebruikers met 24 procent (Van Lonkhuyzen, 2016). Facebook verwerkt naar eigen zeggen 60 miljard berichten per dag via Messenger en WhatsApp, wat drie keer zoveel is als het hoogtepunt van het wereldwijde sms-gebruik (Van Lonkhuyzen, 2016). Op Instagram loggen zo'n 300 miljoen mensen dagelijks in en het volledige aantal gebruikers blijft groeien; in december 2016 had Instagram meer dan 600 miljoen gebruikers wereldwijd, waarvan de laatste 100 miljoen gebruikers lid zijn geworden in de laatste zes maanden (Instagram, 2016; "Instagram stoomt door," 2016). Snapchat, dat in 2011 werd opgericht en daarmee een vrij jong sociaal medium is, heeft al meer dan 150 miljoen dagelijkse gebruikers en is daarmee Twitter voorbijgegaan dat 140 miljoen dagelijkse gebruikers heeft ("Snapchat heeft meer dagelijkse gebruikers," 2016).



Figuur 1. Sociale mediagebruikers wereldwijd in 2016, overgenomen uit "Cijfers: Welke social media heeft de toekomst in Nederland?" van Smeets, 2016 (http://www.dutchcowboys.nl/socialmedia/cijfers-welke-social-media-heeft-de-toekomst-in-nederland). Copyright 2016, Smeets.

Ook in Nederland zijn sociale media populair; 80.1 procent van de Nederlandse bevolking maakte in 2016 gebruik van sociale media (CBS, 2016). Het onderzoeksbureau Newcom Research & Consultancy voert sinds 2010 een grootschalig onderzoek uit naar het gebruik van sociale media onder Nederlanders ouder dan 15 jaar (Van der Veer, 2016). Uit hun cross-sectionele studie kwam naar voren dat het aantal sociale mediagebruikers in Nederland de afgelopen jaren is blijven groeien (Van der Veer, 2016). Uit hun landelijke onderzoek in 2016 kwam naar voren dat WhatsApp het grootste sociale mediaplatform is met 9.8 miljoen gebruikers, gevolgd door Facebook met 9.6 miljoen

gebruikers waarvan circa 42 procent tussen de 18 en 34 jaar is (Facebook, n.d.; Van der Veer, 2016). Daarnaast zijn Instagram, Snapchat en Pinterest vooral populair onder Nederlandse jongeren (Van der Veer, 2016). Van de 2.1 miljoen Nederlandse Instagrammers is 58 procent tussen de 15 en 19 jaar en 24 procent tussen de 20 en 39 jaar (Oosterveer, 2016). Snapchat, met 2 miljoen Nederlandse gebruikers, bestaat voor 56 procent uit jongeren tussen de 15 en 19 jaar en voor 11 procent tussen de 20 en 39 jaar (Oosterveer, 2016).

Wat sociale media populair maakt onder vooral jongeren is de mogelijkheid om met vrienden in contact te blijven en ermee te communiceren; om online een persoonlijk beeld of ook wel identiteit te ontwikkelen, waarbij zelf kan worden bepaald welke informatie naar voren wordt gebracht om zo een beter of positiever beeld van zichzelf te kunnen scheppen; om ideeën, meningen en andere vormen van content te delen; om zich te vermaken met entertainment en om hun sociale netwerken in het openbaar te publiceren (Boyd, 2008; Livingstone, 2008; Young & Quan-Haase 2013). Op deze manier zijn sociale media onderdeel van de dagelijkse leefwereld; informele ruimtes die als het ware een verlenging zijn van de privésfeer naar de online wereld (Baelden, 2013; Batist, 2015). De vormgeving en de aard van sociale media moedigen gebruikers aan om grote hoeveelheden persoonlijk gegevens weer te geven, omdat er geen persoonlijk beeld op sociale media kan worden ontwikkeld zonder enige persoonlijke informatie te delen (Baelden, 2013; Tufekci, 2008; Young & Quan-Haase 2013). Ondanks de genoemde voordelen heeft de openbaarmaking van persoonlijke gegevens op sociale media echter ook gezorgd voor privacyrisico's, dankzij het surveillance mechanisme waarop sociale media draaien.

2.2. Digitaal panopticum

Volgens Schnitzler (2015b) is de maatschappij in een digitaal panopticum terecht gekomen, dankzij de surveillance-technologieën op het internet en vooral op sociale media. De bedenker van het panopticum was de 18^{e}-eeuwse filosoof Jeremy Bentham. Bentham ontwierp het panopticum dat een gevangenisontwerp was waarmee gevangenen konden worden gedisciplineerd door de machtsbeoefenaar zichtbaar maar tegelijkertijd ook onzichtbaar te maken (Schnitzler, 2015b; Storey, 2012). Om dit te bewerkstelligen ontwierp Bentham de gevangenis in een ronde vorm met in het midden een wachttoren met geblindeerde ramen waarachter de gevangenisbewakers de gevangenen in de gaten konden houden (Schnitzler, 2015b; Storey, 2012). Hiermee was de machtsbeoefenaar zichtbaar voor de gevangenen, omdat zij uitkeken op de wachttoren die in hun midden stond, en anderzijds was de machtsbeoefenaar onzichtbaar, omdat de ramen van de wachttoren waren geblindeerd en de gevangenen daardoor niet konden zien of iemand hen op dat moment in de gaten hield (Schnitzler, 2015b). De gevangenen woonden daarmee in een transparante wereld waarin er geen plaats was om zich schuil te kunnen houden, omdat de gevangenen zich altijd bewust waren van de (mogelijke) aanwezigheid van de machtsbeoefenaar, al wisten zij dat nooit helemaal zeker en daar

kwam bovenop dat zij ook niet wisten door wie (welke bewaker) zij werden bekeken (Schnitzler, 2015b; Siapera, 2012). Er werd dus het gevoel gecreëerd dat de gevangenen altijd in de gaten konden worden gehouden, waardoor zij zich leerden te gedragen in de wetenschap dat zij anders zouden worden betrapt (Siapera, 2012). In plaats van gevangen lichamelijk te straffen, door middel van bijvoorbeeld foltering of openbare ophanging zoals werd gedaan voor 1800, werd surveillance ingezet om gevangenen te disciplineren (Foucault, 1989; Schnitzler, 2015b; Storey, 2012).

De Franse filosoof Michel Foucault (1989) paste het panoptische principe van Bentham toe op het dagelijkse leven, waar volgens hem ook op discipline gebaseerde machtsuitoefening plaatsvond. Volgens Foucault (1989) werd net als in gevangenissen ook in allerlei andere instellingen, zoals het onderwijs, het leger, de medische en psychiatrische zorg, de fabriek, maar ook binnen de familie, een vorm van macht uitgeoefend die zich richtte op discipline en het gezond maken van de ziel. Foucault (1981) benoemde deze op discipline gebaseerde machtsvorm ook wel 'biomacht', waarin er macht wordt verkregen over het biologische en sociale leven van de populatie via het disciplineren en onderscheiden van individuen. Individuen werden namelijk binnen afgesloten omgevingen geplaatst, zoals klaslokalen of ziekenhuiskamers, waarin zij voortdurend konden worden geobserveerd (Foucault, 1979; Leezenberg & De Vries, 2012). Via het observeren van individuen kon er kennis over de populatie worden verkregen, zoals geboorte- en ziektecijfers, en werden op basis hiervan normen opgesteld waarmee kon worden onderzocht of individuen afweken van deze normen in termen of iets normaal of niet normaal was, goed of slecht, gezond of ongezond, of wat iemand wel en niet mocht doen (Foucault, 1979, 1981; Leezenberg & De Vries, 2012; Storey, 2012). Biomacht werkt dus op basis van discipline en normalisering.

Na de Tweede Wereld Oorlog en mede dankzij de opkomst van de moderne informatie- en communicatietechnologieën begon de disciplinaire maatschappij vervangen te worden tot de huidige controlemaatschappij, waarin het individu is omgezet tot een datasubject (Deleuze, 1992; Schnitzler, 2013). In de controlemaatschappij lijkt vrijheid te zijn toegenomen. Mensen wordt immers niet meer beheerst door afgesloten ruimtes, zoals die van de school of de fabriek, maar men kan nu ook educatie in de eigen vrije tijd volgen en vanuit huis werken (Crain, 2013). Tegelijkertijd lijkt echter ook het in de gaten houden van menselijke activiteiten te zijn verhoogd (Crain, 2013). Het gebruik van surveillance-technologie om controle uit te kunnen oefenen is de afgelopen jaren namelijk toegenomen (Siapera, 2012). De mogelijke manieren en middelen om mensen en hun gedrag te observeren is volgens Siapera (2012) tevens explosief gegroeid. Zo zijn er bijna overal wel meerdere beveiligingscamera's te zien in openbare gebouwen, banken, winkels, pleinen, treinplatformen, vliegvelden, boven snelwegen en in bussen (Siapera, 2012). Omdat mensen weten te worden bekeken door onzichtbare handhavers, gedragen zij zich (over het algemeen) ook (Siapera, 2012). Via deze manier wordt bijvoorbeeld de maximumsnelheid op snelwegen gehandhaafd, want wanneer een autobestuurder te hard rijdt wordt deze geflitst en beboet, waarna die informatie wordt gekoppeld aan het kenteken en door de politie wordt bewaard (Martijn & Tokmetzis, 2016a). Vooral het internet

wordt gebruikt om menselijk gedrag te observeren zonder dat internetgebruikers dat weten (Martijn & Tokmetzis, 2016a). In plaats van surveillance wordt dit ook wel 'dataveillance' genoemd, wat een vorm van continue surveillance is via online data (Van Dijck, 2014). De overheid houdt burgers steeds meer in de gaten door het monitoren, registreren en verzamelen van data. De overheid doet dit om onder andere de orde te kunnen handhaven, veiligheid te kunnen bieden en criminaliteit, terrorisme en fraude te kunnen bestrijden (Martijn & Tokmetzis, 2016a). Steeds meer overheidsdatabases worden opgetuigd en aan elkaar gekoppeld, zodat de informatie effectiever kan worden gebruikt door verschillende overheidsinstanties, terwijl niet alle overheidsinstanties die data zelf zouden mogen vorderen (Martijn & Tokmetzis, 2016a).

Het monitoren van menselijk gedrag en bezigheden wordt echter steeds persoonlijker en men werkt daar zelf ook aan mee door zichzelf te onderwerpen aan zelfsurveillance (Schnitzler, 2015b). Dit gebeurt aan de hand van bijvoorbeeld persoonlijke klantenkaarten die scannen wat en wanneer iemand iets koopt, maar ook via het accepteren van (tracking) cookies op websites. Cookies registreren namelijk het surfgedrag, de locatie en informatie over de computer of laptop, zoals het IP-adres, waarmee een persoonlijk dossier wordt opgebouwd (Martijn & Tokmetzis, 2016a). Een cookie doet dit door een klein gecodeerd tekstbestandje op de harde schijf van de computer te zetten op het moment dat een website wordt bezocht (Consumentenbond, n.d.). Het aantal cookies kan per website tot in de tientallen oplopen. Zo vonden Martijn en Tokmetzis (2016a) via een tracking-tool wel 44 trackers, waarvan de meeste cookies zijn, op de nieuwswebsite Nu.nl. Ook via apps op smartphones worden er allerlei zaken geregistreerd, zoals de contactenlijst en de locaties waar de eigenaar in kwestie is geweest. Het gebruik van openbare wifinetwerken zorgt ook voor de registratie van allerlei gegevens. En gebruikers geven zelf ook een grote hoeveelheid aan persoonlijke informatie prijs via internet- en sociale mediaprofielen, zoals leeftijd, seksuele voorkeur, favoriete films, muziek, kledingsmaak enzovoort. Daarnaast geeft men ook informatie prijs over het eigen lichaam via slimme gadgets, zoals smartwatches die de hartslag en het calorieverbruik meten (Schnitzler, 2015b). Volgens Schnitzler (2013) verworden individuen steeds meer tot een datasubject; door *self-tracking* en het delen van eigen gedragspatronen, zet men zichzelf om tot kwantificeerbare data.

Volgens Schnitzler (2013, 2015b) is de maatschappij hiermee in een digitaal panopticum terecht gekomen waarbij de gevangenisarchitectuur vervangen is door het internet en het algoritme; het vermogen van computersystemen om grote hoeveelheden data te verwerken en daarin patronen en verbanden te ontdekken die anders onder de oppervlakte waren gebleven. Het controleren van het menselijk gedrag wordt steeds meer overgeheveld van menselijke observeerders naar computers (Haggerty & Ericson, 2000). Om de orde in stand te houden is het isolement dat individuen gescheiden houdt van anderen niet meer nodig; communicatie is nu de nieuwe voorwaarde om de orde in stand te houden (Schnitzler, 2015b). Sociale media, zoals Facebook, Instagram en Snapchat, zijn als het ware de nieuwe digitale cipiers geworden die de mens in het gareel houdt via zijn eigen communicatie- en informatiestromen, waaraan ze grof geld verdienen (Schnitzler, 2015b). Want sociale media

registreren alle inhoud die gebruikers op deze media achterlaten. In de voorwaarden van Facebook en Instagram staat bijvoorbeeld dat ze een licentie verkrijgen over de inhoud die gebruikers delen en deze inhoud dus mogen gebruiken voor hun eigen doeleinden, waaronder delen met andere partijen, zoals adverteerders (Facebook, 2015; Instagram, 2013). Voor Snapchat geldt dit voor de inhoud die publiekelijk wordt gedeeld via LiveStories (Snap Inc., 2017). En al zou iemand geen sociale media gebruiken kan Facebook deze persoon alsnog in de gaten houden doordat meer dan 10 miljoen websites een vind-ik-leuk-knop hebben geïnstalleerd, waardoor de websitebezoeker automatisch een cookie krijgt van Facebook waarmee hij of zij wordt gevolgd (Martijn & Tokmetzis, 2016a).

Daarnaast is de alziende blik van het digitale panopticum niet gecentraliseerd, zoals de wachttoren in Benthams gevangenis, maar juist gedecentraliseerd, omdat de positie van observant en geobserveerde tot op zekere hoogte uitwisselbaar zijn (Schnitzler, 2015b). Mensen kunnen zichzelf in de gaten houden aan de hand van apps die zijn geïnstalleerd op smartwatches en smartphones. Ook relaties met vrienden draait steeds meer om surveillance, omdat gebruikers aan de hand van hun sociale mediakanalen anderen in de gaten kunnen houden maar zelf door deze anderen ook kunnen worden bekeken (Trotter, 2012). Het nadeel vergeleken met het panoptische principe van Bentham is dat de alziende blik van het digitale panopticum bijna volledig verborgen is (Schermer, 2007; Schnitzler, 2015b). Mensen worden continue bespied; offline door camera's en online door allerlei partijen die van alles willen weten, zonder dat men hen kan zien of er weet van heeft (Martijn & Tokmetzis, 2016a). Waar de gevangenen zicht hadden op de wachttoren en dus wisten waarvandaan zij elk moment wellicht konden worden geobserveerd, is het in de huidige maatschappij niet duidelijk wie elkaar wanneer bekijkt (Schnitzler, 2015b). Daarnaast draait het bij het digitale panopticum niet meer om biomacht, maar om psychomacht; controle over de menselijke geest: "[Het] vermogen om te denken, te willen en te oordelen" (Schnitzler, 2015b, alinea 62).

2.3. Exploitatie van het bewustzijn

Nog voor de komst van het internet werd er al geprobeerd om het menselijk handelen te voorspellen (Schnitzler, 2015b). Na de industriële revolutie werd de menselijke geest ontdekt als een bron van waarde (Schnitzler, 2015b). Er werd en wordt steeds meer geprobeerd het menselijke bewustzijn – aandacht, emoties, fantasieën, verlangens en ideeën – te vangen, te sturen en te exploiteren (Schnitzler, 2015b; Van Looveren, 2015). En dat exploiteren gebeurt nu aan de hand van dataveillance dat het nieuwe verdienmodel is geworden op het internet (Martijn & Tokmetzis, 2016a; Van Dijck, 2014). De industrie kan door algoritmes en data opgeslagen in databases de bewustzijnsexploitatie steeds meer verwezenlijken, wat in feite betekent dat ze steeds meer macht hebben over het menselijk bewustzijn (Schnitzler, 2015b). Het omzetten van het menselijk gedrag in gekwantificeerde data wordt ook wel 'dataficatie' genoemd (Mayer-Schoenberger & Cukier, 2013). Steeds meer aspecten van het sociale leven worden gekwantificeerd, zoals vriendschappen, interesses,

emotionele reacties, gesprekken, zoekwoorden, expressies, maar ook Facebook-likes et cetera (Van Dijck, 2014). Het menselijk lichaam wordt dus steeds meer omgezet tot informatiestromen die vervolgens worden samengevoegd tot een dataprofiel (Haggerty & Ericson, 2000). Hierdoor krijgen bedrijven en andere instanties steeds meer toegang tot diepgaande en gedetailleerde data over gebruikers, om daarmee (klant)inzicht te krijgen die is gebaseerd op emotionele, psychologische en gedragsintelligentie (Schnitzler, 2014b; Van Eeden, 2014). Zo kwam in het onderzoek van Bits of Freedom samen met de Correspondent naar voren dat in Nederland meer dan tweehonderd bedrijven actief zijn die grote hoeveelheden persoonlijke data verzamelen over gebruikers en deze combineren om dataprofielen te maken en inzichten te creëren (De Zwart, 2015).

Deze data wordt dus gezien als handelswaar en wordt dan ook door de (sociale) media-industrie veelvuldig gebruikt om advertenties te plaatsen die afgestemd zijn op persoonlijke interesses en eigenschappen, zodat de kans groter is dat men daarop ingaat (Baelden, 2013). Zo verzamelt het advertentiebedrijf DoubleClick, overgekocht door Google in 2007 voor 3.1 miljard dollar, meer dan honderd eigenschappen van websitebezoekers om de meest geschikte advertenties te kunnen laten zien aan de juiste persoon (Martijn & Tokmetzis, 2016a). In datzelfde jaar begon Facebook inkomsten te genereren door advertenties te koppelen aan gebruikersactiviteiten en gebruikersvoorkeuren (Gane & Beer, 2008). Negen jaar later vermeldt Facebook (2016a) dat ze verkopers kunnen helpen om het menselijk gedrag te begrijpen, omdat ze informatie kunnen bieden die volgens eigen zeggen nergens anders te vinden is: “We provide marketers a true understanding of people − who they are, what they do and why they do it − … We look at what drives people to stop, look, feel, share, do and buy. We then translate what these insights mean for brands” (Facebook IQ, alinea 2). Facebook heeft namelijk gegevens over meer dan 1.7 miljard Facebook- en Instagramgebruikers en stelt dan ook een expertiseteam te hebben, bestaande uit onderzoekers, sociologen, wetenschappers, antropologen, trendspotters et cetera om de data te analyseren.

Hoe meer informatie en data bekend is over mensen en hun gedrag, hoe betere voorspellingen er kunnen worden gemaakt, wat weer leidt tot meer winst (Martijn & Tokmetzis, 2016a). Het afstellen op persoonlijke interesses en eigenschappen gebeurt niet alleen voor advertenties, maar ook voor het tonen van informatie. Algoritmes worden gebruikt om in te schatten wat voor informatie bij iemand past (Martijn & Tokmetzis, 2016a). Zo zijn de zoekresultaten van Google niet neutraal, maar gepersonaliseerd, wat betekent dat de ene persoon andere zoekresultaten kan krijgen dan de ander met dezelfde zoekterm (Martijn & Tokmetzis, 2016a). Niet alleen Google laat geen neutrale weergave van informatie zien, ook Facebook laat maar een fractie zien van alle berichten die vrienden hebben gedeeld (Martijn & Tokmetzis, 2016a). Aan de hand van de verzamelde gebruikersdata leveren steeds meer bedrijven gepersonaliseerde content en gebruiken aanbevelingen voor content die individuele gebruikers wellicht interessant vinden, zoals Spotify met nieuwe muziek, LinkedIn met nieuwe vacatures of nieuwe connecties en Netflix met nieuwe films en series (Martijn & Tokmetzis, 2016a; Van Eeden, 2014).

Volgens informatici De Rijke en Graus (2016) is gebrek aan neutraliteit helemaal niet zo onwenselijk. De Rijke en Graus (2016) stellen juist dat dit noodzakelijk is, omdat zoek- en aanbevelingssystemen ons in staat stellen "toegang te geven tot de bergen informatie, en ons nieuwe muziek of films te laten ontdekken. Met objectieve, neutrale algoritmen, zouden we niets meer kunnen vinden" (alinea 1). Er is gewoonweg te veel informatie en zonder deze zoek- en aanbevelingssystemen zouden mensen de bomen door het bos als het ware niet meer kunnen zien. Dan zouden mensen overspoeld raken door duizenden berichten op hun Facebookpagina (De Rijke & Graus, 2016). Daarom moet deze informatie worden gefilterd, omdat datgene waarnaar men op zoek is anders niet kan worden gevonden (De Rijke & Graus, 2016). Wat daarnaast ook belangrijk is om te beseffen, volgens De Rijke en Graus (2016), is dat het gebrek aan neutraliteit niet komt doordat machines worden verteld wat te doen, maar worden verteld om zelf te leren wat te doen. Algoritmes leren van mensen; van hun interesses, kliks, likes, surfgedrag et cetera en zijn daarmee een reflectie van de subjectieve mens (De Rijke & Graus, 2016). Zo worden er honderden (persoonlijke) kenmerken in beschouwing genomen om te bepalen welke resultaten er worden getoond (De Rijke & Graus, 2016).

Het nadeel van deze zoek- en aanbevelingssystemen is dat men als het ware in een filterbubbel terecht kan komen, waardoor men informatie, die men wellicht interessant had gevonden, over het hoofd ziet. Er wordt namelijk zonder dat men het doorheeft getracht gedragingen te beïnvloeden; bepaald wat men wel of niet belangrijk vindt (Martijn & Tokmetzis, 2016a). Door internetgiganten, zoals Facebook en Google, wordt een soort van venster aangereikt waardoor mensen de wereld ervaren zonder het besef dat dat venster er is (Martijn & Tokmetzis, 2016a). Keuzes en ervaringen worden wellicht vergemakkelijkt, maar tegelijkertijd beperkt. Hiermee komt de autonomie in het geding, wat betekent dat mensen steeds minder in staat zijn zelf beslissingen te kunnen nemen, omdat de keuzes en aanbevelingen voor hen worden gedaan zonder zich hier bewust van te zijn en zonder er kritisch op te kunnen reflecteren (Martijn & Tokmetzis, 2016a).

2.4. Eendimensionalisering van de geest

Het exploiteren van het menselijk bewustzijn gaat volgens Schnitzler (2015b) nog verder dan dat. Zo kunnen werkgevers via digitale profielen potentiële werknemers beoordelen of bestaande werknemers monitoren (Batist, 2015). Uit een onderzoek onder 825 recruiters bleek dat 73 procent van hen sociale media gebruikt om kandidaten te controleren (Levinson, 2010). Ook wordt er op sommige verkoopwebsites gediscrimineerd aan de hand van de locatie van de potentiële koper (Valentino-Devries, Singer-Vine, & Soltani, 2012). De Wall Street Journal kwam in 2012 erachter dat Staples Inc. verschillende prijzen toonde op de website voor hetzelfde product (Valentino-Devries et al, 2012). Deze prijs werd gebaseerd op het feit of de websitebezoeker in de buurt van een concurrent woonde en wanneer dat zo was kreeg hij of zij een gereduceerde prijs (Valentino-Devries et al., 2012). En zo wordt er meer geëxperimenteerd door websites, zoals het wel of niet tonen van bepaalde producten

voor verschillende websitebezoekers aan de hand van hun geo-locatie of browsergeschiedenis, zonder dat zij dit weten (Valentino-Devries et al., 2012).

Daarnaast worden er ook risicoprofielen opgesteld aan de hand van verzamelde data, waarmee individuen kunnen worden geïdentificeerd die mogelijk een gevaar voor de veiligheid zijn of voor hun eigen of andermans gezondheid (Haggerty & Ericson, 2000; Schnitzler, 2015b). Wanneer een individu een risicoprofiel krijgt toegeschreven kan er worden getracht zijn of haar handelen te voorspellen en aan te passen (De Zwart, 2015). Zo kunnen hiermee (potentiële) terroristen of belastingfraudeurs worden opgespoord (Schnitzler, 2015b). Ook zorgverzekeraars experimenteren met dataficering, waarbij de premie van de polis afhankelijk is van de hoeveelheid gedeelde data van de klant (Schnitzler, 2015b). Aan de hand van data, zoals eetgewoontes, drankgebruik en bewegingsgewoontes kan de gezondheid worden voorspeld en kan bijvoorbeeld de premie worden verhoogd wanneer bekend is dat iemand rookt of niet sport (Schnitzler, 2015b). Hiermee ontstaat er een nieuw veiligheidsbeleid dat Schinkel en De Graaf (2010) 'prepressie' noemen; een combinatie van preventie en repressie, wat wil zeggen dat er onder het mom van preventie repressief wordt opgetreden om risico's (risicopersonen) uit te sluiten. Dit heeft als gevolg dat de gewone burger steeds meer in de gaten wordt gehouden; iedereen vormt namelijk een potentieel risico (Schinkel & De Graaf, 2010).

Er wordt dus steeds meer digitaal geprofileerd, wat ook wel *social sorting* wordt genoemd, waarmee mensen in categorieën worden geplaatst "om de 'goeden' van de 'kwaden' te onderscheiden en daarmee risico's te voorkomen of kansen te benutten" (Martijn & Tokmetzis, 2016a, p. 142). Wie klikt wel op een advertentie en levert daarmee het meeste geld op, wie zal zich ontpoppen tot fraudeur, wie is betrouwbaar genoeg voor een lening et cetera (Martijn & Tokmetzis, 2016a). Hiermee leeft men steeds meer in een maatschappij die gebaseerd is op scores (Citron & Pasquale, 2014). Deze scores worden bepaald aan de hand van data van bijvoorbeeld buurtgegevens, de Kamer van Koophandel, kredietverleden en steeds vaker sociale media (Martijn & Tokmetzis, 2016a). Deze scores bepalen van wat voor diensten er gebruik mag worden gemaakt, zoals een lening aanvragen of het in aanmerking komen voor een bepaalde verzekering of baan en aan de hand van deze scores kan er worden voorspeld welk gedrag individuen hoogstwaarschijnlijk gaan vertonen (Citron & Pasquale, 2014; Martijn & Tokmetzis, 2016a; Solove, 2001). Kortom, kennis is macht; degenen die de meeste informatie over individuen bezitten kunnen het gedrag beïnvloeden, sturen of zelfs bepalen (Brunton & Nissenbaum, 2015; Martijn & Tokmetzis, 2016a; Schermer, 2007).

Volgens Schnitzler (2015a, 2015b) wordt hiermee de menselijke geest gereduceerd tot een eendimensionale interpretatie die geen geheimen meer heeft, zijn uniekheid verliest en net zo voorspelbaar en controleerbaar is als een machine. Volgens Mark Zuckerberg, de oprichter van Facebook, zijn de dagen, waarin vrienden, familie, collega's en onbekenden verschillende identiteiten van iemand te zien krijgen, ten einde gekomen (Fowler, 2012). Volgens Zuckerberg hebben Facebookgebruikers maar één identiteit (Fowler, 2012). Wie de menselijke geest probeert te reduceren tot iets eendimensionaals vergeet echter, volgens Schnitzler (2015b), dat het individu ook een product

is van allerlei andere zaken, zoals zijn of haar sociale en economische omgeving: “Weerbarstige vraagstukken, zoals de relatie tussen armoede en leefstijlen of tussen inkomensongelijkheid en maatschappelijke spanningen, verdwijnen daarmee uit zicht” (alinea 29). Ieder individu heeft meerdere identiteiten die gezamenlijk diens persoonlijkheid vormen (Schnitzler, 2015a). Volgens Schnitzler (2015a) kunnen deze identiteiten elkaar gedeeltelijk overlappen, maar nooit samenvallen tot een eendimensionaal beeld.

Het toedienen van (eendimensionale) digitale identiteiten, *social sorting* of (risico)scores kan als gevolg hebben dat er onterechte stempels op bepaalde individuen worden gedrukt. Omdat iemand wellicht niet altijd op tijd de belastingen betaalt hoeft dit niet te betekenen dat diegene dan ook een fraudeur is. De verzamelde data die wordt gebruikt om digitale dossiers op te bouwen geven geen genuanceerd portret van individuele persoonlijkheden weer, maar leggen alleen stereotypes en feiten vast, zonder de redenen erachter (Solove, 2001). Het zelf kunnen beïnvloeden van die (misplaatste) interpretatie lijkt echter onmogelijk te worden, omdat men gewoonweg niet weet waar dit vandaan komt en hoe dit tot stand komt (Februari, 2016). Hiermee kunnen gelijke behandeling en de onschuldpresumptie, wat betekent dat een persoon onschuldig is tot het tegendeel is bewezen, in het geding komen, omdat mensen in een hokje worden geplaatst en daarmee worden gediscrimineerd “gebaseerd op geautomatiseerde beslissingen” (Martijn & Tokmetzis, 2016a, p. 156). Subjectieve waarden kunnen niet zomaar worden omgezet tot objectieve waarden (Schnitzler, 2015b). Een computer kan nu eenmaal geen oorzaken berekenen tussen verbanden en kan ook geen neutrale berekeningen maken, omdat een computer van de subjectiviteit van mensen leert (Martijn & Tokmetzis, 2016a). Daarnaast zou men ook niet moeten willen dat alles − gedachtes en verlangens − bekend zou zijn. “Wie namelijk zijn psyche . . . al dan niet vrijwillig uit handen geeft, verliest feitelijk zichzelf” (Schnitzler, 2015b, alinea 43). Als een eendimensionale reductie verwordt het individu tot een object dat makkelijk kan worden gemanipuleerd. Gedachtes behoren tot een individu en zijn dan ook een voorwaarde voor zelfbeschikking; het recht om zelf beslissingen en keuzes te maken (Schnitzler, 2015b).

2.5. Privacy in het digitale tijdperk

Een gevolg van de explosieve toename aan surveillance-technologieën en het exploiteren van het menselijk bewustzijn is dat privacy op de tocht is komen te staan (Schnitzler, 2015b). In dit subhoofdstuk wordt besproken wat privacy betekent, hoe de focus van privacy aan het verschuiven is en hoe het onderscheid tussen de privé- en publieke sfeer wordt ondermijnt door de informatie- en communicatietechnologie.

2.5.1. Persoonlijke levenssfeer

De behoefte aan privacy is waarschijnlijk net zo oud als de mensheid zelf (Schermer, 2007). Ondanks dat er kan worden getwist over de precieze betekenis van het begrip 'privacy', verwijst dit begrip volgens Blok (2002) naar "een levenssfeer die eigen is aan de persoon" waar buitenstaanders in principe geen zeggenschap over hebben (pp. 277-8). Privacy wordt voornamelijk als een subjectief recht gezien, wat betekent dat het individu zelf mag bepalen voor wie de persoonlijke levenssfeer beschermd blijft en wie daarover kennis mag verkrijgen (Blok, 2002). Privacy is een selectieve controle over de kennisneming en toegang tot de eigen levenssfeer en kan daarmee als het ware worden gezien als een tegenwicht tegen andermans macht en controle (Altman, 1975; Blok, 2002; Schermer, 2007).

De persoonlijke levenssfeer, zoals opgesteld in de Nederlandse grondwet, is op te delen in vier verschillende kernonderdelen: ten eerste fysieke privacy of ook wel lichamelijke integriteit, wat gaat over het zelf bepalen wie het eigen lichaam aan mag raken; ten tweede ruimtelijke privacy of ook wel het huiselijke leven, wat gaat over het zelf bepalen wie daar toegang tot heeft en wie te weten krijgt wat daar gebeurt; ten derde relationele privacy, wat gaat over het vrijelijk aangaan van verschillende relaties, zoals seksuele of gezinsrelaties; en ten vierde communicationele privacy, wat gaat over de vrijheid om met anderen van gedachten te kunnen wisselen binnen vertrouwelijke kanalen, zoals via de post en de telefoon (Blok, 2002). Dan is er ook nog informationele privacy die betrekking heeft op persoonlijke gegevens, zoals naam en achternaam, huisadres, telefoonnummer, e-mailadres, burgerservicenummer, IP-adres, surfgedrag op het internet, ras, geloof en interesses; kortom allerlei informatie die direct over een persoon gaan ofwel naar een persoon te herleiden zijn (Autoriteit Persoonsgegevens, n.d.; Blok, 2002; Martijn & Tokmetzis, 2016a).

Volgens het Nederlandse grondrecht moet er op zorgvuldige wijze worden omgegaan met de verwerking van persoonsgegevens om de persoonlijke levenssfeer te respecteren (Blok, 2002). De Wet Bescherming Persoonsgegevens is in Nederland de belangrijkste wetgeving die de informationele privacy moet beschermen (Schermer, 2007). Deze wet geeft het individu het recht om zijn of haar persoonlijke gegevens verborgen te houden. Deze wet kent twee uitgangspunten, namelijk transparantie en keuzevrijheid. Transparantie betekent in dit geval dat bedrijven en overheden niet zomaar persoonlijke gegevens mogen verwerken, maar dat ze via privacyvoorwaarden moeten uitleggen wat ze ermee doen en waarom ze dat doen (Martijn & Tokmetzis, 2016a). Wanneer iemand akkoord gaat met de privacyvoorwaarden mag een bedrijf zijn of haar gegevens gebruiken. Het tweede punt is keuzevrijheid. Het individu moet de keuze hebben om wel of niet akkoord te gaan met het delen van persoonlijke gegevens (Nissenbaum, 2011). Ondanks dat de Wet Bescherming Persoonsgegevens draait om keuzevrijheid en transparantie, betekent dit niet dat het in de praktijk ook het geval is. Vaak is het zo dat men niet anders kan dan akkoord te gaan met het onthullen van persoonlijke gegevens, omdat er geen of weinig alternatief wordt geboden (Nissenbaum, 2011; Schermer, 2007). Ook zijn bedrijven vaak niet transparant met de redenen waarvoor ze persoonlijke

gegevens verzamelen en wat ze daarmee doen. Volgens Schermer (2007) beschermt het huidige privacy recht onvoldoende tegen de data die over individuen wordt verzameld. Om de gegevensbeschermingswetgeving toe te passen moet de verwerkte data direct of indirect een natuurlijk persoon kunnen identificeren (Schermer, 2007). Van veel data is echter onduidelijk of deze kunnen worden beschouwd als identificeerbare data, helemaal wanneer er wordt gekeken naar individuele stukjes data (Schermer, 2007). Of deze individuele stukjes data identificerend zijn of niet, wanneer deze datastukjes worden gecombineerd kan dat leiden tot een panoptisch effect dat van negatieve invloed kan zijn op individuen zonder te worden beschermd door de gegevensbeschermingswet (Schermer, 2007).

2.5.2. Informationele privacy als focus

Vanwege de snelle groei van informatie- en communicatietechnologieën is de focus van het privacy-debat verschoven van het beschermen van de meer klassieke dimensies van privacy, zoals het lichaam en de huiselijke sfeer, naar de bescherming van persoonlijke gegevens (Schermer, 2007). Veel van de activiteiten in de maatschappij zijn voor een groot deel afhankelijk van de verwerking van (persoonlijke) data (Schermer, 2007). Volgens Mark Zuckerberg zijn mensen gewend geraakt aan het delen van persoonlijke informatie met anderen en is privacy daardoor niet langer een sociale norm (Johnson, 2010; Martijn & Tokmetzis, 2016a). Volgens Nissenbaum (2011) is het echter niet juist om te concluderen dat de privacynorm is veranderd door nieuwe technologieën. Nissenbaum (2011) stelt dat de privacynorm online hetzelfde is als offline, omdat de dingen die men online doet bijna allemaal zijn gerelateerd aan uiteenlopende offline contexten; zoals het doen van aankopen, het nieuws lezen, het luisteren van muziek en het contact onderhouden met vrienden. Al deze zaken doet men ook offline en zijn gerelateerd aan diens offline leven en daarom zou de online privacy niet anders moeten worden beoordeeld dan de offline privacy (Nissenbaum, 2011). Wanneer men bijvoorbeeld geld wil overmaken naar de bank via het internet betreft de context het doen van financiële zaken met de bank en niet internetbankieren met allerlei nieuwe regels, zoals het verzamelen en doorverkopen van data aan adverteerders (Martijn & Tokmetzis, 2016a; Nissenbaum, 2011). Dit gebeurt namelijk ook niet wanneer men naar de bank zelf gaat om geld over te maken (Martijn & Tokmetzis, 2016a; Nissenbaum, 2011). Dit betekent dat de online privacy dus continue wordt geschonden doordat er allerlei informatiestromen over individuen naar bedrijven gaan waar zij geen weet van hebben, terwijl dat in de offline wereld zeer opgepast zou zijn in vergelijkbare situaties (Martijn & Tokmetzis, 2016a).

Bedrijven beargumenteren veelal dat die informatiestromen op anonieme of onpersoonlijke wijze gebeuren, maar desondanks verzamelen vele websites informatie die direct te herleiden zijn tot individuen, zoals voor- en achternaam, e-mailadres, woonadres, seksuele oriëntatie en medicijngebruik, en verkopen dit weer door aan derde partijen, zoals adverteerders (De Zwart, 2015; Valentino-Devries & Singer-Vine, 2012). Onpersoonlijke gegevens kunnen ook veel onthullen; de registratie van een kenteken kan bijvoorbeeld onthullen waarnaartoe iemand reist, waar diens werk is

en waar hij of zij vaak parkeert (Martijn & Tokmetzis, 2016a). Ook aan de hand van Facebook-likes kan onder andere iemands seksuele geaardheid, politieke opvattingen of intelligentie op vrij accurate wijze worden voorspeld (Kosinski, Stillwell, & Graepel, 2013). Kortom, allerlei persoonlijke zaken kunnen uit 'onpersoonlijke' gegevens worden afgeleid (Martijn & Tokmetzis, 2016a). Men laat (zelf) dus steeds meer digitale sporen achter in diens dagelijkse interacties die een steeds accuratere digitale kopie van de eigen identiteit weergeven (Schermer, 2007). En dan is het ook nog zo dat persoonlijke data die nu nog privé zijn dat in de toekomst wellicht niet meer zullen zijn (Martijn & Tokmetzis, 2016a). Bedrijven kunnen namelijk hun privacyvoorwaarden aanpassen waarmee de manieren waarop persoonlijke data worden gebruikt kunnen veranderen (Martijn & Tokmetzis, 2016a; Nissenbaum, 2011). Zo heeft Google in 2012 zijn privacybeleid aangepast om (bijna) alle informatie die ze hebben over hun gebruikers te kunnen combineren, waarmee digitale identiteiten nog accurater worden (Angwin & Valentino-Devries, 2012). Ook Facebook heeft in de loop der jaren zijn privacyvoorwaarden meerdere keren aangepast; sinds de aanpassing in 2009 kan Facebook meer gebruikersdata verzamelen dan daarvoor en sinds de aanpassing in 2011 kan Facebook gebruikersdata delen met adverteerders, terwijl Facebook daarvoor had beloofd dat niet te doen (Martijn & Tokmetzis, 2016a). De controle die privacy hoort te geven over wie toegang zou mogen hebben tot de informationele privacy begint hierdoor steeds meer te eroderen, omdat men geen controle meer heeft over de manier waarop persoonlijke gegevens worden gebruikt of zullen worden gebruikt in de toekomst (Solove, 2001).

2.5.3. Vervagend onderscheid tussen de privé- en publieke sfeer

Waar er eerst nog een duidelijk onderscheid was tussen de privésfeer en de publieke sfeer begint dit onderscheid tussen publiek en privé steeds vager te worden (Martijn & Tokmetzis, 2016a; Schermer, 2007; Schnitzler, 2015b; Siapera, 2012). Waar de privésfeer betrekking heeft op zaken die niemand anders aangaan dan het individu en waarbinnen er wordt gestreefd naar eigen belangen, heeft de publieke sfeer betrekking op zaken die voor iedereen toegankelijk zijn en is deze gericht op het algemene belang (Blok, 2002). Internetgiganten, zoals Facebook en Google, doen er echter alles aan om het gehele gordijn tussen deze twee sferen naar beneden te trekken door zoveel mogelijk data te verzamelen en mensen actief op het internet en sociale media te pushen deze vrijwillig af te geven (Schnitzler, 2015b). Ook mensen zelf schuiven dit gordijn steeds verder opzij, doordat men de buitenwereld steeds meer koppelt aan de binnenwereld: via alle slimme apparaten in huis, zoals een slimme thermostaat, een smartwatch of een interactieve televisie; via cookies op computers, laptops en smartphones, die allerlei data over de eigenaars registreren en communiceren met andere partijen; en via individuele vrijwilligheid om gegevens online te delen (Martijn & Tokmetzis, 2016a; Schnitzler, 2015b). Hierdoor wordt men gevolgd tot in het eigen huis, dat toch echt bij de privésfeer hoort, waarbij een "duizendkoppig monster [meeleest en meeluistert]" (Schnitzler, 2015b, alinea 45). Een voorbeeld om aan te geven in hoeverre de privésfeer al is aangetast komt uit een reportage uit de New

York Times. Hierin kwam naar voren dat de Amerikaanse kortingsketen Target zwangere vrouwen als doelgroep had bestempeld aan de hand van hun aankooppatronen (Duhigg, 2012; Schnitzler, 2015b). Via een lijst van bepaalde producten, die zwangere vrouwen meer schijnen te kopen, kon het zwangerschapsstadium worden berekend en kon de kortingsketen deze vrouwen gerichtere aanbiedingen verschaffen (Duhigg, 2012). Een Amerikaanse man reageerde hier boos op, omdat hij kortingen kreeg voor babyspullen, terwijl zijn dochter nog maar een tiener was (Duhigg, 2012). Wat bleek, zijn dochter was dus inderdaad zwanger (Duhigg, 2012).

De blik vanuit de buitenwereld die de privésfeer aantast is niet alleen van bedrijven en overheden, maar ook van sinistere partijen, zoals hackers en cybercriminelen (Martijn & Tokmetzis, 2016a). Volgens data van het CBS (2017) zijn in 2016 17.9 op de 100 personen slachtoffer geweest van een vorm van cybercrime, waarvan 7.4 op de 100 personen slachtoffer waren van hackers. Doordat steeds meer dataverkeer via het internet verloopt en steeds meer apparaten aan het internet zijn verbonden, zoals de al eerdergenoemde slimme thermostaten en interactieve televisies, maar ook printers, webcams, beveiligingscamera's, externe harde schijven, routers en geluidsinstallaties, wordt het voor hackers steeds interessanter om digitaal in te breken (Martijn & Tokmetzis, 2016a).

Een populaire vorm van hacken is onbevoegd inbreken, waarbij de hacker controle krijgt over de toegang tot iemand anders zijn apparaat en deze vervolgens actief kan laten werken zonder dat de eigenaar hiervan af weet (Siapera, 2012). Hackers kunnen namelijk via een openbare zoekmachine, genaamd Shodan, apparaten opsporen die zijn gekoppeld aan het internet (Martijn & Tokmetzis, 2016a). Veel mensen vergeten hier een wachtwoord aan te koppelen of gebruiken het standaard wachtwoord dat is aangeleverd door de fabrikant, zoals 'admin/admin' (Martijn & Tokmetzis, 2016a). Deze standaard wachtwoorden zijn vaak bekend, waardoor de hacker kan inloggen op het apparaat en hierdoor achter bijvoorbeeld privéfoto's, paspoort kopieën, jaarrekeningen of contracten kan komen die zijn opgeslagen op de externe harde schijf (Martijn & Tokmetzis, 2016a). Een hacker kan hiermee ook meekijken met beveiligingscamera's of babycams, de printgeschiedenis bekijken of zelfs een printopdracht geven, of het internetverkeer omleiden en opvangen via de router waardoor de hacker toegang krijgt tot inloggegevens van bijvoorbeeld de bank (Martijn & Tokmetzis, 2016a).

Ook openbare wifinetwerken zijn een makkelijke prooi voor een hacker. Via een speciaal apparaatje, de WiFi Pineapple, dat zich voor kan doen als een vertrouwd wifinetwerk, kan de hacker smartphones en laptops, die automatisch op zoek zijn naar een netwerk waarop deze al eerder ingelogd zijn geweest, op het netwerk in laten loggen dat hoort bij de Pineapple (Martijn & Tokmetzis, 2016a). Daarnaast kan de hacker met datzelfde apparaat een openbaar wifinetwerk nabootsen van een bepaalde locatie, zoals een café (Martijn & Tokmetzis, 2016a). Er zijn namelijk openbare wifinetwerken die een naam hebben bestaande uit willekeurige letters en cijfers, waarbij de hacker vervolgens alleen maar zijn eigen netwerk de naam van de desbetreffende locatie hoeft te geven waarop men logischerwijs sneller op zal inloggen (Martijn & Tokmetzis, 2016a). Ook via deze methode kunnen hackers het internetverkeer omleiden en daarmee aan inlogcodes komen (Martijn & Tokmetzis, 2016a).

Criminelen proberen ook vaak aan inloggegevens van bijvoorbeeld bankrekeningen te komen via *phishing* e-mails, waarin de crimineel zich voor doet als de bank en vraagt om de inloggegevens te bevestigen of te updaten via een link die doorverwijst naar een neppe website die lijkt op de originele website (Siapera, 2012).

Daarnaast koppelen mensen de binnenwereld ook steeds meer aan de buitenwereld; via de smartphone neemt men een groot deel van het privéleven mee naar buiten, want in smartphones staan vaak fotoalbums, adressen van vrienden, familie en collega's en persoonlijke correspondentie (Martijn & Tokmetzis, 2016a). Mensen leven steeds meer in een gepersonaliseerde wereld, ook buiten de privésfeer. De publieke sfeer is een ruimte die draait om het collectieve belang en het bieden van bestendigheid, omdat iedereen voor de wet gelijk is en zich daar ook naar moet gedragen (Schnitzler, 2014a). De publieke sfeer begint echter zijn tegenwicht tegen de privésfeer, die gekenmerkt wordt door veranderlijkheid, te verliezen en transformeert steeds meer in een ruimte die draait om persoonlijke belangen (Schnitzler, 2014a). Schnitzler (2014a) gaat zelfs zo ver door te stellen dat hierdoor de maatschappij uiteen kan vallen, doordat iedereen niet meer betrokken is met elkaar.

2.6. Privacy paradox

Ondanks dat mensen veel informatie op het internet en sociale media delen, betekent dit niet dat zij online privacy niet meer belangrijk zijn gaan vinden. Privacy op het internet wordt nog wel degelijk belangrijk gevonden, maar er wordt in de praktijk niet of nauwelijks naar gehandeld. Gebruikers construeren namelijk hun identiteit online via de openbaarmaking van persoonlijke gegevens (Young & Quan-Haase, 2013). De contradictie tussen bezorgdheden over online privacy en de bereidheid om persoonlijke gegevens te onthullen heet ook wel de privacy paradox (TNO, 2015; Young & Quan-Haase, 2013). Een recent onderzoek dat in Nederland de privacy-beleving onder de Nederlandse bevolking heeft onderzocht in opdracht van de Tweede Kamer is dat van TNO (2015). Ook daarin kwam de privacy paradox naar voren. Zo gaf 82.5 procent van de 1.066 respondenten aan het belangrijk te vinden dat hun persoonsgegevens worden beschermd en gaf 71.2 procent van de respondenten aan dat het online delen van persoonlijke informatie een onderwerp van aandacht moet zijn in de maatschappij (TNO, 2015). Desondanks kwam uit het onderzoek naar voren dat meer dan de helft van de respondenten de privacyvoorwaarden van een online dienst niet leest, omdat deze te lang of te moeilijk zijn en bleek dat 74 procent van de respondenten het minste vertrouwen heeft in de manier waarop sociale media omgaan met hun gebruikersgegevens, terwijl het overgrote deel van de respondenten desondanks heeft aangegeven sociale media dagelijks te gebruiken (TNO, 2015).

2.6.1. Oorzaken van de privacy paradox

Privacy verliest het vaak van andere waarden (Martijn & Tokmetzis, 2016a). Redenen waarom er in de praktijk niet naar online privacy wordt gehandeld is ten eerste vanwege het al eerdergenoemde

gebrek aan keuzevrijheid. Zo is het internet steeds meer nodig om gebruik te kunnen maken van bepaalde diensten die er offline niet of in mindere mate zijn, zoals het boeken van een hotel in het buitenland. Hiermee worden mensen als het ware verplicht gebruik te maken van het internet. En wanneer men het internet gebruikt wordt men verplicht om de cookies op websites te accepteren, omdat de website anders niet goed werkt en is men verplicht de gebruikersvoorwaarden van online diensten te accepteren om daar gebruik van te kunnen maken (Martijn & Tokmetzis, 2016a; TNO, 2015). Daarnaast zijn lage of vrijwel geen kosten ook een reden waarom er niet wordt gehandeld naar privacy; er zal sneller voor een gratis dienst in ruil voor persoonlijke gegevens worden gekozen dan een privacy-vriendelijker alternatief waarvoor moet worden betaald (Schermer, 2007; TNO, 2015). Een andere reden is gebruikersgemak, wat meerdere dingen inhoudt, zoals dat er via het internet en vooral via sociale media makkelijker contact met anderen kan worden gehouden (Baelden, 2013; Batist, 2015). Ook het uitdrukken van de eigen identiteit is mogelijk via sociale media en het internet en wordt dan ook belangrijker gevonden dan de bijkomende privacyrisico's (Baelden, 2013; Batist, 2015). Ook de mogelijkheid om achter persoonlijke informatie van anderen te komen, zoals een mogelijke romantische partner, is een reden (Trotter, 2012). Nog een andere reden is *peer pressure* of ook wel sociale druk. Dit houdt in dat gebruikers zich gedwongen voelen door hun omgeving om bepaalde internetdiensten te gebruiken, omdat velen in hun omgeving dat ook doen (Batist, 2015; TNO, 2015; Trotter, 2012). Ook veiligheid is een reden om privacy op te geven (Martijn & Tokmetzis, 2016a; Van Dijck, 2014). Zo gaf 70 procent van de 24.143 ondervraagde internetgebruikers uit 24 verschillende landen aan dat de rechtshandhaving het recht zou moeten hebben om toegang te krijgen tot de inhoud van online communicatie van burgers voor nationale veiligheidsredenen (Centre for International Governance Innovation & IPSOS, 2016).

Nog een reden is het gebrek aan kennis, ook wel onwetendheid, wat in meerdere vormen naar voren komt. Veel gebruikers beseffen niet dat de informatie die op hun sociale mediaprofiel als privé staat alsnog tot de beschikking staat van het sociale medium zelf en de bedrijven en organisaties waarmee het desbetreffende sociale medium mee samenwerkt (Batist, 2015). Ook beseffen veel gebruikers niet dat zij de controle over hun persoonlijke informatie kunnen verliezen aan derde partijen door hun eigen connecties, wanneer deze gebruikmaken van applicaties en daarbij toegang tot gegevens van hun connecties hebben gegeven aan de ontwikkelaar van de desbetreffende applicatie (Baelden, 2013). Ook zijn veel mensen laks of lui in het beschermen van hun persoonlijke gegevens; de meesten gebruiken de simpelste wachtwoorden, zoals postcodes of geboortedata, omdat deze gemakkelijk te onthouden zijn, of installeren hun beveiligingsupdates niet of te laat, omdat dit vaak tijd in beslag neemt (Martijn & Tokmetzis, 2016a). Daarnaast denken sommige internetgebruikers dat er tegenwoordig geen online privacy meer is, dat alles dankzij de informatie- en communicatietechnologieën al bekend is en dat daar ook niks meer aan te doen valt (Batist, 2015; Martijn & Tokmetzis, 2016a; Schermer, 2007). Dit kwam tevens naar voren in een onderzoek onder 1.500 Amerikanen, waarin 60 procent van hen verlies van online privacy als onvermijdelijk

beschouwen en dit dus maar accepteren (Turow, Hennesy, & Draper, 2015). Anderen vinden dat zij niks te verbergen hebben, omdat zij naar eigen zeggen geen terrorist of crimineel zijn en zien dus ook geen probleem dat moet worden opgelost (Batist, 2015; Martijn & Tokmetzis, 2016a; Schermer, 2007). De meeste mensen vinden het niet erg dat er gegevens worden verzameld, zoals de locaties die zij bezoeken of wat voor soort mineraalwater zij kopen (Schermer, 2007). Het gevaar schuilt echter niet in de overlevering van individuele stukjes gegevens, maar juist in de koppeling van deze verschillende stukjes (Schermer, 2007). Hiermee stellen bedrijven en andere organisaties digitale profielen op met alle gevolgen van dien en daar zijn veel mensen zich niet van bewust. Ook berichten de media nog te weinig over slachtoffers, van bijvoorbeeld identiteitsdiefstal, wat een misplaatst gevoel van veiligheid en privacy kan geven ((NTR, 2016).

Dan is er ook nog onwetendheid door het gebrek aan informatie en transparantie (Martijn & Tokmetzis, 2016a). Het is namelijk onmogelijk om exact op de hoogte te zijn over waar persoonlijke informatie is opgeslagen, waar het naartoe wordt verzonden en hoe het wordt gebruikt, want lang niet alles staat in de privacyvoorwaarden van websites en online diensten (Nissenbaum, 2011). Wat wel in de privacyvoorwaarden staat is meestal op zo'n ingewikkelde en uitgebreide manier beschreven dat bijna niemand in de praktijk nog de moeite neemt om het te lezen (Nissenbaum, 2011). Daarnaast kunnen en worden privacyvoorwaarden in de loop van de tijd aangepast (Nissenbaum, 2011). Bedrijven zelf hebben ook vaak niet het volledige inzicht in wat derde partijen, op bijvoorbeeld hun eigen website of dienst, met verzamelde gegevens doen en verwijzen dan ook weer door naar de privacyvoorwaarden van die partijen (Martijn & Tokmetzis, 2016a). Daar komt nog bovenop dat de meeste mensen de bedrijven, die data over hen verzamelen, verkopen of opkopen, niet kennen (Martijn & Tokmetzis, 2016a).

Men ziet niet wat er met persoonlijke gegevens gebeurt, wat er mee wordt gedaan, wie er allemaal toegang tot heeft, wie er toegang tot probeert te krijgen en wat de consequenties daarvan zijn (Martijn & Tokmetzis, 2016a; Schermer, 2007). Men moet op de hoogte zijn van deze datastromen om te kunnen bepalen of een datastroom naar bepaalde ontvangers gepast of ongepast is (Martijn & Tokmetzis, 2016a). Volgens Martijn en Tokmetzis (2016a) komt het door deze onzichtbaarheid dat de urgentie van het beschermen van persoonlijke gegevens en daarmee de privacy niet wordt ingezien. De menselijke beoordeling van apparaten zoals smartphones en computers gaat niet verder dan de vraag of deze werken of niet en het vertrouwen in het gebruik ervan, aangezien alleen de interface zichtbaar is (Martijn & Tokmetzis, 2016a). Gebruikers zien niet hoe de technologie echt werkt, dat er anderen mee (kunnen) kijken en hen in bepaalde richtingen proberen op te sturen of gegevens (kunnen) gebruiken voor ongewenste doeleinden (Martijn & Tokmetzis, 2016a). Daardoor "is het lastig om te beoordelen of het vertrouwen wel terecht is" (Martijn & Tokmetzis, 2016a, p. 66). Volgens Martijn en Tokmetzis (2016a) is dit een belangrijke reden voor de privacy paradox; men vindt privacy belangrijk, vertrouwt de technologie niet helemaal, maar doet er niks aan, omdat het wantrouwen naar de achtergrond verdwijnt bij het gebruik van deze technologie omdat de risico's niet

zichtbaar zijn (Martijn & Tokmetzis, 2016a). Pas als er echt iets zichtbaars zou gebeuren, zoals een computerhack, dan zal het belang van privacy wellicht doordringen (Martijn & Tokmetzis, 2016a). Voor al deze gevallen geldt dat de gepercipieerde privacy afwijkt van de daadwerkelijke privacy. Dit betekent dat er een gebrek aan kennis is over de daadwerkelijke privacy die de gebruiker wel of niet heeft. Dit zorgt voor een illusie van online privacy (Batist, 2015).

2.6.2. Privacy paradox onder jongeren

Volgens eerder onderzoek is de privacy paradox vooral onder jongeren aanwezig die sociale media gebruiken (Batist, 2015; Van der Velden & El Emam, 2013). Jongeren die sociale media gebruiken vinden hun privacy belangrijk, maar ondernemen nauwelijks actie (Van der Velden & El Emam, 2013). Een belangrijke reden hiervoor is het al eerdergenoemde gebrek aan kennis. Zo vinden jongeren het beheren van privacy via de privacy-instellingen op sociale media soms te ingewikkeld waardoor zij deze links laten liggen (Baelden, 2013; Livingstone, 2008; Van der Velden & El Emam, 2013). Het gebrek aan kennis is ook te zien aan het feit dat veel jongeren zich niet realiseren dat sociale media publieke ruimtes zijn; zij denken alleen te communiceren en hun content te delen met vrienden, familie en andere leeftijdsgenoten, terwijl deze communicatie en content op een publiekelijk platform komt te staan, wat betekent dat hun publiek ook uit andere partijen bestaat (Barnes, 2006; Batist, 2015). Daarnaast maken veel jongeren zich nauwelijks zorgen over gepersonaliseerde reclame op sociale media en vinden zij dit zelfs wenselijk, omdat zij daarmee reclames krijgen aangeboden die bij hun interesses passen (Baelden, 2013). Uit het onderzoek van Baelden (2013) kwam ook naar voren dat jongeren zich niet of nauwelijks bewust zijn hoe gepersonaliseerde advertenties werken en dat jongeren vaak het privacybeleid van sociale media niet lezen. Daarnaast komt het ook voor dat jongeren de bescherming van hun persoonlijke gegevens gewoonweg minder belangrijk vinden, omdat het delen van informatie zo vanzelfsprekend lijkt (Baelden, 2013; TNO, 2015; Van der Velden & El Emam, 2013).

Daarnaast is de controle paradox ook een reden voor de privacy paradox onder jongeren. De controle paradox houdt in dat hoe meer controle er wordt gedacht te hebben over persoonlijke informatie, hoe meer persoonlijke informatie wordt onthuld, ondanks dat de risico's die hieraan verbonden zijn niet zijn veranderd (Van der Velden & El Emam, 2013). Veel jongeren trachten hun sociale mediaprofiel te beheren via de privacy-instellingen en aan de hand van de personen die zij bevrienden op hun sociale media (Van der Velden & El Emam, 2013; Young & Quan-Haase, 2013). De controle paradox heeft daarmee betrekking op de sociale privacy; het hebben van controle over wie van de andere gebruikers toegang heeft tot diens persoonlijke informatie (Raynes-Goldie, 2010; Siapera, 2012; Van der Velden & El Emam, 2013; Young & Quan-Haase, 2013). De institutionele privacy, die betrekking heeft op hoe sociale media zelf, andere bedrijven en derde partijen persoonlijke gegevens gebruiken of misbruiken, wordt door jongeren vaak links gelaten (Raynes-Goldie, 2010; Siapera, 2012; Young & Quan-Haase, 2013). Volgens Young en Quan-Haase (2013)

zijn een gebrek aan directe communicatie met instellingen en bedrijven, die persoonlijke informatie beheren, evenals een gebrek aan transparantie, van wat voor soort persoonlijke gegevens er worden verzameld en gebruikt, oorzaken waardoor er geen inzicht is in de gevolgen voor de institutionele privacy bij het delen van persoonlijke informatie.

2.7. Privacybewustzijn

Gebruikers hoeven niet altijd naïef te zijn als het gaat om het onthullen van persoonlijke gegevens (Tufekci, 2008; Young & Quan-Haase, 2013). Uit het onderzoek van TNO (2015) is gebleken dat het merendeel van de Nederlandse respondenten wel degelijk met enige regelmaat bewust nadenkt over wat er met hun persoonlijke gegevens kan gebeuren tijdens het internetgebruik. Het privacybewustzijn betreft de perceptie, aandacht en kennis over online privacy-kwesties (Van der Velden & El Emam, 2013). Met perceptie wordt bedoeld hoe er op subjectieve wijze wordt gedacht over online privacy. Met kennis wordt bedoeld de mate van onjuiste en juiste kennis. Met aandacht wordt bedoeld de aandacht die wordt gegeven aan online privacy, door er bijvoorbeeld over te praten met anderen of bepaalde maatregelen te nemen. Uit het onderzoek van TNO (2015) kwam naar voren dat het merendeel van de respondenten, namelijk 77.2 procent, weleens praat met anderen over de bescherming van persoonlijke gegevens (TNO, 2015). Een andere conclusie uit het onderzoek van TNO (2015) was dat respondenten verschillende maatregelen nemen om hun institutionele privacy te beschermen; zo maakt 88.5 procent gebruik van een *firewall* of virusscanner en heeft 63.8 procent cookiefilters geïnstalleerd. Dit onderzoek focust, wat betreft de aandacht die wordt gegeven aan online privacy, alleen op het aantal maatregelen die zijn toegepast om de online privacy te beschermen.

Er zijn onderzoeken gedaan naar wat voor maatregelen en strategieën jongeren op bewuste wijze toepassen om hun privacy te beschermen op sociale media. Van der Velden en El Emam (2013) hebben onderzoek hiernaar gedaan aan de hand van semigestructureerde interviews onder Canadese tienerpatiënten tussen de 12 en 18 jaar oud, Young en Quan-Haase (2013) via een enquête onder Canadese universiteitsstudenten, Raynes-Goldie (2010) via een etnografische studie onder Canadese Facebookgebruikers van onder de 30 jaar en Tufekci (2008) via een enquête onder Amerikaanse studenten. Uit deze onderzoeken kwam naar voren dat jongeren onder andere hun privacy-instellingen beperken door deze in te stellen op ‘alleen vrienden’, geen openbare statusupdates plaatsen, selectief zijn in het ‘bevrienden’ van mensen online, verschillende media gebruiken voor verschillende groepen, verschillende publieken gescheiden houden, fototags verwijderen zodat (onflatteuze) foto’s niet op hun tijdlijn te zien zijn, gebruikmaken van privéberichten om toegang tot de inhoud te beperken en bepaalde persoonlijke informatie niet op hun profiel zetten zodat vreemden deze niet kunnen gebruiken (Raynes-Goldie, 2010; Tufekci, 2008; Van der Velden & El Emam, 2013; Young & Quan-Haase, 2013).

Voor de genoemde strategieën geldt dat deze voornamelijk worden gebruikt om privacyschendingen door onbekenden tegen te gaan, waarmee de al eerdergenoemde sociale privacy in acht wordt genomen maar niet de institutionele privacy (Raynes-Goldie, 2010; Van der Velden & El Emam, 2013; Young & Quan-Haase, 2013). Uit het onderzoek van Young en Quan-Haase (2013) kwam namelijk naar voren dat er weinig bezorgdheid wordt geuit over hoe Facebook zelf, andere bedrijven en derde partijen persoonlijke gegevens gebruiken of misbruiken. Maar één respondent in het onderzoek van Young en Quan-Haase (2013) uitte haar zorgen over haar institutionele privacy, met name hoe haar persoonlijke informatie kan worden gebruikt zonder haar toestemming. Deze respondent meldde dat zij haar institutionele privacy beschermt door bepaalde informatie voor Facebook uit te sluiten (Young & Quan-Haase, 2013). In het onderzoek van Tufekci (2008) kwam naar voren dat een klein percentage respondenten bepaalde informatie, zoals hun telefoonnummer, niet op hun Facebookprofiel zetten, omdat zij geloven dat hun profiel door de overheid kan worden bekeken.

De bevindingen afkomstig uit de onderzoeken van Raynes-Goldie (2010), Young en Quan-Haase (2013) en Van der Velden en El Emam (2013) suggereren dat jongeren beter inzicht hebben in hoe vrienden, familie en andere personen die deel uitmaken van hun Facebook netwerk hun privacy mogelijk kunnen bedreigen dan in mogelijke risico's die afkomstig zijn van instellingen en andere partijen. Wat aan deze onderzoeken opvalt, is dat er onderzocht is hoe jongeren, die gebruikmaken van sociale media, zelf denken hun online privacy te kunnen beschermen. Echter, omdat er vaak een gebrek is aan kennis (over bijvoorbeeld wat voor maatregelen en hoe deze genomen kunnen worden), wijkt de gepercipieerde privacy vaak af van de daadwerkelijke privacy, wat voor een illusie van online privacy kan zorgen (Batist, 2015). In dit onderzoek staat het privacybewustzijn centraal, bestaande uit de perceptie, aandacht (in de vorm van maatregelen om de online privacy te beschermen) en kennis over online privacy-kwesties, waarmee wordt onderzocht in hoeverre de gepercipieerde privacy afwijkt van de daadwerkelijke privacy.

2.8. Nieuwe digitale kloof

In de hedendaagse informatie- en communicatiemaatschappij lijkt het logisch om te stellen dat de zogezegde digitale kloof, ook wel *digital devide*, kleiner wordt. De notie van *digital devide* wordt vaak gebruikt om de kloof aan te geven tussen de mensen die toegang tot het internet hebben tegenover de mensen die hier geen toegang tot hebben (Siapera, 2012). Vooral de jongere generaties, ook wel de *technoholics* en *digital natives* genoemd, maken het meest gebruik van het internet in vergelijking met oudere generaties (Siapera, 2012; Sitompoel, 2015). De digitale kloof schijnt echter kleiner te worden nu steeds meer mensen toegang hebben tot het internet, zoals ouderen, etnische minderheden en mensen met lagere inkomens (Siapera, 2012). Toegang tot het internet betekent echter niet dat de ongelijkheid daarmee verdwenen is. Integendeel, ondanks het hebben van toegang kan het gebruik

ervan gelimiteerd zijn (Hargittai & Walejko, 2008; Siapera, 2012). Hargittai en Walejko (2008) stellen dat het concept van de digitale kloof moet worden verfijnd, omdat de digitale geletterdheid en de mogelijkheid te kunnen participeren op het internet ongelijk verdeeld is onder individuen, ongeacht het hebben van toegang tot nieuwe media. Hierbij behandelen Hargittai en Walejko (2008) digitale geletterdheid als vaardigheden om op participatieve wijze content te kunnen creëren en te kunnen delen. Het hebben van digitale vaardigheden om op participatieve wijze van het internet gebruik te maken betekent echter niet dat het internet daarmee volledig kan worden begrepen. Zoals Martijn en Tokmetzis (2016a) beargumenteren, zien gebruikers alleen de interface van hun apparaten, niet hoe de technologie daarachter echt werkt en dat anderen mee (kunnen) kijken met als doel om gebruikers bepaalde richtingen op te sturen of hun gegevens (kunnen) gebruiken voor ongewenste doeleinden. Daarom wordt in dit onderzoek digitale geletterdheid geïnterpreteerd als het kritisch kunnen evalueren en begrijpen van nieuwe media, omdat de gebruiker hierdoor bevooroordeelde of uitbuitende (online) mediabronnen beter kan onderscheiden en beter kan beoordelen of de privacy in het geding is bij het gebruikmaken van bepaalde internetdiensten (Livingstone, 2004).

Ondanks het hebben van de status van *technoholics* en *digital natives* lijken ook jongeren dus digitale geletterdheid te missen, vooral wanneer het gaat over het kritisch evalueren van sociale media wat betreft hun online privacy (Baelden, 2013; Livingstone, 2004). Zoals het er nu naar lijkt kan de digitale kloof worden toegepast op de mensen die op een hoog niveau digitaal geletterd zijn en via geavanceerde dataveillance-technologieën toegang hebben tot andermans data aan de ene kant en de mensen wiens data worden verzameld en gebruikt aan de andere kant (Schermer, 2007). De digitale geletterdheid wat betreft informatie- en communicatietechnologie (ICT) onder de gewone bevolking is nog niet voldoende (Livingstone, 2004). Volgens Schnitzler (2015b) is het eigenlijk noodzakelijk dat de maatschappij de technologie eigen maakt door, vooral jongeren, te leren programmeren, zodat de digitale kloof tussen de gewone burgers tegenover de programmeurs en experts van onder andere Facebook wordt verkleind (Michiels, 2015).

Door meer mediawijsheid te creëren over online privacy leren mensen op kritische en bewustere wijze om te gaan met de voordelen en nadelen van het internet en sociale media. Een betere kennis en een groter bewustzijn wat betreft nieuwe mediavormen en online privacy geeft gewone mensen, naast de grote (commerciële) internetbedrijven die data over hen verzamelen en gebruiken, de mogelijkheid (beter) te profiteren van informatie en communicatie in een technologisch-gemedieerde maatschappij (Livingstone, 2004). Kennis is namelijk macht en sinds digitale kopieën steeds accurater worden betekent dit dat de effectiviteit van controle daarover ook groter wordt (Schermer, 2007). Door zelf meer digitale kennis te vergaren en te leren de hoeveelheid beschikbare data op bewuste wijze te beperken, wordt het vermogen van derde partijen om individueel gedrag te voorspellen, te reguleren en te controleren verminderd (Schermer, 2007). Volgens Schermer (2007) betekent dit dat online mediagebruikers zichzelf en hun persoonlijke gegevens moeten beschermen voor de blik van anderen.

2.9. Hypotheses

Het doel van dit onderzoek is het privacybewustzijn, bestaande uit de perceptie, aandacht (in de vorm van maatregelen om de eigen online privacy te beschermen) en kennis wat betreft online privacy-kwesties, onder Nederlandse jongeren vanaf 16 tot en met 29 jaar te onderzoeken, sinds het vooral jongeren zijn die van sociale media gebruikmaken. In dit onderzoek wordt tevens onderzocht wat voor onafhankelijke variabelen van invloed kunnen zijn op het privacybewustzijn. Er wordt verwacht dat leeftijd, opleidingsniveau en actief sociale mediagebruik invloed kunnen hebben op de perceptie, aandacht en kennis over online privacy. Daarnaast wordt ook verwacht dat de onderzochte jongeren van plan zullen zijn bewuste actie te ondernemen om de online privacy beter te beschermen wanneer hun initiële kennis over online privacy, als onafhankelijke variabele, is vergroot.

2.9.1. Leeftijd

Een van de factoren die van invloed kan zijn op het privacybewustzijn is leeftijd. Uit de resultaten van TNO (2015) kwam naar voren dat de jongste leeftijdscategorie (tussen de 18 tot 34 jaar) privacy minder belangrijk vindt dan de oudere leeftijdscategorieën. De reden die hiervoor werd gegeven is dat jongeren het meer vanzelfsprekend vinden om gegevens te delen in de huidige informatiemaatschappij dan ouderen (TNO, 2015). Van jongeren in de ondergrens van de leeftijdsspanne vanaf 16 tot en met 29 jaar kan dan worden verwacht dat zij wellicht ook minder bezorgd zijn over hun online privacy, wat betekent dat zij een positievere perceptie hebben over online privacy, vergeleken met jongeren in de bovengrens van de leeftijdsspanne vanaf 16 tot en met 29 jaar. Daarnaast kwam ook uit het onderzoek van TNO (2015) naar voren dat de jongste leeftijdscategorie minder beschermend optreedt. Van jongeren in de ondergrens van de leeftijdsspanne vanaf 16 tot en met 29 jaar kan dan worden verwacht dat zij minder aandacht geven aan het toepassen van maatregelen om hun online privacy te beschermen dan jongeren in de bovengrens van de leeftijdsspanne vanaf 16 tot en met 29 jaar. Omdat jongeren tevens zo gemakkelijk omgaan met het delen van hun gegevens, kan van jongeren in de ondergrens van de leeftijdsspanne vanaf 16 tot en met 29 jaar worden verwacht dat hun daadwerkelijke kennis over online privacy lager is en zij hier minder bij stilstaan (Batist, 2015). Naarmate jongeren ouder worden kan het besef van online privacy groeien en kan daarmee worden verwacht dat jongeren in de bovengrens vanaf 16 tot en met 29 jaar een hogere kennis hebben over online privacy (TNO, 2015). Omdat de populatie voor dit onderzoek bestaat uit jongeren vanaf 16 tot en met 29 jaar en daarmee een beperkte leeftijdsspanne in beslag neemt, kan het zijn dat er geen grote verschillen naar voren komen in de resultaten wat betreft de perceptie, aandacht en kennis als onderdelen van het privacybewustzijn. Desondanks is de volgende hypothese opgesteld:

H_1: Hoe hoger de leeftijd is, hoe hoger het privacybewustzijn.

De deelhypotheses luiden als volgt:

- $H_{1.1}$: Hoe hoger de leeftijd is, hoe negatiever de perceptie over online privacy.
- $H_{1.2}$: Hoe hoger de leeftijd is, hoe meer maatregelen zijn toegepast om de online privacy te beschermen.
- $H_{1.3}$: Hoe hoger de leeftijd is, hoe hoger de kennis over online privacy.

2.9.2. Opleidingsniveau

Een tweede factor die van invloed kan zijn op het privacybewustzijn is opleidingsniveau. TNO (2015) heeft onderzocht of er een relatie is tussen opleidingsniveau en privacy. Uit de resultaten kwam naar voren dat er geen significant verschil bestaat tussen hoger en lager opgeleiden in hoe er wordt gedacht over privacy (TNO, 2015). TNO (2015) heeft hierbij echter alleen gekeken naar de gepercipieerde privacy; wat mensen zelf denken te weten over hun online privacy, zoals of zij wel of niet denken te weten wie er toegang heeft tot hun gegevens en niet of dit ook strookt met de werkelijke privacy die zij hebben. Daarom kan er alsnog een verschil worden verondersteld in het privacybewustzijn tussen hoger en lager opgeleiden, wanneer (het gebrek aan) kennis over online privacy van de respondent wordt getest. Er kan alsnog worden verwacht dat lager opgeleiden een positievere perceptie hebben over online privacy, minder aandacht geven aan het toepassen van maatregelen om hun online privacy te beschermen en een lagere kennis hebben over online privacy in vergelijking met hoger opgeleiden. Hieruit volgt de volgende hypothese:

H_2: Hoe hoger het opleidingsniveau is, hoe hoger het privacybewustzijn.

De deelhypotheses luiden als volgt:

- $H_{2.1}$: Hoe hoger het opleidingsniveau is, hoe negatiever de perceptie over online privacy.
- $H_{2.2}$: Hoe hoger het opleidingsniveau is, hoe meer maatregelen zijn toegepast om de online privacy te beschermen.
- $H_{2.3}$: Hoe hoger het opleidingsniveau is, hoe hoger de kennis over online privacy.

2.9.3. Actief sociale mediagebruik

Een derde factor die van invloed kan zijn op het privacybewustzijn is de mate waarin er actief gebruik wordt gemaakt van sociale media. Uit de resultaten van TNO (2015) kwam naar voren dat er geen significant verband is met het aantal uur dat iemand per dag online is. Hierbij is echter niet de manier onderzocht waarop iemand online is; passief of actief. Hoe meer er namelijk op actieve wijze gebruik wordt gemaakt van sociale media, zoals het zelf delen of posten van foto's, video's, statusupdates, comments, gevoel of locaties, in plaats van het alleen passief bekijken van content van anderen, hoe meer data het sociale medium kan gebruiken over de desbetreffende gebruiker. Er kan dan worden verwacht dat de mensen die minder op actieve wijze gebruikmaken van sociale media hier bewust voor hebben gekozen. Uit de resultaten van het onderzoek van Tufekci (2008), die onder

andere algemene privacyzorgen en het wel en niet onthullen van bepaalde informatie op sociale media onder studenten heeft onderzocht, kwam naar voren dat de respondenten die geen gebruik maken van sociale media een hogere mate aan zorgen over privacy uitdrukken dan de respondenten die wel gebruikmaken van sociale media. Er kan dan worden verwacht dat de mensen die op actieve wijze gebruikmaken van sociale media minder bezorgd zijn over hun online privacy wat een positievere perceptie inhoudt, minder aandacht geven aan het toepassen van maatregelen om hun online privacy te beschermen en een lagere kennis hebben over online privacy in vergelijking met mensen die op minder actieve wijze gebruikmaken van sociale media. Omdat het vooral jongeren zijn die veel op actieve wijze sociale media gebruiken en de populatie voor dit onderzoek ook uit jongeren bestaat, kan het zijn dat er geen grote verschillen naar voren komen in de mate van actief en minder actief sociale mediagebruik. Desondanks is de volgende hypothese als volgt opgesteld:

H_3: Hoe actiever het sociale mediagebruik is, hoe lager het privacybewustzijn.
De deelhypotheses luiden als volgt:

- $H_{3.1}$: Hoe actiever het sociale mediagebruik is, hoe positiever de perceptie over online privacy.
- $H_{3.2}$: Hoe actiever het sociale mediagebruik is, hoe minder maatregelen zijn toegepast om de online privacy te beschermen.
- $H_{3.3}$: Hoe actiever het sociale mediagebruik is, hoe lager de kennis over online privacy.

Om de hoeveelheid van verschillende sociale media te beperken is er gekozen om alleen het (actieve) sociale mediagebruik op drie verschillende sociale netwerksites, waarop content ook openbaar kan worden gedeeld, te includeren in dit onderzoek, namelijk; Facebook, Snapchat en Instagram. Er is voor Facebook gekozen, omdat Facebook met zijn 9.6 miljoen Nederlandse gebruikers het op een na grootste sociale mediaplatform is en circa 42 procent van die gebruikers uit de leeftijdscategorie tussen de 18 en 34 jaar bestaat (Facebook, n.d.; Van der Veer, 2016). Ondanks dat WhatsApp het grootste sociale mediaplatform is met 9.8 miljoen Nederlandse gebruikers is er voor gekozen om WhatsApp niet in dit onderzoek op te nemen (Van der Veer, 2016), omdat dit geen sociale netwerksite is, maar enkel een berichtservice waarop geen content kan worden gedeeld met een openbaar publiek. Er is voor Instagram en Snapchat gekozen, omdat deze twee sociale media vooral populair zijn onder Nederlandse jongeren (Oosterveer, 2016; Van der Veer, 2016).

2.9.4. Bewuste actie

Ondanks dat het verzamelen, gebruiken, opkopen en verkopen van persoonlijke data op steeds grotere schaal gebeurt en individuen daar weinig aan kunnen doen, is het van belang dat men anders over data en online privacy gaat denken. Er moet meer besef komen over de keerzijde van het internet

en sociale media en de dataverzamelzucht van bedrijven die hierin werkzaam zijn (Martijn en Tokmetzis, 2016a). Volgens Martijn en Tokmetzis (2016a) moeten mensen bewuster omgaan met de eigen persoonlijke gegevens. Martijn en Tokmetzis (2016b) hebben daarvoor een zelfverdedigingsgids opgezet om als individu zelf maatregelen te nemen om de eigen privacy meer te waarborgen. Zo kan het gebruik van *ad blockers* adverteerders weren en cookies blokkeren, zijn wachtwoorden sterker wanneer deze meerdere tekens en cijfers bevatten en kan het gebruik van *firewalls* en virusscanners onbevoegden buiten de inhoud van computers en laptops houden (Martijn & Tokmetzis, 2016b). Door meer digitale geletterdheid te creëren kan een gebruiker beter beoordelen of zijn of haar online privacy in het geding is bij het gebruiken van bepaalde internetdiensten (Livingstone, 2004).

Daarom is het doel van dit onderzoek om tevens de initiële kennis over online privacy onder de onderzochte jongeren te bevorderen door informatie te geven over online privacy, waardoor de gepercipieerde privacy meer zal overeenkomen met de daadwerkelijke privacy. Dit is gedaan door respondenten quizvragen te laten beantwoorden waarop, ongeacht of deze juist of onjuist zijn beantwoord, na elke vraag het juiste antwoord met uitleg volgde, zodat respondenten ervan konden leren. Een lage score zou dan betekenen dat de respondent kennis over online privacy miste, maar deze kennis is (hopelijk) gestegen door de bijgevoegde informatie. De (initiële) kennis wat betreft online privacy is in dit geval een onafhankelijke variabele waarvan wordt verwacht dat deze van invloed is op het van plan zijn bewuste actie te ondernemen om de online privacy beter te beschermen. Er kan worden verwacht dat bij een lage quizscore, de kans groter is dat er na de quiz actie wordt gepland om de online privacy beter te beschermen door bewuster om te gaan met het delen van persoonlijke gegevens op het internet en sociale media. De volgende hypothese is dan als volgt opgesteld:

> H_4: Hoe lager de initiële kennis (in de vorm van de quizscore) is, hoe hoger de kans dat er bewuste actie wordt gepland om de online privacy beter te beschermen.

Dit onderzoek heeft hiermee een vorm van actieonderzoek uitgevoerd waarbij is getracht niet alleen de inzichten van de onderzoeker zelf te vergroten, maar ook dat van de onderzoeksobjecten (Reason & Bradbury, 2007). Actieonderzoek focust zicht vooral op het oplossen van problemen om daarmee tot sociale verandering te komen (Reason & Bradbury, 2007). Dit onderzoek heeft ernaar gestreefd om reflectie, kennis en een kritischer bewustzijn over online privacy bij de onderzochte jongeren bij te dragen (Reason & Bradbury, 2007). Dit heeft er hopelijk voor gezorgd dat zij wellicht zelf actie zullen ondernemen om hun online privacy beter te beschermen door bewuster om te gaan met het delen van persoonlijke gegevens op het internet en sociale media.

3. Methodologie

In dit hoofdstuk wordt besproken voor welke onderzoeksmethode en bijbehorende dataverzamelingsmethode is gekozen en de redenen die hieraan ten grondslag liggen. Hierna wordt de populatie gedefinieerd. Vervolgens wordt aan de hand van de steekproefkeuze en de bijbehorende strategie belicht hoe de eenheden zijn verzameld. Daarna wordt er achtergrondinformatie verschaft over de uiteindelijke steekproef. Vervolgens wordt in de operationalisering besproken wat de afhankelijke en onafhankelijke variabelen zijn, hoe deze zijn gemeten en hoe deze zijn gehercodeerd. Als laatste worden de statistische testen besproken, namelijk de meervoudige lineaire regressie en de binaire logistieke regressie, die zijn gebruikt om de data te analyseren.

3.1. Kwantitatieve methode

Voor dit onderzoek is er gekozen voor een kwantitatieve methode. Kwantitatief onderzoek, in tegenstelling tot kwalitatief onderzoek, is een statistische benadering voor het verzamelen van gegevens en draait vooral om numerieke data, metingen en de mogelijkheid om gegevens te generaliseren (Gilbert, 2008; USC Libraries, n.d.). Net als kwalitatief onderzoek kan kwantitatief onderzoek ook de sociale wereld meten maar dan met als doel het creëren van een numerieke beschrijving (Gilbert, 2008). Voordelen van kwantitatief onderzoek zijn de hoge betrouwbaarheid die eraan te pas komt vanwege zijn objectiviteit en de relatieve nauwkeurigheid (Berger, Nici, & Blomdahl, 2016; Gilbert, 2008). Daarnaast kan een kwantitatieve methode een grotere steekproefomvang verkrijgen die representatief is aan de populatie, waarmee conclusies over de gehele populatie kunnen worden gemaakt aangaande de steekproef (Gilbert, 2008; USC Libraries, n.d.). Ook kunnen aan de hand van kwantitatief onderzoek relaties tussen afhankelijke en onafhankelijke variabelen worden vastgesteld, waarmee hypotheses over de variabelen getest en bevestigd kunnen worden (Saunders, Lewis, & Thornhill, 2009; USC Libraries, n.d.). Maar het nadeel van kwantitatief onderzoek in vergelijking met kwalitatief onderzoek is dat het moeilijker is te achterhalen welke variabele de oorzaak is en welke het gevolg (Gilbert, 2008). Omdat in dit onderzoek hypotheses zijn geformuleerd die betrekking hadden op een grote populatie en kwantitatief onderzoek een grote steekproefomvang kan bereiken, was een kwantitatieve benadering voor dit onderzoek het meest geschikt.

3.2. Dataverzamelingsmethode

Om de data te verzamelen is er gebruikgemaakt van een enquête opgesteld in Qualtrics. Hier is voor gekozen omdat met een enquête een groot aantal respondenten kan worden bereikt (Matthews & Ross, 2010). Sociale wetenschappers zien de enquête als een onschatbare bron om data te verkrijgen over opvattingen, waarden, persoonlijke ervaringen en gedragingen van respondenten (Gilbert, 2008). De enquête kan worden uitgevoerd via de telefoon, *face-to-face*, de post en online.

Voor dit onderzoek is gekozen om de enquête online te verspreiden. Voordelen van een online enquête zijn dat er ten eerste makkelijker een groot geografisch gebied en daarmee een grotere steekproefomvang kunnen worden bereikt (Gilbert, 2008; Matthews & Ross, 2010; USC Libraries, n.d.). Ten tweede kunnen gesloten vragen binnen de enquête worden voor-gecodeerd, wat het analyseproces versnelt en wat het maken van vergelijkingen makkelijker maakt (Gilbert, 2008; Saunders et al., 2009). Ten derde kunnen respondenten de enquête beantwoorden in hun eigen tijd, wat het aantrekkelijker voor hen maakt om de enquête in te vullen (Gilbert, 2008). Tot slot is een online enquête goedkoop, doordat er geen bel-, reis- en verzendkosten zijn. Het nadeel van een online enquête is dat er weinig inzicht kan worden verschaft over de (gedeeltelijke) non-responsredenen (Saunders et al., 2009). Omdat de populatie in dit onderzoek actief is op sociale media en daarmee internet tot zijn beschikking heeft, was een online enquête het meest geschikt, omdat er hiermee geen respondenten konden worden uitgesloten.

3.3. Populatie

De populatie zijn Nederlandse jongeren vanaf 16 tot en met 29 jaar die gebruikmaken van sociale media. Er is voor 'jongeren' gekozen, omdat het vooral jongeren zijn die gebruikmaken van sociale media. Zo bestaat circa 42 procent van de 9.6 miljoen Nederlandse Facebookgebruikers uit de leeftijdscategorie tussen de 18 en 34 jaar (Facebook, n.d.). Snapchat en Instagram worden ook voornamelijk door jongeren gebruikt (Van der Veer, 2016). Van de 2.1 miljoen Nederlandse Instagrammers is 58 procent tussen de 15 en 19 jaar en 24 procent tussen de 20 en 39 jaar (Oosterveer, 2016). Snapchat, met 2 miljoen Nederlandse gebruikers, bestaat voor 56 procent uit jongeren tussen de 15 en 19 jaar en voor 11 procent tussen de 20 en 39 jaar (Oosterveer, 2016).

Er is voor de leeftijdsspanne vanaf 16 tot en met 29 jaar gekozen, omdat in de Nederlandse taal 'jongeren' worden gedefinieerd als jonge mensen tussen circa 16 en 30 jaar oud ("Jongere," n.d.). Deze leeftijdsspanne beslaat daarmee het grootste deel van de circa 4 miljoen Facebookgebruikers tussen de 18 en 34 jaar en van de circa 1.7 miljoen Instagrammers en circa 1.3 miljoen Snapchatgebruikers tussen de 15 en 39 jaar (zie ook bovenstaand genoemde percentages). Daarnaast hebben jongeren vanaf 16 jaar geen toestemming meer nodig van hun ouders om te beslissen aan een dergelijk onderzoek mee te doen (Boeije, 2014).

3.4. Steekproef

Er is gebruikgemaakt van een steekproef, omdat de populatie voor dit onderzoek bestaat uit Nederlandse jongeren vanaf 16 tot en met 29 jaar die gebruikmaken van sociale media en daarmee te groot was om in zijn geheel te onderzoeken. Een steekproef kan op willekeurige en niet-willekeurige basis worden gedaan. Bij een willekeurige steekproef wordt er gebruikgemaakt van een steekproefkader, dat een lijst is met alle leden van de populatie waaruit de steekproef op willekeurige

wijze wordt geselecteerd, waardoor elk lid van de populatie evenveel kans heeft om te worden geselecteerd (Gilbert, 2008). Bij een niet-willekeurige steekproef wordt er geen steekproefkader gebruikt en wordt de steekproef geselecteerd op subjectieve basis (Gilbert, 2008).

Er is besloten de steekproef op niet-willekeurige basis te voltrekken, omdat er voor dit onderzoek geen adequate lijst van alle leden van de te onderzoeken populatie beschikbaar was, die kon worden gebruikt om een steekproefkader op te stellen (Gilbert, 2008). Daarnaast zou, wanneer er wel een steekproefkader aanwezig was, het doen van een willekeurige steekproef van een grote en geografisch verspreide populatie te veel tijd kosten (Gilbert, 2008). Het nadeel van een niet-willekeurige steekproef is dat de steekproef niet representatief is voor de populatie en er dan geen generalisaties over de gehele populatie kunnen worden gemaakt (Gilbert, 2008). Dit onderzoek richtte zich echter niet op een representatief beeld van Nederlandse jongeren. De interesse lag in de effecten van leeftijd, opleidingsniveau en actief sociale mediagebruik op het privacybewustzijn en in het effect van kennis over online privacy op het van plan zijn bewuste actie te ondernemen om de online privacy beter te beschermen. Hierdoor waren er geen uitspraken nodig over de gehele populatie.

3.5. Steekproefmethode

Er zijn verschillende manieren om een niet-willekeurige steekproef te trekken. Zo is er de clusteringmethode, waarin de steekproef in stappen wordt uitgevoerd zodat de individuele steekproefeenheden in relatief geografische nabijheid worden gehouden (Gilbert, 2008). Een voorbeeld hiervan is het verspreiden van een enquête op verschillende scholen waar verschillende leerlingen vervolgens willekeurig worden geselecteerd. Een gevolg hiervan is echter dat er te grote gelijkenissen tussen de steekproefeenheden zullen voorkomen, dan wanneer de steekproefeenheden van de gehele populatie op onafhankelijke wijze worden geselecteerd (Gilbert, 2008). Wanneer een clusteringsmethode op diverse scholen zou worden toegepast voor dit onderzoek, zou het kunnen betekenen dat de leeftijd van rond 25 tot en met 29 jaar is ondervertegenwoordigd, omdat deze leeftijdscategorie minder voorkomt op hogescholen en universiteiten.

Daarom is er gekozen voor de sneeuwbalsteekproef, waarbij er gebruik wordt gemaakt van verschillende netwerken (Gilbert, 2008). Het voordeel hiervan is dat er geen steekproefkader nodig is. Een nadeel is dat er homogeniteit kan optreden, omdat de connecties ofwel *entrypoints* bepalend zijn voor het soort respondenten die worden bereikt en zij hoogstwaarschijnlijk alleen andere potentiële respondenten bereiken met dezelfde karakteristieken als zijzelf. Daarom is er geprobeerd om onder verschillende soort connecties de enquête te verspreiden, zodat er verschillende soort respondenten konden worden bereikt. De *entrypoints* zijn gedeeltelijk geselecteerd op basis van de karakteristieken van de populatie, omdat *entrypoints* dus over het algemeen potentiële respondenten bereiken met dezelfde karakteristieken als zijzelf. De *entrypoints* zijn (gedeeltelijk) geselecteerd op basis van verschillende niveaus in onderwijs waarvan werd verwacht dat zij weer respondenten zouden bereiken

binnen hun eigen opleidingsniveau. Verder zijn de *entrypoints* (gedeeltelijk) geselecteerd op basis van de leeftijdsspanne vanaf 16 tot en met 29 jaar. Er werd namelijk verwacht van een *entrypoint* met de leeftijd van 28 jaar dat deze eerder respondenten zou bereiken in de bovengrens van de te onderzoeken leeftijdsspanne en van een *entrypoint* met de leeftijd van 17 jaar dat deze eerder respondenten zou bereiken in de ondergrens van de te onderzoeken leeftijdsspanne. Er zijn echter ook *entrypoints* geselecteerd die potentiële respondenten konden bereiken die niet dezelfde karakteristieken hadden als zijzelf, maar wel binnen de populatie vielen. De enquête is tussen 25 april en 2 mei 2017 door veertien *entrypoints* verspreid door deze te delen op hun Facebook Wall, in WhatsApp-groepen, via e-mail of via hun Twitterpagina (Tabel 1).

Tabel 1. Lijst met *entrypoints*

Geslacht	Leeftijd	Opleiding	Verspreid via	Vriendenaantal	Opmerking
Man	20	Havo	Facebook	439	Bereikte mbo & hbo
Vrouw	28	Wo	Facebook & e-mail	441	Bereikte eind-twintigers
Man	24	Wo	Facebook	1.001	-
Vrouw	23	Wo	Facebook	Niet bekend	Bereikte hbo & wo
Vrouw	23	Hbo	Facebook & WhatsApp-groepen	619	Bereikte hbo & wo
Vrouw	22	Hbo	Facebook & WhatsApp-groepen	319	Bereikte hbo & wo
Vrouw	22	Wo	Facebook	Niet bekend	Bereikte hbo & wo
Vrouw	24	Wo	Facebook	425	-
Vrouw	60	N.v.t.	Facebook	271	Bereikte eind-twintigers
Man	17	Vmbo	Facebook	341	Bereikte vooral tieners
Vrouw	22	Mbo	Facebook	513	-
Vrouw	24	Wo	Facebook	582	Bereikte mbo, hbo & wo
Man	22	Wo	Twitter	5.927	Bereikte vooral tieners
Vrouw	22	Wo	E-mail	Niet bekend	Bereikte eind-twintigers; hbo

3.6. Aantal eenheden

Volgens Saunders et al. (2009) is er geen specifiek getal wat betreft de steekproefgrootte voor niet-willekeurige steekproeftrekkingen, wanneer er geen steekproefkader is. De steekproefgrootte is in plaats daarvan afhankelijk van de beschikbare middelen (Saunders et al., 2009). Het aantal respondenten die de enquête volledig heeft ingevuld was 261, maar omdat één respondent heeft aangeven geen gebruik te maken van sociale media is deze eruit gefilterd en kwam het uiteindelijke aantal respondenten uit op 260. De leeftijd van de respondenten varieerde tussen de 16 en 29 jaar (Appendix B1), met een gemiddelde leeftijd van 21.70 (*SD* = 3.38). Het aantal vrouwelijke

respondenten is oververtegenwoordigd met 72.7 procent tegenover 27.3 procent aan mannelijke respondenten. De meerderheid van de respondenten, namelijk 82.7 procent, heeft aangegeven nog steeds scholier of student te zijn. Het merendeel van de respondenten, namelijk 48.5 procent, heeft aangegeven wo als afgeronde of huidige opleidingsniveau te hebben. Het aantal respondenten met mbo als opleidingsniveau is ondervertegenwoordigd met 5.8 procent. Een volledig overzicht met de percentages van alle opleidingsniveaus is te vinden in Tabel 2.

Tabel 2. Hoogst afgeronde of huidige opleidingsniveau

Opleidingsniveau	Percentage
Geen	0.8%
Basisschool	3.5%
Vmbo	5.8%
Havo	6.5%
Vwo	8.5%
Mbo	5.8%
Hbo	20.8%
Wo	48.5%

3.7. Operationalisering

De operationalisering is een belangrijk onderdeel om validiteit en betrouwbaarheid van het onderzoek te waarborgen. Validiteit betekent dat het onderzoek op de juiste wijze concepten meet (Gilbert, 2008). Er is getracht validiteit te bereiken door valide indicatoren uit voorgaand onderzoek te gebruiken. Betrouwbaarheid betekent dat het onderzoek repliceerbaar is; herhaalde metingen van hetzelfde item moeten consistent zijn (Gilbert, 2008). Het meten van de betrouwbaarheid van schalen is gedaan via een betrouwbaarheidsanalyse. Via de operationalisering zijn concepten gedefinieerd tot meetbare variabelen (Berger et al., 2016).

3.7.1. Afhankelijke variabelen

De afhankelijke variabelen die in dit onderzoek van belang zijn, zijn het privacybewustzijn en bewuste actie aangaande het beschermen van de eigen online privacy. Het privacybewustzijn is op drie manieren gemeten, namelijk via de perceptie, aandacht en kennis wat betreft verschillende online privacy-kwesties (Van der Velden & El Emam, 2013). Om deze termen te vergemakkelijken zijn deze privacyperceptie, privacy-aandacht en privacykennis genoemd.

3.7.1.1. Privacyperceptie

Privacyperceptie is geoperationaliseerd op een subjectief niveau, sinds perceptie wordt gevormd door hoe er over iets wordt gedacht. Privacyperceptie is gemeten aan de hand van zes items via een Likertschaal (1 = Heel erg oneens, 2 = Oneens, 3 = Redelijk oneens, 4 = Neutraal, 5 = Redelijk eens, 6 = Eens, 7 = Heel erg eens) (Appendix A: Q8). Item 1 'Ik heb vertrouwen in hoe sociale media persoonlijke gegevens beschermen', item 3 'Ik maak sneller gebruik van een gratis online dienst in ruil voor persoonlijke gegevens dan een privacy vriendelijkere dienst waarvoor ik moet betalen' en item 5 'Ik vind het niet prettig wanneer ik persoonlijke gegevens moet geven aan online diensten om deze te kunnen gebruiken' zijn ontwikkeld naar aanleiding van het onderzoek van TNO (2015). Item 2 'Sociale media, zoals Facebook, beschouw ik als privé omgevingen' is ontwikkeld aan de hand van Barnes (2006) en Batist (2015). Item 4 'Ik ben bang dat mijn persoonlijke gegevens voor ongewenste doeleinden worden gebruikt' en item 6 'Ik heb het gevoel te worden gemonitord op het internet' zijn ontwikkeld naar aanleiding van het onderzoek van Centre for International Governance Innovation & IPSOS (2016). Voor items 4, 5 en 6 is de schaal vervolgens omgedraaid (7 = Heel erg oneens, 6 = Oneens, 5 = Redelijk oneens, 4 = Neutraal, 3 = Redelijk eens, 2 = Eens, 1 = Heel erg eens), omdat deze items negatief zijn geformuleerd in vergelijk tot items 1, 2 en 3, die positief zijn geformuleerd.

Er is een factoranalyse uitgevoerd om te achterhalen of de items wel hetzelfde maten of uit meerdere factoren ofwel onderliggende dimensies bestonden. Hierbij is de Oblimin rotatie uitgevoerd, omdat er werd verwacht dat de factoren zijn gecorreleerd. De correlatiematrix toonde meerdere correlatiecoëfficiënten van .3 en hoger aan (Appendix B2). Dit is een voorwaarde voor het uitvoeren van een factoranalyse (Pallant, 2007). De Kaiser-Meyer-Olkin waarde was .643, dat daarmee de aanbevolen minimale waarde van .6 heeft overschreden en de Barlett's Test of Sphericity bereikte statistische significantie (p = .000). Hiermee kon worden geconcludeerd dat de items geschikt waren voor een factoranalyse.

De principal components analyse toonde de aanwezigheid van twee factoren aan met een eigenwaarde boven de 1 (eigenwaarde van 2.11 en 1.27) (Appendix B3), die respectievelijk 35.1 en 21.2 procent van de variantie verklaarde. De Oblimin rotatie toonde aan dat beide factoren een aantal sterke factorladingen (boven .5) hadden en dat de variabelen voornamelijk op een van beide factoren van invloed waren (Appendix B3). Er waren drie items die positief correleerden met de eerste factor, waarbij het item 'Ik vind het niet prettig wanneer ik persoonlijke gegevens moet geven aan online diensten om deze te kunnen gebruiken' de hoogste correlatie had (factorlading was .826 en .835) (Appendix B3). Al deze items hadden betrekking op bezorgde percepties wat betreft het internetgebruik (Appendix B3). Deze factor is gelabeld als 'Bezorgde privacypercepties'. Er waren twee items die positief correleerden met de tweede factor, waarbij het item 'Sociale media, zoals Facebook, beschouw ik als privé omgevingen' de hoogste correlatie had (factorlading was .874 en .817) (Appendix B3). Deze twee items hadden betrekking op vertrouwende percepties wat betreft het internetgebruik (Appendix B3). Deze factor is gelabeld als 'Vertrouwende privacypercepties'.

De gevonden factoren zijn vervolgens getest op hun consistentie via een betrouwbaarheidsanalyse. De Cronbach's Alpha waarde voor de eerste factor was .687, waarmee kon worden geconcludeerd dat de items binnen de eerste factor wat betreft bezorgde privacypercepties een matige consistentie hadden (Appendix B3). De Cronbach's Alpha waarde voor de tweede factor was onder de .6, namelijk .488, waarmee kon worden geconcludeerd dat de items binnen de tweede factor wat betreft vertrouwende privacypercepties niet consistent genoeg waren (Appendix B3). Daarom is besloten om alleen een nieuwe variabele te creëren voor het gemiddelde van de items van de eerste factor met de naam 'Bezorgde privacyperceptie'. Deze variabele kon een waarde vanaf 1 tot en met 7 aannemen. Omdat de drie items wat betreft bezorgde privacyperceptie negatief waren geformuleerd vergeleken de andere drie items en de schaal voor deze drie items dus was omgedraaid, betekent het minimum dat de respondent heeft aangegeven het heel erg eens te zijn met de drie items wat betreft bezorgde privacyperceptie. Een hoge mate van bezorgdheid staat gelijk aan een negatieve perceptie over online privacy. Het maximum betekent dat de respondent heeft aangegeven het heel erg oneens te zijn met de drie items wat betreft bezorgde privacyperceptie en dus vrijwel geen bezorgdheid hierover uitdrukte, wat gelijk staat aan een positieve perceptie over online privacy.

3.7.1.2. Privacy-aandacht

Privacy-aandacht is geoperationaliseerd door de respondenten een lijst van maatregelen voor te leggen, die kunnen worden genomen om de eigen privacy te beschermen en die met vrij weinig moeite kunnen worden toegepast. In deze lijst konden de respondenten aangeven welke items voor hen van toepassing waren (Appendix A: Q9). Item 1 'Ik accepteer geen vriendschapsverzoeken van vreemden op Facebook' en item 4 'Mijn Facebookberichten (statusupdates, foto's, video's, locatie, gevoel) staan ingesteld op 'alleen vrienden'' zijn overgenomen uit het onderzoek van Young en Quan-Haase (2013). Item 12 'Ik heb mijn mobiele telefoonnummer niet gedeeld met Facebook' is overgenomen uit het onderzoek van Tufekci (2008). Item 13 'Ik gebruik een *firewall* en/of virusscanner op mijn computer/laptop' is overgenomen uit het onderzoek van TNO (2015). Item 2 'Ik gebruik wachtwoorden met speciale tekens en cijfers erin', item 3 'Ik lees de privacyvoorwaarden van een online dienst voordat ik deze accepteer', item 5 'Ik verwijder en/of blokkeer cookies', item 7 'Ik gebruik zoveel mogelijk verschillende wachtwoorden voor verschillende online diensten', item 14 'De locatievoorziening op mijn telefoon staat compleet uit', item 16 'Ik laat mijn wachtwoorden niet door de browser onthouden' en item 18 'Ik internet niet op openbare wifi-hotspots of gebruik een VPN-dienst' zijn overgenomen uit het onderzoek gedaan door het Erasmus Magazine aangaande de hack van de website van de Erasmus Universiteit van Rotterdam (Smaling, 2017). Item 9 'Mijn computer/laptop/telefoon is vergrendeld met een wachtwoord/pincode bij het opstarten' en item 11 'Voor al mijn apparaten installeer ik vrijwel altijd direct de beveiligingsupdates' zijn overgenomen uit de zelfverdedigingsgids van Martijn & Tokmetzis (2016b). Item 6 'Ik maak geen gebruik van liveStories op Snapchat' en item 15 'Ik stuur geen Snaps op Snapchat die niet voor iedereen zijn

bedoeld om te zien' zijn ontworpen naar aanleiding van de privacyvoorwaarden van Snapchat (Snap Inc., 2017). Item 10 'Mijn persoonlijke Instagram-profiel staat op privé' is overgenomen aangaande tips op de website van Mijn Online Identiteit (n.d.b). Item 8 'Ik heb mijn e-mailadres op Facebook afgeschermd voor alleen mijzelf of alleen mijn vrienden' en item 17 'Ik ben geen lid van openbare groepen op Facebook' zijn ontworpen naar aanleiding van het eigen Facebookgebruik.

Deze items zijn maatregelen die de sociale en institutionele privacy beschermen. Sociale privacy betreft de controle over wie er toegang heeft tot de persoonlijke informatie van een individueel persoon (Raynes-Goldie, 2010; Siapera, 2012; Van der Velden & El Emam, 2013). Sociale privacy heeft niet alleen betrekking op welke andere sociale mediagebruikers er toegang hebben tot iemands gegevens, maar ook op bijvoorbeeld hackers die toegang proberen te krijgen tot iemands gegevens. Maatregelen die hier van toepassing op zijn, zijn onder andere het gebruiken van wachtwoorden met speciale tekens en cijfers erin of het niet accepteren van vriendschapsverzoeken van vreemden op Facebook. De institutionele privacy heeft betrekking op hoe instituties, zoals sociale media, bedrijven en derde partijen persoonlijke gegevens gebruiken of misbruiken (Raynes-Goldie, 2010; Siapera, 2012; Van der Velden & El Emam, 2013). Maatregelen die hier van toepassing op zijn, zijn onder andere het verwijderen of blokkeren van cookies en het uitzetten van de locatievoorziening op de telefoon. In dit onderzoek is er geen onderscheid gemaakt tussen welke maatregelen de sociale privacy beschermen en welke de institutionele privacy, omdat beiden belangrijk worden geacht. Daarnaast zijn sommige maatregelen op beiden van toepassing, zoals; het niet delen van het telefoonnummer op Facebook waarmee de toegang tot deze informatie verborgen blijft voor andere Facebookgebruikers en waarmee Facebook zelf deze informatie niet kan gebruiken of delen met andere bedrijven, maar ook het niet gebruik maken van LiveStories op Snapchat waarmee een openbaar publiek geen toegang verkrijgt tot de content en waarmee de zakenpartners van Snapchat deze content niet kunnen hergebruiken (Snap Inc., 2017).

Het aantal items waaruit de respondent kon kiezen, was afhankelijk van wat voor antwoord er op vraag 5 'Geef aan van welke sociale media je gebruikmaakt' in de enquête is gegeven (Appendix A: Q5). Wanneer de respondent bij vraag 5 bijvoorbeeld heeft aangegeven geen gebruik te maken van Facebook, Instagram of Snapchat, kreeg de respondent de items die betrekking hadden op de desbetreffende sociale media niet te zien. Wanneer de respondent heeft aangegeven van alle drie de sociale media gebruik te maken, kreeg de respondent alle achttien items te zien. De items die de respondent niet te zien heeft gekregen én de items die de respondent wel te zien heeft gekregen maar niet had aangevinkt, werden allemaal als ontbrekende waarden aangegeven. Om een nieuwe variabele te creëren met een gelijkwaardig gemiddelde van alle toegepaste items per respondent, ongeacht het aantal items waaruit de respondent kon kiezen, zijn alle relevante items die als ontbrekende waarden werden aangegeven (dus de items die de respondent wel te zien heeft gekregen, maar niet had aangevinkt) met de hand naar een nul gecodeerd. Hierdoor zijn alleen de relevante items in de berekening van het gemiddelde opgenomen. Daarom is er gekozen om dit gemiddelde vervolgens te

vermenigvuldigen met honderd, zodat elke respondent het percentage kreeg van het aantal items die voor hem of haar van toepassing waren van het totale aantal relevante items. Deze variabele is 'Privacy-aandacht' genoemd. Deze variabele kon een waarde vanaf 0 tot en met 100 procent aannemen. Het minimum betekent dat er geen enkele maatregel is toegepast, het maximum betekent dat alle relevante maatregelen zijn toegepast.

3.7.1.3. Privacykennis

Privacykennis is op een objectief niveau geoperationaliseerd, waarmee is gemeten in hoeverre de gepercipieerde privacy afweek van de daadwerkelijke privacy ofwel hoe groot het gebrek aan kennis was over online privacy (Batist, 2015). Dit is in de enquête getoetst door middel van goede en foute stellingen, waarbij de respondent kon aangeven of de stelling goed of fout was en wanneer de respondent het antwoord niet wist dit tevens kon aangeven met de optie 'Weet ik niet' (Appendix A: Q10). Om de kennis over privacy te vergroten kreeg de respondent, telkens na het antwoord te hebben gegeven, voor elke quizvraag te zien of hij of zij het antwoord juist of onjuist had met tevens een uitleg van het antwoord, zodat de respondent hier als het ware van kon leren.

Quizvraag 1 is opgesteld aan de hand van Mijn Online Identiteit (n.d.a) en quizvraag 2 aan de hand van het boek van Siapera (2012). Quizvraag 3 is gebaseerd op de privacyvoorwaarden van Facebook (2015). Quizvraag 4, 6 en 7 zijn ontworpen naar aanleiding van het boek van Martijn en Tokmetzis (2016a). Quizvraag 5 is opgesteld aan de hand van de privacyvoorwaarden van Facebook (2015) en Snapchat (Snap Inc., 2017). Quizvraag 8 en 10 zijn gebaseerd op de privacyvoorwaarden van Instagram (2013) en Mijn Online Identiteit (n.d.b). Quizvraag 9 en 11 zijn ontworpen aan de hand van het programma *Hunted* en de privacyvoorwaarden van Snapchat (AVROTROS, 2016b; Snap Inc., 2017). De quizvragen zijn zo opgesteld dat er vijf vragen, namelijk vraag 1, 5, 7, 8 en 10, 'Juist' als goede antwoord hadden en zeven vragen, namelijk vraag 2, 3, 4, 6, 9, 11 en 12, 'Onjuist' als goede antwoord hadden. Deze zijn vervolgens op zo'n manier geplaatst dat er zo min mogelijk een patroon in kon worden gevonden.

Het aantal quizvragen dat de respondent moest beantwoorden, was afhankelijk van wat voor antwoord er op vraag 5 'Geef aan van welke sociale media je gebruikmaakt' in de enquête is gegeven (Appendix A: Q5). Wanneer de respondent bij vraag 5 bijvoorbeeld heeft aangegeven geen gebruik te maken van Facebook, Instagram of Snapchat, kreeg de respondent de quizvragen die betrekking hadden op de desbetreffende sociale media niet te zien. Wanneer de respondent heeft aangegeven van alle drie de sociale media gebruik te maken, kreeg de respondent alle twaalf quizvragen te zien. Omdat alle quizvragen '1 = Juist', '2 = Onjuist' en '3 = Weet ik niet' hadden, ongeacht of het antwoord goed of fout was, zijn de quizvragen afzonderlijk gehercodeerd met '0 = Fout', dat bestaat uit de optie 'Misschien' en het foute antwoord, en '1 = Goed', dat bestaat uit het goede antwoord. Vervolgens is er een nieuwe variabele gecreëerd door het gemiddelde van alle beantwoorde quizvragen te nemen en deze te vermenigvuldigen met tien. Hier is voor gekozen, omdat hierdoor elke respondent een

gelijkwaardig gemiddelde kreeg, ongeacht het aantal quizvragen die de respondent heeft moeten invullen. Deze variabele is 'Privacykennis' genoemd. Deze variabele kon een waarde vanaf 0 tot en met 10 aannemen. Het minimum betekent dat alle quizvragen fout zijn beantwoord en het maximum betekent dat alle relevante quizvragen goed zijn beantwoord.

3.7.1.4. Bewuste actie

Met bewuste actie wordt bedoeld het van plan zijn de eigen online privacy beter te beschermen door bewuster om te gaan met het delen van persoonlijke gegevens op het internet en sociale media. Om bewuste actie te operationaliseren is er gevraagd of de respondent van plan was anders om te gaan met het delen van zijn of haar persoonlijke gegevens na het invullen van de enquête (Appendix A: Q11). Er is naast de opties 'Ja' en 'Nee' ook de optie 'Misschien' toegevoegd, omdat een respondent bijvoorbeeld wel actie zou willen ondernemen, maar niet zou weten hoe of hier eerst beter over na wil denken. Omdat de opties 'Ja' en 'Misschien' allebei aangeven dat er (eventueel) bewuste actie wordt ondernomen én om een binaire logistieke regressie uit te kunnen voeren, is bewuste actie gehercodeerd tot twee categorieën, namelijk; '1 = Positief', dat bestaat uit de opties 'Ja' en 'Misschien', en '0 = Negatief', dat bestaat uit de optie 'Nee'.

3.7.2. Onafhankelijke variabelen

De onafhankelijke variabelen die voor dit onderzoek van belang zijn, zijn leeftijd, opleidingsniveau en actief sociale mediagebruik sinds in de hypotheses is vastgesteld dat deze van invloed kunnen zijn op het privacybewustzijn. Geslacht is in dit onderzoek de controle variabel.

3.7.2.1. Leeftijd

Omdat uit de theorie naar voren kwam dat leeftijd van invloed kan zijn op het privacybewustzijn, is leeftijd als een onafhankelijke variabele opgenomen. Leeftijd is op ratio meetniveau gemeten door de respondent zijn of haar leeftijd aan te laten geven uit de opties 16 tot en met 29 jaar (Appendix A: Q1). Er is gekozen voor een lijst met opties, in plaats van een open veld, zodat mogelijke respondenten die niet binnen de leeftijdspanne van de populatie vielen, konden worden uitgesloten. De veertien verschillende leeftijden, die in het databestand als 1 tot en met 14 werden opgenomen, zijn gehercodeerd met de nummers 0 tot en met 13 om de meervoudige lineaire regressie te vereenvoudigen.

3.7.2.2. Opleidingsniveau

Omdat in de hypotheses is verondersteld dat opleidingsniveau van invloed kan zijn op het privacybewustzijn, is opleidingsniveau als een onafhankelijke variabele opgenomen. Opleidingsniveau is op ordinaal meetniveau gemeten door de respondent zijn of haar huidige of laatste opleidingsniveau

aan te laten geven via een lijst met acht opties (‘1 = Geen’, ‘2 = Basisschool’, ‘3 = Vmbo’, ‘4 = Havo’, ‘5 = Vwo’, ‘6 = Mbo’, ‘7 = Hbo’, ‘8 = Wo)’ (Appendix A: Q3). Deze zijn gehercodeerd tot drie groepen om daarmee een meer evenredige frequentie te verkrijgen tussen de groepen onderling, namelijk; ‘0 = Lagere opleidingsniveaus’, dat bestaat uit de respondenten die geen onderwijs, basisonderwijs, middelbaar onderwijs of mbo hebben aangegeven, ‘1 = Hbo’ en ‘2 = Wo’. Om een meervoudige lineaire regressie uit te kunnen voeren, zijn er twee dummy variabelen gecreëerd; ‘1 = Hbo’ met ‘0 = Anders’ en ‘1 = Wo’ met ‘0 = Anders’, waarbij ‘Lagere opleidingsniveaus’ als referentie fungeerde.

3.7.2.3. Actief sociale mediagebruik

Omdat in de hypotheses is verondersteld dat actief sociale mediagebruik van invloed kan zijn op het privacybewustzijn, is (de frequentie van) actief sociale mediagebruik als een onafhankelijke variabele opgenomen. Met actief sociale mediagebruik wordt bedoeld het zelf delen of posten van foto’s, video’s, statusupdates, comments, gevoel of locaties op sociale netwerksites, waarop deze content ook openbaar kan worden gedeeld. Voordat er in de enquête informatie over het actieve sociale mediagebruik aan de respondent werd gevraagd, werd er eerst gevraagd van welke sociale media hij of zij gebruikmaakt (Appendix A: Q5), zodat de items van vraag 8 en de quizvragen (Appendix A: Q8 & Q10), via weergavelogica’s in Qualtrics, hier automatisch op konden worden afgesteld. De respondent kreeg hierbij de mogelijkheid om meerdere opties aan te geven met ‘1 = Facebook’, ‘2 = Instagram’, ‘3 = Snapchat’ en ‘4 = Anders, namelijk’, waarbij de respondent andere sociale media die hij of zij gebruikt kon aangeven via een open veld. Deze vierde optie is toegevoegd, zodat het aantal opties exhaustief zou zijn. Respondenten die helemaal geen gebruik maken van sociale media werden aan de hand van een filteroptie doorverwezen naar vraag 8, waardoor zij het actieve sociale mediagebruik en de frequentie hiervan niet hoefden in te vullen.

Om actief sociale mediagebruik te meten is ten eerste aan de respondent gevraagd het sociale medium te kiezen waar hij of zij het meest op actieve wijze gebruik van maakt, waarbij de respondent maar één optie kon kiezen (Appendix A: Q6). Om te zorgen dat het aantal opties exhaustief zou zijn, is ook hier de optie ‘Anders, namelijk’ toegevoegd, waarbij de respondent een ander sociaal medium kon aangeven dat hij of zij het meest gebruikt via een open veld. Respondenten die nooit op actieve wijze van sociale media gebruikmaken werden aan de hand van een filteroptie doorverwezen naar vraag 8, waardoor zij de frequentie van actief sociale mediagebruik niet hoefden in te vullen.

De frequentie van actief sociale mediagebruik is gemeten door de respondenten de frequentie van hun actief sociale mediagebruik aan te laten geven via een vierpuntsschaal (‘1 = 1 of meerdere keren per dag’, ‘2 = Minder dan 1 keer per dag maar meer dan 1 keer per week’, ‘3 = Minder dan 1 keer per week maar meer dan 1 keer per maand’, ‘4 = Minder dan 1 keer per maand’) (Appendix A: Q7). Om een meervoudige lineaire regressie uit te kunnen voeren is de frequentie van actief sociale mediagebruik gehercodeerd tot twee categorieën, namelijk; ‘1 = Actiever sociale mediagebruik’, dat

bestaat uit het eerste en tweede item van de vierpuntsschaal, en ‘0 = Minder actief sociale mediagebruik’, dat bestaat uit het derde en vierde item van de vierpuntsschaal. Omdat er in dit onderzoek is gefocust op de mate van het actieve sociale mediagebruik als onafhankelijke variabele, betekent dit dat de twaalf respondenten die bij vraag 6 hebben aangegeven nooit op actieve wijze van sociale media gebruik te maken niet zijn geïncludeerd in de meervoudige lineaire regressies. Met de meervoudige lineaire regressies zijn uiteindelijk dus 248 respondenten geanalyseerd, wat een percentage van 95.4 procent was van het volledige aantal respondenten.

3.7.2.4. Privacykennis

Naast dat privacykennis een afhankelijke variabele is, is het ook een onafhankelijke variabele, omdat in de laatste hypothese is verondersteld dat deze van invloed kan zijn op de kans dat een respondent van plan is bewuste actie te ondernemen om zijn of haar online privacy beter te beschermen.

3.7.2.5. Controle variabelen

Voor het uitvoeren van de meervoudige lineaire regressie analyses en de binaire logistieke regressie analyse is geslacht als controle variabele opgenomen. De respondent is gevraagd zijn of haar geslacht aan te geven (‘1 = Man’ en ‘2 = Vrouw’) (Appendix A: Q2). Om een meervoudige lineaire regressie uit te kunnen voeren is geslacht gehercodeerd naar ‘0 = Man’ en ‘1 = Vrouw’. Voor het uitvoeren van de binaire logistieke regressie zijn tevens opleidingsniveau en leeftijd als controle variabelen opgenomen. Voor opleidingsniveau zijn de drie gehercodeerde groepen ‘0 = Lagere opleidingsniveaus’, ‘1 = Hbo’ en ‘2 = Wo’ gebruikt. Om een binaire logistieke regressie uit te kunnen voeren is leeftijd gehercordeerd, waarbij de leeftijden zijn aangegeven zoals deze werkelijk waren; vanaf 16 tot en met 29.

3.8. Data-analyse

De data is geanalyseerd met SPSS-versie 24. Om het analyseren te vergemakkelijken is er handmatig een case-nummering toegevoegd, zodat de respondenten zijn geordend met de nummers 1 tot en met 260. Er zijn drie meervoudige lineaire regressies uitgevoerd om te testen of de onafhankelijke variabelen leeftijd, opleidingsniveau, actief sociale mediagebruik en de controle variabele geslacht van invloed waren op de afhankelijke variabelen bezorgde privacyperceptie, privacy-aandacht en privacykennis. Daarnaast is er een binaire logistieke regressie uitgevoerd om te testen of privacykennis als onafhankelijke variabele en de controle variabelen geslacht, leeftijd en opleidingsniveau van invloed waren op bewuste actie als afhankelijke variabele.

3.8.1. Meervoudige lineaire regressie analyse

Een meervoudige lineaire regressie analyse wordt gebruikt om de waarde van een afhankelijke variabele te voorspellen aan de hand van twee of meerdere onafhankelijke variabelen (Laerd Statistics, n.d.b). Er is onderzocht of bezorgde privacyperceptie, privacy-aandacht en privacykennis konden worden voorspeld op basis van leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht en in welke mate deze onafhankelijke variabelen van invloed waren op elk van de afhankelijke variabelen. Om een meervoudige regressie uit te kunnen voeren moet de data eerst worden gecontroleerd of deze wel geschikt is voor het uitvoeren van een meervoudige regressie om een valide resultaat te krijgen (Laerd Statistics, n.d.b). Acht aannames zijn daarvoor van belang.

De eerste aanname betreft de afhankelijke variabele die een interval of ratio meetniveau moet hebben (Laerd Statistics, n.d.b). Een interval meetniveau betekent dat de variabele kan worden gemeten langs een continuüm en een getal als waarde heeft (Laerd Statistics, n.d.c). Dit geldt ook voor het ratio meetniveau, maar hier komt bovenop dat deze een absoluut nulniveau heeft, wat aanduidt dat er niks is van de desbetreffende variabele (Laerd Statistics, n.d.c). Bezorgde privacyperceptie bestaat uit het gemiddelde van drie Likertschalen, waarmee deze variabele werd beschouwd als een variabele met een interval meetniveau. Privacy-aandacht en privacykennis werden beschouwd als variabelen met een ratio meetniveau, omdat deze uit scores bestaan met een absoluut nulpunt.

De tweede aanname heeft betrekking op het aantal onafhankelijke variabelen dat een minimum van twee moet zijn met een continue meetniveau (interval of ratio) of een dichotoom nominaal meetniveau (Laerd Statistics, n.d.b). Een dichotoom nominaal meetniveau betekent dat de nominale variabele twee categorieën heeft (Laerd Statistics, n.d.c). Het aantal onafhankelijke variabelen betrof voor alle drie de meervoudige regressies een aantal van vijf, namelijk; leeftijd (ratio), actief sociale mediagebruik (dichotoom nominaal), geslacht als controle variabele (dichotoom nominaal) en de twee dummy variabelen voor opleidingsniveau (dichotoom nominaal).

De derde aanname betreft de onafhankelijkheid van waarnemingen. Dit betekent dat alle waarden van een uitkomst van een andere persoon moeten zijn, wat kan worden getest via de Durbin-Watson test (Laerd Statistics, n.d.b). Ondanks de enquête-bescherming in Qualtrics die verhinderde dat respondenten de enquête meerdere malen konden invullen, waardoor de onafhankelijkheid van waarnemingen niet zou hoeven worden getest, is dit toch wel getest. Het was namelijk wel mogelijk voor respondenten om de enquête meerdere malen in te vullen via verschillende apparaten, zoals een smartphone en een laptop. Een Durbin-Watson waarde van 2 betekent dat de waarnemingen onafhankelijk zijn, een waarde van 0 tot < 2 betekent een positieve correlatie en een waarde van > 2 tot 4 betekent een negatieve correlatie (Grande, 2015). Een waarde dicht bij de 2 is wenselijk. Een vuistregel is dat waarden tussen 1.5 tot 2.5 relatief normaal zijn (Grande, 2015).

De vierde aanname betreft lineariteit tussen de afhankelijke variabele en elk van de onafhankelijke variabelen apart en tussen de afhankelijke variabele en de onafhankelijke variabelen gezamenlijk (Laerd Statistics, n.d.b). Om te bepalen of er een lineaire relatie bestaat tussen de

afhankelijke en de onafhankelijke continue variabelen kunnen partiële regressieplots worden gebruikt (Laerd Statistics, n.d.b). Om te bepalen of er een lineaire relatie bestaat tussen de afhankelijke en onafhankelijke variabelen gezamenlijk kan een scatterplot van *studentized* residuen tegenover ongestandaardiseerde voorspelde waarden worden geanalyseerd (Laerd Statistics, n.d.b). Wanneer de waarnemingen een horizontale band vormen kan worden aangenomen dat er een lineaire relatie is.

De vijfde aanname betreft homoscedasticiteit, wat betekent dat de spreiding (standaardafwijking) van de residuen hetzelfde is voor elke voorspelde waarde van de afhankelijke variabele (Laerd Statistics, n.d.b). Deze kan tevens worden beoordeeld aan de hand van de scatterplot van *studentized* residuen tegenover ongestandaardiseerde voorspelde waarden, waarbij de residuen willekeurig moeten zijn verspreid (Laerd Statistics, n.d.b).

De zesde aanname betreft de afwezigheid van multicollineariteit. Dit betekent dat de onafhankelijke variabelen niet zeer gecorreleerd met elkaar mogen zijn, wat tot problemen kan leiden in het begrijpen van welke onafhankelijke variabele bijdraagt aan de variantie die in de afhankelijke variabele wordt uitgelegd (Laerd Statistics, n.d.b). Multicollineariteit kan worden beoordeeld aan de hand van een controle van de correlatiecoëfficiënten, die geen correlaties hoger dan .7 mogen aantonen, en aan de hand van de tolerantie/VIF-waarden, die geen waarden lager dan .1 – wat een VIF-waarde groter dan 10 is – mogen aantonen (Laerd Statistics, n.d.b).

De zevende aanname betreft de afwezigheid van significante uitschieters, hoge aangrijpingspunten of invloedrijke punten die van negatieve invloed kunnen zijn op de meervoudige regressie analyse en daarmee de voorspellende nauwkeurigheid van de resultaten evenals de statistische significantie kunnen verminderen (Laerd Statistics, n.d.b). De *Casewise Diagnostics* tabel toont gestandaardiseerde residuen groter dan drie standaarddeviaties aan. Een waarde die groter is dan 3 wordt representatief gezien voor een significante uitschieter (Laerd Statistics, n.d.b). Aangrijpingspunten kunnen aan de hand van de *Leverage* waarde worden aangetoond; waarden onder .2 worden als veilig beschouwd, tussen .2 en .5 als riskant en hoger dan .5 als gevaarlijk (Laerd Statistics, n.d.b). Invloedrijke punten kunnen worden opgespoord aan de hand van de *Cook's Distance* die niet groter dan 1 mag zijn (Laerd Statistics, n.d.b).

De achtste en laatste aanname betreft de normale verdeling; waarnemingen moeten redelijk normaal verdeeld zijn om statistische significantie te kunnen bepalen (Laerd Statistics, n.d.b). Dit kan worden aangetoond via visuele inspectie van een histogram met een bovenliggende normale curve en via een P-P Plot waarvan de punten zo veel mogelijk langs de diagonale lijn moeten liggen.

3.8.2. Binaire logistieke regressie analyse

Een binaire logistieke regressie analyse probeert de waarschijnlijkheid te voorspellen dat een waarneming binnen een van de twee categorieën valt van een dichotoom afhankelijke variabele gebaseerd op een of meerdere onafhankelijke variabelen; een waarneming wordt toegewezen aan de categorie die is voorspeld als het meest waarschijnlijke (Laerd Statistics, n.d.a). Er is onderzocht of

aan de hand van privacykennis, geslacht, leeftijd en opleidingsniveau kon worden voorspeld of een waarneming binnen de positieve of negatieve categorie van bewuste actie zou vallen. Om een binaire logistieke regressie uit te kunnen voeren, zijn er zeven aannames die moeten worden overwogen om te controleren of de data wel geschikt is voor het uitvoeren van een binaire logistieke regressie (Laerd Statistics, n.d.a).

De eerste aanname betreft de afhankelijke variabele die dichotoom moet zijn. Bewuste actie was om deze reden gehercodeerd tot '1 = Positief' en '0 = Negatief'. De tweede aanname heeft betrekking op de onafhankelijke variabelen, waarvan er een of meerdere een continue of nominaal meetniveau heeft (Laerd Statistics, n.d.a). Leeftijd[1] als controle variabele en privacykennis werden beschouwd als variabelen met een ratio meetniveau en de twee controle variabelen geslacht en opleidingsniveau werden beschouwd als variabelen met een nominaal meetniveau. De derde aanname betreft onafhankelijkheid van waarnemingen en de exclusiviteit en exhaustiviteit van de afhankelijke en onafhankelijke variabelen (Laerd Statistics, n.d.a). De onafhankelijkheid van waarnemingen is al naar voren gekomen aan de hand van de meervoudige lineaire regressie analyses. Daarnaast mogen de respondenten niet worden geplaatst in beide categorieën binnen de afhankelijke en onafhankelijke variabelen. In dit geval was dat ook zo, omdat de respondenten steeds maar één antwoordoptie konden aangeven wat betreft de vragen die de afhankelijke en onafhankelijke variabelen betroffen (Appendix A: Q1, Q2, Q3 & Q11). De vierde aanname betreft de minimale steekproefgrootte, dat een minimum van vijftien gevallen per onafhankelijke variabele moet zijn (Laerd Statistics, n.d.a). De onafhankelijke variabelen bevatten in dit geval 260 gevallen. De vijfde aanname betreft lineariteit tussen de continue onafhankelijke variabelen en de logit-transformatie van de afhankelijke variabele, wat aan de hand van de Box-Tidwell procedure kan worden beoordeeld met een Bonferroni-correctie (Laerd Statistics, n.d.a). De zesde aanname betreft de afwezigheid van multicollineariteit, wat al naar voren is gekomen aan de hand van de meervoudige lineaire regressie analyses (Laerd Statistics, n.d.a). De zevende en laatste aanname betreft de afwezigheid van significante uitschieters (Laerd Statistics, n.d.a). De *Casewise Diagnostics* tabel toont *studentized* residuen groter dan twee standaarddeviaties aan. Een waarde die groter is dan 2.5 wordt representatief gezien voor een significante uitschieter (Laerd Statistics, n.d.a).

[1] Leeftijd zoals deze werkelijk was, namelijk vanaf 16 tot en met 29 jaar.

4. Resultaten

In dit hoofdstuk worden eerst de descriptieve resultaten besproken en daarna de uitkomsten van de meervoudige lineaire regressie analyses wat betreft bezorgde privacyperceptie, privacy-aandacht en privacykennis. Hierna komt de binaire logistieke regressie analyse met betrekking tot bewuste actie aan bod.

4.1 Descriptieve resultaten

Bijna alle respondenten, namelijk 91.2 procent, gaven aan een Facebookaccount te hebben. Instagram volgde Facebook op met 76.5 procent en Snapchat volgde met 70.8 procent. Meer dan de helft van de respondenten, namelijk 56.2 procent, gaf aan gebruik te maken van alle drie de sociale media en 1.2 procent van de respondenten gaf aan andere sociale media te gebruiken dan Facebook, Instagram en Snapchat. Van de 95.4 procent van de respondenten die heeft aangegeven op actieve wijze van sociale media gebruik te maken (wat het zelf delen of posten van foto's, video's, comments, statusupdates, gevoel of locaties op sociale netwerksites is), gaf 46.4 procent aan dit meer dan één keer per week te doen en 53.6 procent minder dan één keer per week (Tabel 1). Facebook was ook het medium waarvan het meest actief gebruik wordt gemaakt, namelijk door 35.1 procent van de respondenten die heeft aangegeven op actieve wijze van sociale media gebruik te maken. Snapchat en Instagram deden daar niet voor onder met respectievelijk 30.6 en 29.8 procent van de respondenten die heeft aangegeven op actieve wijze sociale media te gebruiken.

Tabel 1. Frequentie van actief content delen op het meest gebruikte sociale medium in procenten (N = 248)

Frequentie		Percentage
Actiever sociale mediagebruik	1 of meerdere keren per dag	29.8%
	Minder dan 1 keer per dag maar meer dan 1 keer per week	16.5%
Minder actief sociale mediagebruik	Minder dan 1 keer per week maar meer dan 1 keer per maand	24.2%
	Minder dan 1 keer per maand	29.4%

Uit deze gegevens blijkt dus dat bijna alle respondenten aangaven gebruik te maken van Facebook en dat meer dan de helft van het aantal respondenten aangaf gebruik te maken van alle drie de sociale media; Facebook, Instagram en Snapchat. Daarnaast gaf bijna de helft van de respondenten aan meer dan één keer per week op actieve wijze gebruik te maken van sociale media. Dit strookt met de theorie dat veel jongeren gebruikmaken van sociale media en tevens op actieve wijze (persoonlijke) data delen met de desbetreffende sociale media (Baelden, 2013; Oosterveer, 2016; Van der Veer, 2016; Young & Quan-Haase 2013).

Wat betreft bezorgde privacyperceptie was het gemiddelde van de drie stellingen bij elkaar 3.40 (*SD* = 1.15), wat tussen 'Redelijk eens' (3) en 'Neutraal' (4) ligt. Daarnaast gaf 53.9 procent van de respondenten aan het redelijk tot heel erg mee eens te zijn met de stelling 'Ik ben bang dat mijn persoonlijke gegevens voor ongewenste doeleinden worden gebruikt'. Ook gaf 69.3 procent van de respondenten aan het redelijk tot heel erg mee eens te zijn met de stelling 'Ik vind het niet prettig wanneer ik persoonlijke gegevens moet geven aan online diensten om deze te kunnen gebruiken' en gaf 58.5 procent van de respondenten aan het redelijk tot heel erg mee eens te zijn met de stelling 'Ik heb het gevoel te worden gemonitord op het internet'. Het merendeel van de respondenten drukte zich dus bezorgd uit, wat betekent dat zij een negatieve perceptie hadden over online privacy. Respectievelijk 15.0, 13.1 en 16.9 procent van de respondenten gaf aan neutraal te zijn wat betreft deze drie stellingen. Respectievelijk 31.2, 17.8 en 24.6 procent van de respondenten was het redelijk tot heel erg oneens met de drie stellingen. Dit betekent dat zij minder tot geen bezorgdheid uitdrukten en dus een positievere perceptie hadden over online privacy. Een volledig overzicht met de percentages voor alle posities per stelling wat betreft bezorgde privacyperceptie is te vinden in Tabel 2.

Tabel 2. Overzicht van alle posities van de drie stellingen wat betreft bezorgde privacyperceptie in procenten (*N* = 260)

Positie	Ik ben bang dat mijn persoonlijke gegevens voor ongewenste doeleinden worden gebruikt	Ik vind het niet prettig wanneer ik persoonlijke gegevens moet geven aan online diensten om deze te kunnen gebruiken	Ik heb het gevoel te worden gemonitord op het internet
Heel erg eens	3.5%	11.2%	7.7%
Eens	16.2%	28.1%	22.7%
Redelijk eens	34.2%	30.0%	28.1%
Neutraal	15.0%	13.1%	16.9%
Redelijk oneens	17.3%	10.8%	12.7%
Oneens	10.8%	5.8%	9.2%
Heel erg oneens	3.1%	1.2%	2.7%

Wat betreft privacy-aandacht, in de vorm van maatregelen om de online privacy te beschermen, is 'Mijn computer/laptop/telefoon is vergrendeld met een wachtwoord/pincode bij het opstarten' het meest toegepast, namelijk door 92.3 procent van het totale aantal respondenten. Dit werd gevolgd door 'Ik accepteer geen vriendschapsverzoeken van vreemden op Facebook' wat door 91.1 procent van de respondenten die Facebook gebruikt is toegepast. 'Ik internet niet op openbare wifi-hotspots of gebruik een VPN-dienst' en 'Ik lees de privacyvoorwaarden van een online dienst voordat ik deze accepteer' zijn het minst toegepast, namelijk door respectievelijk 10.0 en 9.6 procent van het totale aantal respondenten. Een volledig overzicht van alle privacymaatregelen met het percentage

respondenten dat deze maatregelen heeft toegepast is te vinden in Tabel 3. Wat opvalt is dat bepaalde maatregelen maar heel weinig zijn toegepast. Zo heeft slechts 29.6 procent van het totale aantal respondenten aangegeven beveiligingsupdates direct te installeren op apparaten. Dit kan juist grote schade veroorzaken wanneer het niet wordt gedaan, zoals vele bedrijven en instanties hebben kunnen ondervinden tijdens de al eerdergenoemde internationale gijzelsoftware-aanval op 12 mei 2017, omdat ze niet meteen de nieuwste systeemupdate van Windows hadden geïnstalleerd (Houthuijs, 2017). Ook het verwijderen of blokkeren van cookies is door een opvallend laag percentage van het totale aantal respondenten toegepast, namelijk door 20.4 procent, terwijl cookies juist zeer veel data over gebruikers verzamelen wat vaak wordt doorverkocht aan derde partijen (Martijn & Tokmetzis, 2016a; Nissenbaum, 2011).

Tabel 3. Overzicht van toegepaste privacymaatregelen in procenten

Maatregel	Percentage	*N* (totaal)
Mijn computer/laptop/telefoon is vergrendeld met een wachtwoord/pincode bij het opstarten	92.3%	260
Ik accepteer geen vriendschapsverzoeken van vreemden op Facebook	91.1%	237
Mijn Facebookberichten (…) staan ingesteld op 'alleen vrienden'	84.0%	237
Ik gebruik wachtwoorden met speciale tekens en cijfers erin	80.8%	260
Ik heb mijn e-mailadres op Facebook afgeschermd voor alleen mijzelf/mijn vrienden	70.9%	237
Ik gebruik een firewall en/of virusscanner op mijn computer/laptop	66.2%	260
Ik heb mijn mobiele telefoonnummer niet gedeeld met Facebook	64.6%	237
Ik stuur geen Snaps op Snapchat die niet voor iedereen zijn bedoeld om te zien	62.5%	184
Mijn persoonlijke Instagram-profiel staat op privé	60.3%	199
Ik maak geen gebruik van liveStories op Snapchat	52.7%	184
Voor al mijn apparaten installeer ik vrijwel altijd direct de beveiligingsupdates	29.6%	260
Ik laat mijn wachtwoorden niet door de browser onthouden	26.5%	260
De locatievoorziening op mijn telefoon staat compleet uit	25.4%	260
Ik gebruik zoveel mogelijk verschillende wachtwoorden voor verschillende online diensten	24.2%	260
Ik verwijder en/of blokkeer cookies	20.4%	260
Ik ben geen lid van openbare groepen op Facebook	11.0%	237
Ik internet niet op openbare wifi-hotspots of gebruik een VPN-dienst	10.0%	260
Ik lees de privacyvoorwaarden van een online dienst voordat ik deze accepteer	9.6%	260

Let op: De maatregelen staan in volgorde van meest toegepast tot minst toegepast.

Het gemiddelde percentage van het aantal toegepaste maatregelen was 48.1 procent (*SD* = 14.6). Dit betekent dat de gemiddelde respondent meer dan 50 procent van de voor hem of haar relevante maatregelen niet heeft toegepast.

De gemiddelde quizscore was 6.5 (*SD* = 1.52). Dit betekent dat de privacykennis nog wel degelijk mag en moet worden verhoogd. Het is immers wenselijk om zoveel mogelijk kennis over online privacy te hebben. Wat betreft de quizvragen zelf hebben de meesten, namelijk 93.1 procent van het totale aantal respondenten, vraag 7 over cookies goed beantwoord (Appendix A: Q10.7). Zeven van de twaalf vragen zijn door minder dan 75 procent van de respondenten goed beantwoord. Vraag 11 'Snapchat geeft altijd een melding wanneer en door wie er een screenshot is gemaakt van je Snap' hebben de meesten, namelijk 78.3 procent van de respondenten die Snapchat gebruikt, fout beantwoord; zij dachten dat deze stelling juist was terwijl deze onjuist was (Appendix A: Q10.11). Ook vraag 1 'Een website die begint met 'http://' is een website die gebruikmaakt van een onbeveiligde verbinding' hebben veel respondenten van het totale aantal, namelijk 69.2 procent, fout beantwoord; zij dachten dat deze stelling onjuist was terwijl deze juist was (Appendix A: Q10.1). En vraag 3 'Je bepaalt zelf wie er toegang heeft tot de inhoud en informatie op je Facebookprofiel' hebben veel respondenten die Facebook gebruiken, namelijk 67.1 procent, fout beantwoord; zij dachten dat deze stelling juist was terwijl deze onjuist was (Appendix A: Q10.3). Een volledig overzicht met de percentages van alle goed en fout beantwoorde quizvragen is te vinden in Tabel 4. Uit het overzicht van de quizvragen blijkt dat respondenten kennis misten over bepaalde onderwerpen. Hiermee kan worden gesteld dat voor deze desbetreffende onderwerpen de gepercipieerde privacy afweek van de werkelijke privacy (Batist, 2015).

Tabel 4. Overzicht van de uitkomst van de quizvragen in procenten

Vraag nr.	Onderwerp	Goed	Fout	*N* (totaal)
1	Onbeveiligde websiteverbinding	**30.8**%	69.2%	260
2	Banken en verzekeringsmaatschappijen	86.9%	13.1%	260
3	Toegang Facebookprofiel	**32.9**%	67.1%	237
4	Apparaat hacken	**73.8**%	26.2%	260
5	Sociale media bescherming	91.5%	8.5%	260
6	Openbaar wifinetwerk	**36.5**%	63.5%	260
7	Cookies	93.1%	6.9%	260
8	Instagram hashtags	**53.8**%	46.2%	199
9	Snap verwijderen	**74.5**%	25.5%	184
10	Instagram openbaar profiel	88.9%	11.1%	199
11	Snapchat screenshot	**21.7**%	78.3%	184
12	Facebook opzeggen	82.3%	17.7%	237

Let op: Vragen die juist zijn beantwoord door minder dan 75% van het totale aantal respondenten zijn dikgedrukt.

Wat betreft bewuste actie gaf 18.8 procent van de respondenten, via vraag 11 (Appendix A: Q11), aan van plan te zijn anders om te gaan met het delen van persoonlijke gegevens na het invullen van de vragenlijst. Ook gaf 40.8 procent van de respondenten aan misschien van plan te zijn anders om te gaan met het delen van persoonlijke gegevens (Tabel 5). Dit geeft aan dat 59.6 procent er bewust over nadacht om de online privacy beter te beschermen.

Tabel 5. Frequentie van bewuste actie in procenten (*N* = 260)

Actie	Percentage
Ja	18.8%
Misschien	40.8%
Nee	40.4%

4.2. Resultaat bezorgde privacyperceptie

Een meervoudige lineaire regressie is uitgevoerd om bezorgde privacyperceptie te voorspellen gebaseerd op leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht. Er was onafhankelijkheid van waarnemingen, zoals beoordeeld door een Durbin-Watson statistiek van 2.121. Er was lineariteit, zoals beoordeeld door een partiële regressie plot (Appendix B4) en een scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B5). Er was homoscedasticiteit, zoals beoordeeld door middel van visuele inspectie van de scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B5). Er was geen bewijs van multicollineariteit, zoals beoordeeld aan de hand van een controle van de correlatiecoëfficiënten groter dan .7 (Appendix B6) en de tolerantiewaarden groter dan .1 (Appendix B7). Er waren twee gestandaardiseerde residuen groter dan ± 3 standaarddeviaties (Appendix B8), welke na inspectie uit de analyse zijn gefilterd.

Een nieuwe meervoudige lineaire regressie is uitgevoerd om de bezorgde privacyperceptie te voorspellen gebaseerd op leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht. Er was onafhankelijkheid van waarnemingen, zoals beoordeeld door een Durbin-Watson statistiek van 2.068. Er was lineariteit, zoals beoordeeld door een partiële regressie plot (Appendix B9) en een scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B10). Er was homoscedasticiteit, zoals beoordeeld door middel van visuele inspectie van de scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B10). Er was geen bewijs van multicollineariteit, zoals beoordeeld aan de hand van een controle van de correlatiecoëfficiënten groter dan .7 (Appendix B11) en de tolerantiewaarden groter dan .1 (Appendix B12). Er waren geen gestandaardiseerde residuen groter dan ± 3 standaarddeviaties. Er waren geen *Leverage* waarden groter dan .2 en er waren geen waarden van *Cook's Distance* boven 1. Er was een redelijk normale verdeling, zoals beoordeeld door een histogram met een bovenliggende normale

curve (Appendix B13) en een P-P Plot (Appendix B14).

Het meervoudige lineaire regressiemodel voorspelde bezorgde privacyperceptie statistisch significant, F (5, 240) = 5.261, $p < .0005$. Het regressiemodel was dus nuttig voor het voorspellen van de waarde van bezorgde privacyperceptie, maar de voorspellende kracht was laag; 9.9 procent van de verschillen in de waarde van bezorgde privacyperceptie kon worden voorspeld op basis van leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht (R^2 = .099, aangepaste R^2 = .080). Alleen de onafhankelijke variabelen actief sociale mediagebruik, B = .383, t = 2.68, p = .008, 95% *CI* [.102, .664] en hbo als opleidingsniveau, B = -.483, t = -2.02, p = .045, 95% *CL* [-.955, -.011] hadden een significant effect.

Hoe lager het gemiddelde van bezorgde privacyperceptie is, hoe meer de respondent het eens was met de stellingen 'Ik ben bang dat mijn persoonlijke gegevens voor ongewenste doeleinden worden gebruikt.', 'Ik vind het niet prettig wanneer ik persoonlijke gegevens moet geven aan online diensten om deze te kunnen gebruiken' en 'Ik heb het gevoel te worden gemonitord op het internet'. Hoe hoger het gemiddelde van bezorgde privacyperceptie is, hoe minder de respondent het eens was met deze stellingen. De voorspelde bezorgde privacyperceptie was voor actiever sociale mediagebruik .384 hoger dan voor minder actief sociale mediagebruik. Dit betekent dat respondenten die actiever gebruikmaken van sociale media het iets minder eens waren met de stellingen wat betreft bezorgde privacyperceptie dan respondenten die minder op actieve wijze gebruikmaken van sociale media.

De voorspelde bezorgde privacyperceptie was voor respondenten met hbo als opleidingsniveau .483 lager vergeleken met respondenten die binnen de lagere opleidingsniveaus (= geen, basisschool, middelbare school of mbo) vielen. Dit betekent dat respondenten met hbo als opleidingsniveau het iets meer eens waren met de stellingen wat betreft bezorgde privacyperceptie dan respondenten met een lager opleidingsniveau. Voor deze effecten werd ervan uitgegaan dat de andere onafhankelijke variabelen constant bleven. Regressiecoëfficiënten zijn te vinden in Tabel 6.

$H_{1.1}$: 'Hoe hoger de leeftijd is, hoe negatiever de perceptie over online privacy' wordt niet ondersteund wat betreft bezorgde privacyperceptie als onderdeel van het privacybewustzijn, omdat er geen significantie was. Dit komt niet overeen met eerder onderzoek waarin leeftijd wel een significant effect had op de perceptie (TNO, 2015). $H_{2.1}$: 'Hoe hoger het opleidingsniveau is, hoe negatiever de perceptie over online privacy' wordt deels ondersteund wat betreft bezorgde privacyperceptie als onderdeel van het privacybewustzijn, omdat er geen significant verschil was tussen wo en de lagere opleidingsniveaus, maar wel tussen hbo en de lagere opleidingsniveaus. Uit de meervoudige lineaire regressie kwam namelijk naar voren dat respondenten met hbo als opleidingsniveau het iets meer eens waren met de stellingen wat betreft bezorgde privacyperceptie dan respondenten met een lager opleidingsniveau. Respondenten met hbo als opleidingsniveau uitten dus een iets hogere mate van bezorgdheid en hadden daarmee een iets negatievere perceptie over online privacy dan respondenten met een lager opleidingsniveau. In vorig onderzoek was er geen significant verschil tussen hoger en lager opgeleiden (TNO, 2015). Het is daarom opvallend dat er geen significant verschil was tussen de

respondenten met wo als opleidingsniveau en de respondenten met de lagere opleidingsniveaus, maar wel een significant verschil tussen de respondenten met hbo als opleidingsniveau en de respondenten met de lagere opleidingsniveaus.

$H_{3.1}$: 'Hoe actiever het sociale mediagebruik is, hoe positiever de perceptie is over online privacy' wordt wel ondersteund wat betreft bezorgde privacyperceptie als onderdeel van het privacybewustzijn, omdat de mate van actief sociale mediagebruik een significant effect had op de bezorgde privacyperceptie. Uit de meervoudige lineaire regressie kwam namelijk naar voren dat respondenten die actiever gebruikmaken van sociale media het iets minder eens waren met de stellingen wat betreft bezorgde privacyperceptie dan respondenten die minder op actieve wijze gebruikmaken van sociale media. Respondenten die op actievere wijze gebruikmaken van sociale media uitten dus een iets minder hoge mate van bezorgdheid en hadden daarmee een iets positievere perceptie over online privacy dan respondenten die op minder actieve wijze gebruikmaken van sociale media. In vorig onderzoek kwam naar voren dat de respondenten die geen gebruik maken van sociale media een hogere mate aan zorgen uitdrukken dan de respondenten die wel gebruikmaken van sociale media (Tufekci, 2008). Er is dus ook een verschil in het uitdrukken van bezorgdheden met betrekking tot online privacy tussen sociale mediagebruikers die op actievere wijze en minder actieve wijze van sociale media gebruikmaken.

Tabel 6. Meervoudig regressiemodel voor het voorspellen van bezorgde privacyperceptie (N = 246)

Variabele	*B*
Intercept	3.672
Leeftijd	-.036
Mannelijk geslacht	
Vrouwelijk geslacht	-.117
Minder actief sociale mediagebruik	
Actiever sociale mediagebruik	.383**
Lagere opleidingsniveaus	
Hbo	-.483*
Wo	-.168
R^2	.099
Aangepaste R^2	.080
F	5.261***

Significantie levels: * $p < .05$ ** $p < .01$ *** $p < .0005$

Let op: *B* = ongestandaardiseerde regressiecoëfficiënten.

4.3. Resultaat privacy-aandacht

Een meervoudige lineaire regressie is uitgevoerd om privacy-aandacht te voorspellen gebaseerd op leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht. Er was onafhankelijkheid van waarnemingen, zoals beoordeeld door een Durbin-Watson statistiek van 2.088. Er was lineariteit, zoals beoordeeld door een partiële regressie plot (Appendix B15) en een scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B16). Er was homoscedasticiteit, zoals beoordeeld door middel van visuele inspectie van de scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B16). Er was geen bewijs van multicollineariteit, zoals beoordeeld aan de hand van een controle van de correlatiecoëfficiënten groter dan .7 (Appendix B17) en de tolerantiewaarden groter dan .1 (Appendix B7). Er was één gestandaardiseerde residu groter dan ± 3 standaarddeviaties (Appendix B18), welke na inspectie uit de analyse is gefilterd.

Een nieuwe meervoudige lineaire regressie is uitgevoerd om privacy-aandacht te voorspellen gebaseerd op leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht. Er was onafhankelijkheid van waarnemingen, zoals beoordeeld door een Durbin-Watson statistiek van 2.037. Er was een kleine lineariteit, zoals beoordeeld door een partiële regressie plot (Appendix B19) en een scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B20). Er was homoscedasticiteit, zoals beoordeeld door middel van visuele inspectie van de scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B20). Er was geen bewijs van multicollineariteit, zoals beoordeeld aan de hand van een controle van de correlatiecoëfficiënten groter dan .7 (Appendix B21) en de tolerantiewaarden groter dan .1 (Appendix B22). Er waren geen gestandaardiseerde residuen groter dan ± 3 standaarddeviaties. Er waren geen *Leverage* waarden groter dan .2 en geen waarden van *Cook's Distance* boven 1. Er was een redelijk normale verdeling, zoals beoordeeld door een histogram met een bovenliggende normale curve (Appendix B23) en een P-P Plot (Appendix B24).

Het meervoudige lineaire regressiemodel voorspelde privacy-aandacht niet statistisch significant, F (5, 241) = .810, p = .543. Het regressiemodel was dus niet nuttig voor het voorspellen van de waarde van privacy-aandacht, wat ook te zien was aan de zeer lage voorspellende kracht; 1.7 procent van de verschillen in de waarde van privacy-aandacht kon worden voorspeld op basis van leeftijd, opleidingsniveau, actief sociale mediagebruiken geslacht (R^2 = .017, aangepaste R^2 = -.004). Geen enkele van de onafhankelijke variabelen had een significant effect. Regressiecoëfficiënten zijn te vinden in Tabel 7.

$H_{1.2}$: 'Hoe hoger de leeftijd is, hoe meer maatregelen zijn toegepast om de online privacy te beschermen' wordt niet ondersteund wat betreft privacy-aandacht als onderdeel van het privacybewustzijn, omdat er geen significantie was. Dit komt niet overeen met eerder onderzoek waarin naar voren kwam dat jongvolwassenen minder beschermend optreden wat betreft online privacy dan oudere leeftijdscategorieën (TNO, 2015). $H_{2.2}$: 'Hoe hoger het opleidingsniveau is, hoe

meer maatregelen zijn toegepast om de online privacy te beschermen' wordt niet ondersteund wat betreft privacy-aandacht als onderdeel van het privacybewustzijn, omdat er geen significant verschil was tussen hbo als opleidingsniveau en de lagere opleidingsniveaus en tussen wo als opleidingsniveau en de lagere opleidingsniveaus. $H_{3.2}$: 'Hoe actiever het sociale mediagebruik is, hoe minder maatregelen zijn toegepast om de online privacy te beschermen' wordt niet ondersteund wat betreft privacy-aandacht als onderdeel van het privacybewustzijn, omdat er geen significant verschil was tussen actiever sociale mediagebruik en minder actief sociale mediagebruik.

Daarnaast was het algehele regressiemodel niet statistisch significant, waarmee kan worden geconcludeerd dat leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht als controle variabele geen significant effect hadden op het gemiddelde aantal maatregelen dat respondenten hadden toegepast om hun online privacy te beschermen.

Tabel 7. Meervoudig regressiemodel voor het voorspellen van privacy-aandacht (N = 247)

Variabele	*B*
Intercept	44.559
Leeftijd	-.145
Mannelijk geslacht	
Vrouwelijk geslacht	.989
Minder actief sociale mediagebruik	
Actiever sociale mediagebruik	.492
Lagere opleidingsniveaus	
Hbo	4.566
Wo	4.778
R^2	.017
Aangepaste R^2	-.004
F	.810

Let op: *B* = ongestandaardiseerde regressiecoëfficiënten.

4.4. Resultaat privacykennis

Een meervoudige lineaire regressie is uitgevoerd om de privacykennis te voorspellen gebaseerd op leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht. Er was onafhankelijkheid van waarnemingen, zoals beoordeeld door een Durbin-Watson statistiek van 2.139. Er was lineariteit, zoals beoordeeld door een partiële regressie plot (Appendix B25) en een scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B26). Er was homoscedasticiteit, zoals beoordeeld door middel van visuele inspectie van de scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B26). Er was geen bewijs van multicollineariteit, zoals beoordeeld aan de hand van een controle van de

correlatiecoëfficiënten groter dan .7 (Appendix B27) en de tolerantiewaarden groter dan .1 (Appendix B7). Er was één gestandaardiseerde residu groter dan ± 3 standaarddeviaties (Appendix B28), welke na inspectie uit de analyse is gefilterd.

Een nieuwe meervoudige lineaire regressie is uitgevoerd om privacykennis te voorspellen gebaseerd op leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht. Er was onafhankelijkheid van waarnemingen, zoals beoordeeld door een Durbin-Watson statistiek van 2.136. Er was lineariteit, zoals beoordeeld door een partiële regressie plot (Appendix B29) en een scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B30). Er was homoscedasticiteit, zoals beoordeeld door middel van visuele inspectie van de scatterplot van de *studentized* residuen tegenover de ongestandaardiseerde voorspelde waarden (Appendix B30). Er was geen bewijs van multicollineariteit, zoals beoordeeld aan de hand van een controle van de correlatiecoëfficiënten groter dan .7 (Appendix B31) en de tolerantiewaarden groter dan .1 (Appendix B32). Er waren geen gestandaardiseerde residuen groter dan ± 3 standaarddeviaties. Er waren geen *Leverage* waarden groter dan .2 en geen waarden van *Cook's Distance* boven 1. Er was een redelijk normale verdeling, zoals beoordeeld door een histogram met een bovenliggende normale curve (Appendix B33) en een P-P Plot (Appendix B34).

Het meervoudige lineaire regressiemodel voorspelde privacykennis statistisch significant, F (5, 241) = 4.306, p = .001. Het regressiemodel was dus nuttig voor het voorspellen van de waarde van privacykennis, maar de voorspellende kracht was laag; 8.2 procent van de verschillen in de waarde van privacykennis kon worden voorspeld op basis van leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht (R^2 = .082, aangepaste R^2 = .063). Alleen de onafhankelijke variabele geslacht had een significant effect, B = -.662, t = -2.99, p = .003, 95% *CI* [-1.099, -.225].

Hoe hoger de gemiddelde privacykennis is, hoe meer quizvragen de respondent goed heeft beantwoord. De voorspelde privacykennis was voor vrouwelijke respondenten .662 lager dan voor mannelijke respondenten, wat betekent dat vrouwelijke respondenten iets lager scoorden op de quizvragen dan mannelijke respondenten. Voor dit effect werd ervan uitgegaan dat de andere onafhankelijke variabelen constant bleven. Regressiecoëfficiënten zijn te vinden in Tabel 8.

$H_{1.3}$: 'Hoe hoger de leeftijd is, hoe hoger de kennis over online privacy' wordt niet ondersteund wat betreft privacykennis als onderdeel van het privacybewustzijn, omdat er geen significantie was. $H_{2.3}$: 'Hoe hoger het opleidingsniveau is, hoe hoger de kennis over online privacy' wordt niet ondersteund wat betreft privacykennis als onderdeel van het privacybewustzijn, omdat er geen significant verschil was tussen hbo als opleidingsniveau en de lagere opleidingsniveaus en tussen wo als opleidingsniveau en de lagere opleidingsniveaus. $H_{3.3}$: 'Hoe actiever het sociale mediagebruik is, hoe lager de kennis over online privacy' wordt niet ondersteund wat betreft privacykennis als onderdeel van het privacybewustzijn, omdat er geen significant verschil was tussen actiever sociale mediagebruik en minder actief sociale mediagebruik. De controle variabele geslacht daarentegen had wel een significant effect op de privacykennis als onderdeel van het privacybewustzijn; vrouwelijke

respondenten scoorden significant lager dan mannelijke respondenten.

Tabel 8. Meervoudig regressiemodel voor het voorspellen van privacykennis (N = 247)

Variabele	*B*
Intercept	6.899
Leeftijd	.049
Mannelijk geslacht	
Vrouwelijk geslacht	-.662**
Minder actief sociale mediagebruik	
Actiever sociale mediagebruik	-.250
Lagere opleidingsniveaus	
Hbo	-.237
Wo	-.072
R^2	.082
Aangepaste R^2	.063
F	4.306*

Significantie levels: * $p < .05$ ** $p < .005$

Let op: *B* = ongestandaardiseerde regressiecoëfficiënten.

4.5. Resultaat bewuste actie

Een binaire logistieke regressie is uitgevoerd om het effect van privacykennis na te gaan op de waarschijnlijkheid dat respondenten wel of niet van plan waren bewuste actie te ondernemen. Lineariteit van de continue variabelen met betrekking tot de logit van de afhankelijke variabele is beoordeeld via de Box-Tidwell procedure. Een Bonferroni-correctie is toegepast met behulp van alle negen termen in het model, waardoor er statistische significantie werd geaccepteerd bij $p < .00556$. Op basis van deze beoordeling bleken alle continue onafhankelijke variabelen lineair te zijn aan de logit van de afhankelijke variabele. Er waren geen *studentized* residuen met een waarde groter dan ± 2.5 standaarddeviaties.

Het logistieke regressiemodel was statistisch significant, χ^2 (5) = 14.445, p = .020. Het model legde 6.8 procent (Nagelkerke R^2) uit van de variantie in bewuste actie en classificeerde 61.5 procent van de gevallen op correcte wijze. Gevoeligheid was 84.5 procent, specificiteit was 27.6 procent, de positief voorspellende waarde was 63.3 procent en de negatief voorspellende waarde was 54.7 procent. Van de zes voorspellende variabelen waren de variabelen privacykennis en (werkelijke) leeftijd laag significant[2].

[2] Er wordt gesproken van laag significant, omdat de *p*-waarde kleiner was dan .1 maar groter dan .05.

Een verhoging van één eenheid in privacykennis betekende dat de kans op het van plan zijn bewuste actie te ondernemen verminderde met een factor van .840. Een vermindering van één eenheid in privacykennis betekende dat de kans op het van plan zijn bewuste actie te ondernemen verhoogde met een factor van 1.19 (= 1 / .840). Een toenemende privacykennis werd dus geassocieerd met een verminderde kans op het van plan zijn bewuste actie te ondernemen en een afnemende privacykennis werd geassocieerd met een verhoogde kans op het van plan zijn bewuste actie te ondernemen.

Een verhoging van één eenheid in leeftijd betekende dat de kans op het van plan zijn bewuste actie te ondernemen verminderde met een factor van .909. Een vermindering van één eenheid in leeftijd betekende dat de kans op het van plan zijn bewuste actie te ondernemen verhoogde met een factor van 1.10 (= 1 / .909). Een toenemende leeftijd werd dus geassocieerd met een verminderde kans op het van plan zijn bewuste actie te ondernemen en een afnemende leeftijd werd geassocieerd met een verhoogde kans op het van plan zijn bewuste actie te ondernemen. Voor deze effecten werd ervan uitgegaan dat de andere onafhankelijke variabelen constant bleven. Regressiecoëfficiënten en de kans ratio zijn te vinden in Tabel 9.

Tabel 9. Logistiek regressiemodel die de waarschijnlijkheid van bewuste actie voorspelt (N = 260)

Variabele	*B*	Kans ratio
Mannelijk geslacht		
Vrouwelijk geslacht	.318	1.375
Lagere opleidingsniveaus		
Hbo	.065	1.067
Wo	.344	1.410
(Werkelijke) leeftijd	-.095*	.909
Privacykennis	-.175*	.840
Aangepaste R^2	.068	
χ^2	14.445**	

Significantie levels: * $p < .1$ ** $p < .05$

Let op: *B* = ongestandaardiseerde regressiecoëfficiënten.

H4: ‘Hoe lager de initiële kennis (in de vorm van de quizscore) is, hoe hoger de kans dat er bewuste actie wordt gepland om de online privacy beter te beschermen’ wordt ondersteund, omdat privacykennis een laag significant effect had op het wel of niet van plan zijn bewuste actie te ondernemen om de online privacy beter te beschermen. Uit de binaire logistieke regressie kwam namelijk naar voren dat een toenemende privacykennis werd geassocieerd met een verminderde kans op het van plan zijn bewuste actie te ondernemen en een afnemende privacykennis met een verhoogde kans op het van plan zijn bewuste actie te ondernemen. Hoe hoger de (initiële) privacykennis was, hoe lager de kans dat de respondent van plan was bewuste actie te ondernemen en hoe lager de (initiële)

privacykennis was, hoe hoger de kans dat de respondent van plan was bewuste actie te ondernemen.

Opleidingsniveau en geslacht als controle variabelen hadden geen significant effect op bewuste actie. De controle variabele leeftijd had een laag significant effect op bewuste actie. Uit de binaire logistieke regressie kwam namelijk naar voren dat een toenemende leeftijd werd geassocieerd met een verminderde kans op het van plan zijn bewuste actie te ondernemen en een afnemende leeftijd met een verhoogde kans op het van plan zijn bewuste actie te ondernemen. Hoe ouder de respondent was, hoe lager de kans dat hij of zij van plan was bewuste actie te ondernemen en hoe jonger de respondent was, hoe hoger de kans dat hij of zij van plan was bewuste actie te ondernemen.

5. Conclusie

In dit hoofdstuk wordt er een antwoord gegeven op de onderzoeksvraag en de bijbehorende subvragen door betekenis te geven aan de resultaten. Vervolgens komen de beperkingen van het onderzoek aan bod en worden er aanbevelingen voor vervolgonderzoek gegeven.

5.1. Conclusie & discussie

De onderzoeksvraag die centraal stond in dit onderzoek was: in hoeverre reikt het privacybewustzijn, bestaande uit de perceptie, aandacht en kennis wat betreft online privacy-kwesties, onder Nederlandse jongeren vanaf 16 tot en met 29 jaar die gebruikmaken van sociale media? Om deze onderzoeksvraag en bijhorende subvragen te beantwoorden is er een kwantitatieve onderzoeksmethode gebruikt met een online enquête als dataverzamelingsmethode. Via een sneeuwbalsteekproef zijn uiteindelijk 260 respondenten verzameld.

5.1.1. Discussie privacybewustzijn

Aan de hand van drie meervoudige lineaire regressie analyses is onderzocht of leeftijd, opleidingsniveau, actief sociale mediagebruik en geslacht als controle variabele van invloed waren op het privacybewustzijn bestaande uit drie onderdelen, namelijk; bezorgde privacyperceptie, privacy-aandacht in de vorm van privacymaatregelen en privacykennis in de vorm van een quizscore. Uit de drie meervoudige regressies kwam naar voren dat geslacht als controle variabele alleen van invloed bleek te zijn op privacykennis. De vrouwelijke respondenten scoorden iets lager op de quizvragen dan de mannelijke respondenten. Mogelijke verklaringen hiervoor kunnen een verschil in interesses of soort opleiding zijn. Mannen zijn wellicht meer geïnteresseerd in technische onderwerpen en doen wellicht meer ICT-opleidingen dan vrouwen.

Uit de drie meervoudige regressies kwam naar voren dat leeftijd niet van invloed was op bezorgde privacyperceptie ($H_{1.1}$), privacy-aandacht ($H_{1.2}$) en privacykennis ($H_{1.3}$). De resultaten wat betreft de invloed van leeftijd op bezorgde privacyperceptie en privacy-aandacht kwamen daarmee niet overeen met voorgaande theorie, waarin naar voren kwam dat leeftijd hier wel van invloed op was (TNO, 2015). Een mogelijke verklaring hiervoor kan zijn dat vergeleken met het onderzoek van TNO (2015), waarin de leeftijdsspanne tussen de 18 en 74 jaar was, de leeftijdsspanne in dit onderzoek te klein was, waarmee de steekproef qua leeftijd te homogeen was en er daardoor geen significant verschil kon worden gevonden.

Uit de drie meervoudige regressies kwam naar voren dat het opleidingsniveau niet van invloed was op privacy-aandacht ($H_{2.2}$) en privacykennis ($H_{2.3}$), maar wel deels op bezorgde privacyperceptie ($H_{2.1}$). Er bleek geen significant verschil te zijn tussen respondenten met wo als opleidingsniveau en respondenten die binnen de lagere opleidingsniveaus vielen, maar wel tussen respondenten met hbo als opleidingsniveau en respondenten met een lager opleidingsniveau. Respondenten met hbo als

opleidingsniveau uitten een iets hogere mate van bezorgdheid en hadden daarmee een iets negatievere perceptie over online privacy dan respondenten met een lager opleidingsniveau. In vorig onderzoek was er geen significant verschil tussen hoger en lager opgeleiden (TNO, 2015). Het is daarom opvallend dat er geen significant verschil was tussen de respondenten met wo als opleidingsniveau en de lagere opleidingsniveaus, maar wel een significant verschil tussen de respondenten met hbo als opleidingsniveau en de lagere opleidingsniveaus. Mogelijke verklaringen hiervoor kunnen het praktische verschil tussen hbo en wo zijn of het soort hbo-opleiding, zoals een ICT-opleiding, die is gedaan waarmee er meer (praktische) kennis is opgedaan over online privacy en de negatieve kant van het internet en sociale media.

Uit de drie meervoudige regressies kwam naar voren dat het actieve sociale mediagebruik niet van invloed was op privacy-aandacht ($H_{3.2}$) en privacykennis ($H_{3.3}$), maar wel op bezorgde privacyperceptie ($H_{3.1}$). In vorig onderzoek kwam naar voren dat de respondenten die geen gebruik maken van sociale media een hogere mate aan zorgen uitdrukken over privacy dan de respondenten die wel gebruikmaken van sociale media (Tufekci, 2008). Dit onderzoek heeft hieraan bijgedragen door aan te tonen dat er ook een verschil is in het uitdrukken van bezorgdheden over online privacy tussen sociale mediagebruikers die op actievere wijze en minder actieve wijze van sociale media gebruikmaken. Respondenten die op actievere wijze gebruikmaken van sociale media uitten een iets minder hoge mate van bezorgdheid en hadden daarmee een iets positievere perceptie over online privacy dan de respondenten die op minder actieve wijze van sociale media gebruikmaken.

5.1.2. Discussie privacy paradox

Uit de descriptieve resultaten kwam naar voren dat bijna alle onderzochte jongeren in dit onderzoek op actieve wijze gebruikmaken van sociale media, waarbij dus persoonlijke data wordt gedeeld wat door de desbetreffende sociale media en andere partijen kan worden gebruikt om winst te maken en om gedrag te voorspellen, te sturen, te beïnvloeden en zelfs te bepalen (Baelden, 2013; Brunton & Nissenbaum, 2015; Martijn & Tokmetzis, 2016a; Oosterveer, 2016; Schermer, 2007; Van der Veer, 2016; Young & Quan-Haase 2013). Uit de descriptieve resultaten wat betreft bezorgde privacyperceptie kwam naar voren dat het merendeel van de respondenten op een subjectief niveau bezorgdheden uitten wat betreft online privacy. Dit betekent dat ook onder deze respondenten de privacy paradox aanwezig is, omdat zij ondanks hun bezorgdheid over online privacy toch op actieve wijze content delen op sociale media.

Dat de privacy paradox aanwezig is, was ook te zien aan de privacy-aandacht. Uit de descriptieve resultaten kwam namelijk naar voren dat het percentage van toegepaste maatregelen van het totale aantal maatregelen onder de 50 procent lag, terwijl alle maatregelen met vrij weinig moeite kunnen worden toegepast. Een mogelijke verklaring hiervoor kan onwetendheid zijn door gebrek aan informatie (Batist, 2015; Nissenbaum, 2011); wat inhoudt dat de respondenten niet afweten van deze maatregelen of deze te ingewikkeld vinden om toe te passen. Een andere mogelijke verklaring kan

laksheid zijn (Martijn & Tokmetzis, 2016a), wat inhoudt dat de respondenten denken dat deze maatregelen te veel moeite kosten.

Er is echter nuance noodzakelijk wat betreft de privacy paradox onder de respondenten. De privacy paradox houdt in dat mensen zich juist zorgen maken over hun (online) privacy en tegelijkertijd bereid zijn om persoonlijke gegevens te onthullen (TNO, 2015; Young & Quan-Haase, 2013). In dit onderzoek wordt de privacy paradox gedeeltelijk tegengesproken, omdat uit de derde meervoudige regressie naar voren kwam dat de respondenten die op actievere wijze gebruikmaken van sociale media, wat meer dan één keer per week content delen inhoudt en waarmee dus persoonlijke gegevens worden onthuld, zich juist (iets) minder zorgen maakten over online privacy dan respondenten die minder dan één keer per week content delen op sociale media.

5.1.3. Discussie privacykennis

De maatschappelijke relevantie in dit onderzoek is de conclusie aan de hand van de descriptieve resultaten wat betreft privacykennis dat de respondenten kennis misten over bepaalde onderwerpen. Voorbeelden uit de resultaten hiervan zijn het wel of niet krijgen van een melding op Snapchat wanneer er een screenshot wordt gemaakt en hoe een onbeveiligde websiteverbinding kan worden herkend. Er kon dus worden gesteld dat voor bepaalde onderwerpen de gepercipieerde privacy afweek van de werkelijke privacy (Batist, 2015). Ook wanneer er werd gekeken naar de gemiddelde score van 6.5, kon worden gesteld dat de privacykennis nog wel degelijk verhoogd mag en moet worden. Het is namelijk wenselijk om zoveel mogelijk kennis over online privacy-kwesties te hebben, zodat er op kritische en bewuste wijze kan worden omgegaan met het delen van (persoonlijke) gegevens op het internet en sociale media.

Ook bleek dat het gebrek aan privacykennis onder de respondenten niet sociaal is gestructureerd, omdat in de meervoudige lineaire regressie wat betreft privacykennis naar voren kwam dat leeftijd en opleidingsniveau hier niet van invloed op waren. Een mogelijke verklaring voor het gebrek aan privacykennis kan de nieuwe *digital devide* zijn; de kloof tussen de mensen die op een hoog niveau digitaal geletterd zijn, zoals experts en programmeurs, en via geavanceerde dataveillance-technologie toegang hebben tot andermans data, tegenover de mensen wiens data verzameld en gebruikt wordt (Schermer, 2007). Er kan dan worden gesteld dat ook de jongeren in dit onderzoek digitale geletterdheid missen, ondanks dat zij vallen onder de begrippen *technoholics* en *digital natives* (Siapera, 2012; Sitompoel, 2015).

5.1.4. Discussie bewuste actie

In dit onderzoek was getracht meer bewustzijn te creëren onder de respondenten door informatie te verschaffen met betrekking tot de quizvragen in de hoop dat zij bewuster om zouden gaan met hun persoonlijke data. Er is dan ook onderzocht of de respondenten van plan waren bewuste actie te

ondernemen om de eigen online privacy beter te beschermen. De descriptieve resultaten wat betreft bewuste actie toonde aan dat meer dan de helft van de respondenten er bewust over nadacht om de online privacy beter te beschermen.

Aan de hand van een binaire logistieke regressie was onderzocht of privacykennis (H_4) en de controle variabelen geslacht, leeftijd en opleidingsniveau van invloed waren op het van plan zijn bewuste actie te ondernemen om de eigen online privacy beter te beschermen. Uit de logistieke regressie kwam naar voren dat opleidingsniveau en geslacht als controle variabelen geen significant effect hadden op bewuste actie, maar dat leeftijd wel een laag significant effect had op bewuste actie. Hoe ouder de respondent was, hoe lager de kans dat hij of zij van plan was bewuste actie te ondernemen en hoe jonger de respondent was, hoe hoger de kans dat hij of zij van plan was bewuste actie te ondernemen. Ook privacykennis had een laag significant effect op het wel of niet van plan zijn bewust actie uit te voeren om de online privacy beter te beschermen. Hoe hoger de (initiële) privacykennis was, hoe lager de kans dat de respondent van plan was bewuste actie te ondernemen en hoe lager de (initiële) privacykennis was, hoe hoger de kans dat de respondent van plan was bewuste actie te ondernemen. Er kan worden gesteld dat hoe lager de initiële privacykennis was, hoe meer de respondent wellicht heeft geleerd van de informatie die werd gegeven na elke quizvraag, waardoor de gepercipieerde privacy meer overeenkomt met de daadwerkelijke privacy.

Kortom, meer dan de helft van de respondenten heeft er dus bewust over nagedacht om de online privacy beter te beschermen en de gepercipieerde privacy komt meer overeen met de daadwerkelijke privacy, doordat de respondent wellicht heeft geleerd van de informatie die werd gegeven na elke quizvraag. Hiermee kan er worden geconcludeerd dat het doel van het onderzoek – om reflectie, kennis en een kritischer bewustzijn over online privacy bij de respondenten bij te brengen in de hoop dat zij zelf actie zullen ondernemen door bewuster om te gaan met het delen van persoonlijke gegevens op het internet en sociale media – redelijk is geslaagd (Reason & Bradbury, 2007).

5.2. Beperkingen & aanbevelingen

Er zijn verschillende beperkingen aan dit onderzoek op te merken. De data was afkomstig van een niet-willekeurige steekproef wat de generaliseerbaarheid van de resultaten sterk beperkt. De niet-willekeurige steekproefstrategie die is gebruikt, namelijk de sneeuwbalsteekproef, heeft als nadeel dat het eerste contact maken vaak moeilijk is. Voor dit onderzoek bleek het lastig om *entrypoints* te vinden, die verscheidenheid verschaften in leeftijd, opleidingsniveau en geslacht en tevens bereid waren de enquête te verspreiden. Een nadeel dat hieraan gekoppeld is, is dat er homogeniteit kan ontstaan, omdat de *entrypoints* bepalend zijn voor wat voor soort respondenten er worden bereikt en zij hoogstwaarschijnlijk alleen andere potentiële respondenten bereiken met dezelfde karakteristieken als zijzelf. In dit onderzoek was hierdoor het aantal respondenten met het vrouwelijke geslacht, het aantal respondenten met een wo-opleiding en het aantal respondenten met de leeftijd van 16 en 23

oververtegenwoordigd en het aantal respondenten met een mbo of middelbare school opleiding ondervertegenwoordigd. Ook de vrij kleine leeftijdsspanne vanaf 16 tot en met 29 jaar kan voor homogeniteit hebben gezorgd, omdat dit allemaal jongeren betreffen waarvan dan kan worden verwacht dat zij gelijksoortige antwoorden geven. Deze homogeniteit kan van invloed zijn geweest op de niet significante resultaten wat betreft leeftijd.

Ondanks dat kwam uit de theorie naar voren dat het vooral jongeren zijn die gebruikmaken van sociale media (Oosterveer, 2016; Van der Veer, 2016). Daarom was het een logische keuze om het onderzoek alleen op deze leeftijdsgroep te richten. Het voordeel dat hieraan gekoppeld is, is dat jongeren makkelijker kunnen worden bereikt met een online enquête in vergelijking met oudere leeftijdsgroepen. Desondanks is het voor vervolgonderzoek interessant om een grotere leeftijdsspanne te analyseren om te onderzoeken hoe ook volwassenen omgaan met online privacy en of er een significant verschil bestaat tussen volwassenen en jongeren. Volwassen worden namelijk niet als *digital natives* gezien, zoals jongeren, waardoor er andere resultaten voor hen kunnen worden verwacht. Tevens is het ook interessant om te onderzoeken hoe volwassenen informatie zouden willen verkrijgen om hun privacybewustzijn te verhogen sinds de meeste volwassenen geen onderwijs meer volgen. Daarnaast is het ook wenselijk om in vervolgonderzoek betere middelen te zoeken, zoals meer tijd en geld, om een grotere verscheidenheid te verkrijgen onder de respondenten qua geslacht, leeftijd en opleidingsniveau.

Ook de enquête zelf had beperkingen. De zes stellingen wat betreft privacyperceptie kwamen uit verschillende onderzoeken wat ervoor kan zorgen dat deze stellingen niet valide genoeg zijn om eenzelfde concept te meten, wat ook naar voren kwam aan de hand van de factor- en betrouwbaarheidsanalyse. De stellingen hadden meer van tevoren kunnen worden getest om ervoor te zorgen dat de stellingen meten wat ze zouden moeten meten. Wat betreft de quizvragen waren deze zo opgesteld dat er ongeveer evenveel vragen met ‘juist’ als met ‘onjuist’ beantwoord moesten worden. Maar bijna alle vragen betroffen negatieve aspecten wat betreft online privacy op het internet en sociale media, waardoor sommige quizvragen makkelijker konden worden geraden en daarmee de uiteindelijke quizscores vrij hoog uitvielen. In vervolgonderzoek zouden er meer quizvragen kunnen worden toegevoegd die ook positieve aspecten aankaarten wat betreft online privacy om tevens als strikvraag te kunnen fungeren.

Er bleken ook beperkingen te zijn wat betreft de uitkomsten van de vier regressie analyses. Voor alle vier de regressies bleek de hoeveelheid variantie in de afhankelijke variabele, die kan worden verklaard aan de hand van de onafhankelijke variabelen, laag te zijn. Dit betekent dat het regressiemodel een lage voorspellende kracht had en dat er nog andere factoren waren die verantwoordelijk konden zijn voor de variantie in de afhankelijke variabele. Ook kwam er in de resultaten wat betreft bezorgde privacyperceptie naar voren dat de hbo-ers wel een significant hogere mate aan zorgen uitdrukten vergeleken met de lagere opleidingsniveaus en de wo-ers niet. Een mogelijke verklaring die hiervoor is gegeven was dat dit zou kunnen komen door de soort hbo-

opleiding die er gedaan is of door de meer praktische kant van hbo-opleidingen in vergelijking tot wo-opleidingen. In vervolgonderzoek zouden andere onafhankelijke variabelen kunnen worden gebruikt, zoals beroep, leefomgeving en studierichting. Daarnaast kwam in de resultaten wat betreft bezorgde privacyperceptie naar voren dat de respondenten die op actievere wijze gebruikmaken van sociale media een significant lagere mate aan zorgen uitdrukten dan de respondenten die op minder actieve wijze van sociale media gebruikmaken. De reden hier achter is interessant om in vervolgonderzoek te onderzoeken, door middel van bijvoorbeeld interviews tussen beide groepen. Wat tevens opviel was dat de vrouwelijke respondenten significant lager op de quiz scoorden dan de mannelijke respondenten. Een mogelijke verklaring die hiervoor is gegeven was dat dit zou kunnen komen door een verschil in interesses of soort opleiding. In vervolgonderzoek zou dit ook door middel van interviews verder kunnen worden verdiept om de achterliggende redenen hiervoor te kunnen achterhalen.

In dit onderzoek kwam naar voren dat het merendeel van de respondenten overwoog om actie te ondernemen om de online privacy meer te beschermen, maar dan moet de informatie hiervoor wel op een gemakkelijke wijze worden gegeven. Ook de conclusie dat kennis over online privacy niet sociaal gestructureerd is, betekent dat er kennis hierover moet worden onderwezen op elk opleidingsniveau. Het is dan ook van belang dat het verhogen van het privacybewustzijn op maatschappelijk vlak beter wordt opgepakt. Vooral jongeren moeten meer op de hoogte worden gesteld wat bedrijven en andere instituties met hun gegevens (kunnen) doen en wat voor gevolgen dit voor hen kan hebben, omdat zij de groep zijn die veel en op actieve wijze van sociale media gebruikmaken. Scholen op elk opleidingsniveau zouden meer aandacht moeten geven aan hoe jongeren tegelijkertijd op plezierige wijze gebruik kunnen maken van het internet en sociale media én op kritische en bewustere wijze hun (online) privacy in acht nemen, door het verbeteren van de kennis over online privacy en de vaardigheden om de online privacy te beschermen.

Literatuurlijst

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey: Brooks/Cole Publications.

Angwin, J., & Valentino-Devries, J. (2012, 17 februari). Google's iPhone tracking. *The Wall Street Journal.* Geraadpleegd van https://epic.org/privacy/ftc/google/wsj-google-iphone.pdf

AVROTROS. (2016a, 21 oktober). *De privacytest* [Televisie programma]. Geraadpleegd van http://www.npo.nl/de-privacytest/21-10-2016/AT_2068349

AVROTROS. (2016b, 15 oktober). *Hunted* [Televisie programma]. Geraadpleegd van http://www.funx.nl/news/omg/29634-privacy-snapchat-is-minder-onschuldig-dan-je-denkt

Autoriteit Persoonsgegevens. (n.d.). Wat zijn persoonsgegevens? [Website]. Geraadpleegd op 2 mei 2017, van https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

Baelden, D. (2013). *Jongeren en sociale media: Input voor sensibiliseringsactie rond privacy geletterdheid* (Synthese Rapport D4.1.3a). Geraadpleegd van User Empowerment in a Social Media Culture website: http://emsoc.be/wp-content/uploads/2013/10/Sensibilisering-jongeren-en-sociale-media-D413a1.pdf

Barnes, B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). Geraadpleegd van http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312

Batist, K. (2015). *Beeldvorming van privacy in de digitale eeuw: Een onderzoek naar framing van online privacy in kranten en Facebook-discussies* (Masterthesis). Universiteit Leiden, Leiden. Geraadpleegd van https://openaccess.leidenuniv.nl/handle/1887/37625

Berger, F., Nici, E., & Blomdahl, J. (2016). *Do you trust strangers: A study on what impacts trust in the sharing economy* (Bachelorthesis). Linnaeus University, Växjö. Geraadpleegd van http://lnu.diva-portal.org/ smash/get/diva2:934608/FULLTEXT01.pdf

Blok, P. H. (2002). *Het recht op privacy: Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht.* Den Haag: Boom Juridische Uitgevers. Geraadpleegd van https://pure.uvt.nl/portal/files/ 495931/91967.pdf

Boeije, H. (2014). Hoofdstuk 2: De kwalitatieve onderzoeksopzet. In *Analyseren in kwalitatief onderzoek* (2e druk) (pp. 37-56). Den Haag: Boom Lemma.

Boyd, D. M. (2008). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Red.), *Youth, identity, and digital medias* (pp. 119-142). Cambridge, MA: MIT Press.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13,* 210-230. http://dx.doi.org/10.1111/ j.1083-6101.2007.00393.x

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A user's guide for privacy and protest.* Londen & Cambridge, MA: MIT Press.

CBS. (2016). *Internet; toegang, gebruik en faciliteiten* [Dataset]. Geraadpleegd van http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83429ned&D1=0,2-7,25-31,36-69&D2=0,36&D3=0&D4=a&HDR=T&STB=G1,G2,G3%20&VW=T

CBS. (2017). *Ondervonden delicten; persoonskenmerken* [Dataset]. Geraadpleegd van http://statline.cbs.nl/statweb/publication/?vw=t&dm=slnl&pa =83095ned&d1=0,5,29-32,37,40,45-46,51-52,69,81,99,104,114,124,135&d2=0&d3= 0&d4=a&hd=151216-0953&hdr=g1,g2,g3&stb=t

Centre for International Governance Innovation & IPSOS. (2016). 2016 CIGI-Ipsos global survey on internet security and trust [Opiniepeiling]. Geraadpleegd van https://www.cigionline.org/ internet-survey-2016

Citron, D. K., & Pasquale, F. A. (2014). The scored society: Due process for automated predictions. *Washington Law Review, 89*, 1-34. Geraadpleegd van https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209

Consumentenbond. (2016, 7 maart). Tinder claimt zeggenschap over jouw gegevens [Online actie]. Geraadpleegd van https://www.consumentenbond.nl/acties/privacy/tinder/

Consumentenbond. (n.d.). Wat zijn cookies? [Online artikel]. Geraadpleegd op 10 mei 2017, van https://www.consumentenbond.nl/internet-privacy/wat-zijn-cookies

Crain, C. (2013). Living in a society of control [Blog bericht]. Geraadpleegd van http://www.mantlethought.org/philosophy/living-society-control

Deleuze, G. (1992). Postscript on the societies of control. *October, 59*, 3-7. Geraadpleegd van https://cidadeinseguranca.files.wordpress.com/2012/02/deleuze_control.pdf

De mening van Nederland over het onderwijs. (2015). *Algemeen Dagblad*. Geraadpleegd van http://www.krant.nl/schoolonderzoek-resultaten/#?logo=ad

De Rijke, M., & Graus, D. (2016, 17 juni). Wij zijn racisten, daarom Google ook. *NRC-Handelsblad*. Geraadpleegd van https://www.nrc.nl/nieuws/2016/06/17/wij-zijn-racisten-daarom-google-ook-2726583-a1505954

De Vreede, J. (2015, 17 oktober). Enquête: Ouders willen meer vakken in het basisonderwijs. *Algemeen Dagblad*. Geraadpleegd van http://www.ad.nl/binnenland/enquete-ouders-willen-meer-vakken-in-het-basisonderwijs~a534683f/

Duhigg, C. (2012, 16 februari). How companies learn your secrets. *The New York Times Magazine.* Geraadpleegd van http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Eurobarometer. (2015). Data protection [Opiniepeiling]. Geraadpleegd van http://ec.europa.eu/justice_/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

Facebook. (2015, 30 januari). Verklaring van rechten en verantwoordelijkheden [Gebruikersvoorwaarden]. Geraadpleegd van https://www.facebook.com/legal/terms

Facebook. (2016a, juli). About Facebook IQ [Website]. Geraadpleegd van https://insights.fb.com/about/

Facebook. (2016b, 29 september). Gegevensbeleid [Website]. Geraadpleegd van https://www.facebook.com/about/privacy

Facebook. (n.d.). Doelgroepstatistieken [Website]. Geraadpleegd op 3 januari 2017, van https://www.facebook.com/ads/audience-insights/people?act=10202622661120871&age=18-&country=NL

Februari, M. (2016, 10 mei). Hoe we met slimme data de toekomst kwijtraken. *NRC-Handelsblad*. Geraadpleegd van https://www.nrc.nl/nieuws/2016/05/10/hoe-we-met-slimme-data-de-toekomst-kwijtraken-1616979-a241956

Foucault, M. (1979). *Discipline and punish.* Harmondsworth: Penguin.

Foucault, M. (1981). *The history of sexuality*. Harmondsworth: Penguin.

Fowler, G. A. (2012, 13 oktober). When the most personal secrets get outed on Facebook. *The Wall Street Journal.* Geraadpleegd van http://w3.salemstate.edu/~pglasser/When_the_Most_ Personal _Secrets_Get_Outed_on_Facebook_-_WSJ.pdf

Free Snowden: The Courage Foundation. (n.d.). Who is Edward Snowden? [Website]. Geraadpleegd op 1 maart 2017, van https://edwardsnowden.com/

Gane, N., & Beer, D. (2008). *New media: The key concepts*. Oxford & New York: Berg.

Gilbert, N. (2008). *Researching social life* (3e druk). Los Angeles, Londen, New Delhi, Singapore & Washington DC: Sage.

Grande, T. [Todd Grande]. (2015, 2 december). *Testing the assumption of independent errors with ZRESID, ZPRED, and Durbin-Watson using SPSS* [Online video]. Geraadpleegd van https://www.youtube.com/watch?v=Lyk_S9T-oCw

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622. http://dx.doi.org/10.1080/00071310020015280

Hargittai, E., & Walejko, G. (2008). The participation divide: Content creation and sharing in the digital age. *Information, Communication & Society, 11*(2), 239-256. http://dx.doi.org/10.1080/13691180801946150

Houthuijs, P. (2017, 13 mei). Is dit de digitale watersnoodramp die leidt tot een cyberdeltaplan? *NOS*. Geraadpleegd van http://nos.nl/artikel/2172981-is-dit-de-digitale-watersnoodramp-die-leidt-tot-een-cyberdeltaplan.html

Instagram. (2013, 19 januari). Privacybeleid [Website]. Geraadpleegd van https://help.instagram.com/155833707900388

Instagram. (2016, 15 december). 600 million and counting [Blog bericht]. Geraadpleegd van http://blog.instagram.com/post/154506585127/161215-600million

Instagram stoomt door naar half miljard gebruikers. (2016, 21 juni). *NOS*. Geraadpleegd van http://nos.nl/artikel/2112570-instagram-stoomt-door-naar-half-miljard-gebruikers.html

JijVandaag. (2016, 17 oktober). Jongeren vertrouwen Facebook en Google niet [Opiniepeiling]. Geraadpleegd van http://jij.eenvandaag.nl/uitslagen/69830/jongeren_vertrouwen_facebook_en_google_niet

Johnson, B. (2010, 11 januari). Privacy no longer a social norm, says Facebook founder. *The Guardian*. Geraadpleegd van https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Jongere. (n.d.). In *Van Dale's Online woordenboek*. Geraadpleegd van http://www.vandale.nl/opzoeken?pattern=jongeren&lang=nn

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *PNAS, 110*(15), 5802-5805. Geraadpleegd van http://www.pnas.org/content/110/15/5802.full.pdf

Laerd Statistics. (n.d.a). Binomial logistic regression: SPSS statistics [Website]. Geraadpleegd op 19 mei 2017, van https://statistics.laerd.com/premium/spss/blr/binomial-logistic-regression-in-spss.php

Laerd Statistics. (n.d.b). Multiple regression: SPSS statistics [Website]. Geraadpleegd op 19 mei 2017, van https://statistics.laerd.com/premium/spss/mr/multiple-regression-in-spss.php

Laerd Statistics. (n.d.c). Types of variable [Website]. Geraadpleegd op 19 mei 2017, van https://statistics.laerd.com/statistical-guides/types-of-variable.php

Leezenberg, M., & De Vries, G. H. (2012). Hoofdstuk 11.2A: Foucaults genealogie. In *Wetenschapsfilosofie voor geesteswetenschappen* (pp. 257-260). Amsterdam: Amsterdam University Press.

Levinson, M. (2010, 29 juni). Social networking ever more critical to job search success. *CIO*. Geraadpleegd van http://www.cio.com/article/2417135/careers-staffing/social-networking-ever-more-critical-to-job-search-success.html

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review, 7*(3), 3-14. http://dx.doi.org/10.1080/10714420490280152

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society, 10*(3), 393-411. http://dx.doi.org/10.1177/1461444808089415

Martijn, M., & Tokmetzis, D. (2016a). *Je hebt wél iets te verbergen: Over het levensbelang van privacy*. Zutphen: De Correspondent.

Martijn, M., & Tokmetzis, D. (2016b, 12 september). De digitale zelfverdedigingsgids: Bescherm jezelf op het web. *De Correspondent.* Geraadpleegd van https://decorrespondent.nl/5243/de-digitale-zelfverdedigingsgids-bescherm-jezelf-op-het-web/282193989-b5ee7af1

Matthews, B., & Ross, L. (2010). Chapter 3: Questionnaires. In *Research Methods* (pp. 200-217). Harlow, UK: Pearson Education.

Mayer-Schoenberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think.* Londen: John Murray Publishers.

Michiels, P. (2015, 4 maart). Onze menselijkheid staat op het spel. *De Morgen.* Geraadpleegd van https://hansschnitzler.files.wordpress.com/2015/02/de-morgen.pdf

Mijn Online Identiteit. (n.d.a). 10 tips voor veilig internetgebruik! [Website]. Geraadpleegd op 7 april 2017, van https://www.mijnonlineidentiteit.nl/veilig-internetten-tips/

Mijn Online Identiteit. (n.d.b). Instagram; 7 privacy instellingen die jij moet weten [Website]. Geraadpleegd op 7 april 2017, van https://www.mijnonlineidentiteit.nl/instagram-privacy-instellingen-handleiding/

Nissenbaum, H. (2011). A contextual approach to privacy online. *Dædalus, the Journal of the American Academy of Arts & Sciences, 140*(4), 32-48. Geraadpleegd van https://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf

NPO 3. (2016). Privacy [Website]. Geraadpleegd van http://www.npo.nl/npo3/privacy

NPO Radio 1 (Producent). (2016, 17 oktober). *Privacy* [Audio podcast]. Geraadpleegd van http://jij.eenvandaag.nl/uitslagen/69830/jongeren_vertrouwen_facebook_en_google_niet

NTR. (2016a, 17 oktober). Data en Privacy [Televisie serie aflevering]. In *De Universiteit van Nederland*. Geraadpleegd van http://www.npo.nl/de-universiteit-van-nederland/17-10-2016/VPWON_1265352

OECD. (2007). *Participative web: User-created content* (DSTI/ICCP/IE(2006)7/FINAL). Geraadpleegd van http://oecd.org/dataoecd/57/14/38393115.pdf

Oosterveer, D. (2016, 25 januari). Sociale media in Nederland 2016: WhatsApp overstijgt Facebook [Online artikel]. Geraadpleegd van http://www.marketingfacts.nl/berichten/social-media-in-nederland-2016-whatsapp-overstijgt-facebook

Ouders: Geef kinderen les in omgangsvormen en sociale media (2015, 17 oktober). *NOS*. Geraadpleegd van http://nos.nl/artikel/2063573-ouders-geef-kinderen-les-in-omgangsvormen-en-sociale-media.html

Pallant, J. (2007). Chapter 15: Factor analyse. In *SPSS survival manual* (pp. 179-199). Maidenhead: Open University Press.

Privacy-waakhonden waarschuwen WhatsApp. (2016, 28 oktober). *NOS*. Geraadpleegd van http://nos.nl/artikel/2140092-privacy-waakhonden-waarschuwen-whatsapp.html

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). Geraadpleegd van http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Reason, P., & Bradbury, H. (2007). *The handbook of action research: Participative inquiry & practise* (2e druk). Londen: Sage.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5e druk) (pp. 155-6). Essex: Pearson Education Limited.

Schermer, B. W. (2007). *Software agents, surveillance, and the right to privacy: A legislative framework for agent-enabled surveillance* (Proefschrift). Universiteit Leiden, Leiden. Geraadpleegd van https://openaccess.leidenuniv.nl/bitstream/handle/1887/11951/Thesis.pdf?sequence=1

Schinkel, W., & De Graaf, B. (2010, 31 december). Het recht op veiligheid schept een permanente noodtoestand. *NRC-Handelsblad.* Geraadpleegd van https://www.nrc.nl/nieuws/2010/12/31/het-recht-op-veiligheid-schept-een-permanente-noodtoestand-11984190-a501618

Schnitzler, H. (2013, 25 juli). Dataseksueel [Blog bericht]. Geraadpleegd van https://hansschnitzler.wordpress.com/2013/07/25/dataseksueel/

Schnitzler, H. (2014a, 10 april). Intieme technologie vernietigt publieke ruimte [Blog bericht]. Geraadpleegd van https://hansschnitzler.wordpress.com/2014/04/10/intieme-technologie-vernietigt-publieke-ruimte/

Schnitzler, H. (2014b, 16 oktober). Virtuele dialoog (ook in beeld) [Blog bericht]. Geraadpleegd van https://hansschnitzler.wordpress.com/2014/10/16/virtuele-dialoog-ook-in-audio/

Schnitzler, H. (2015a, 25 juni). Maskerade der eenduidigheid [Blog bericht]. Geraadpleegd van https://hansschnitzler.wordpress.com/2015/06/25/maskerade-der-eenduidigheid/

Schnitzler, H. (2015b, 19 november). Privacyrede [Blog bericht]. Geraadpleegd van https://hansschnitzler.wordpress.com/2015/11/19/privacyrede/

Sebag, G., & Bodoni, S. (2016). Facebook told to stop exploiting WhatsApp data during EU probe. *Bloomberg*. Geraadpleegd van https://www.bloomberg.com/news/articles/2016-10-28/facebook-told-to-stop-exploiting-whatsapp-data-during-eu-probe?cmpid=socialflow-twitter-business&utm_content=business&utm_campaign=socialflow-organic&utm_source=twitter&utm_medium=social

Siapera, E. (2012). *Understanding new media*. Londen: Sage.

Sitompoel, R. (2015). *Outlook special: Behavioural shifts in target audiences* [Publicatie]. Geraadpleegd van PricewaterhouseCoopers: http://www.pwc.nl/nl/publicaties/behavioural-shifts-in-target-audiences.html

Smaling, E. (2017, 16 februari). Hackers op de campus: Hoe veilig ben jij? *Erasmus Magazine.* Geraadpleegd van https://www.erasmusmagazine.nl/2017/02/16/hackers-op-de-campus-hoe-veilig-ben-jij/

Smeets, P. (2016, 16 december). Cijfers: Welke social media heeft de toekomst in Nederland? [Blog bericht]. Geraadpleegd van http://www.dutchcowboys.nl/socialmedia/cijfers-welke-social-media-heeft-de-toekomst-in-nederland

Snapchat heeft meer dagelijkse gebruikers dan Twitter. (2016, 2 juni). *NOS*. Geraadpleegd van http://nos.nl/artikel/2108761-snapchat-heeft-meer-dagelijkse-gebruikers-dan-twitter.html

Snap Inc. (2017, 10 januari). Privacybeleid [Website]. Geraadpleegd van https://www.snap.com/nl-NL/privacy/privacy-policy/

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53,* 1393-1462. Geraadpleegd van https://poseidon01.ssrn.com/delivery.php?ID=569083126081089019083001021114064069001048040012083025025003121122091127110065010093010036118001110127006072113018119016011001082008062059099083092024122004072057086002113098000114080115070123067125123065093100083083025069112083090107104064101092&EXT=pdf

Storey, J. (2012). Chapter 6: Structuralism and post-structuralism. In *Cultural theory and popular culture: An introduction* (6e druk) (pp. 113-136). Londen, New York, Tokyo & Madrid: Pearson.

TNO. (2015). *Privacy beleving op het internet in Nederland* [Rapport R10276]. Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2015/02/01/privacybeleving-op-het-internet-in-nederland

Trotter, D. (2012). Interpersonal surveillance on social media. *Canadian Journal of Communication, 37*(2), 319-332. Geraadpleegd van http://search.proquest.com.eur.idm.oclc.org/docview/1027767558?OpenUrlRefId=info:xri/sid:wcdiscovery&accountid=13598

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36. http://dx.doi.org/10.1177/0270467607311484

Turow, J., Hennesy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting american consumers and opening them up to exploitation* [Rapport]. Geraadpleegd van Annenberg School for Communication University of Pennsylvania: https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and

USC Libraries. (n.d.). Organizing your social sciences research paper: Quantitative methods [Online onderzoekgids]. Geraadpleegd op 26 januari 2017, van http://libguides.usc.edu/writingguide/quantitative

Valentino-Devries, J., & Singer-Vine, J. (2012, 7 december). They know what you're shopping for. *The Wall Street Journal.* Geraadpleegd van http://w3.salemstate.edu/~pglasser/They_Know_What_You_re_Shopping_For_-_WSJ.pdf

Valentino-Devries, J., Singer-Vine, J., & Soltani, A. (2012, 24 december). Websites vary prices, deals based on users' information. *The Wall Street Journal.* Geraadpleegd van https://msu.edu/~conlinmi/teaching/MBA814/WSJpricediscrimination.pdf

Van der Veer, N. (2016, 24 januari). Social media onderzoek 2016 [Online artikel]. Geraadpleegd van http://www.newcom.nl/socialmedia2016

Van der Velden, M., & El Emam, K. (2013). "Not all my friends need to know": A qualitative study of teenage patients, privacy, and social media. *J Am Med Inform Assoc, 20,* 16-24. http://dx.doi.org/10.1136/amiajnl-2012-000949

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197-208. Geraadpleegd van http://search.proquest.com.eur.idm.oclc.org/docview/1547988865?OpenUrlRefId=info:xri/sid:wcdiscovery&accountid=13598

Van Eeden, E. (2014). *Profitable growth in the digital age: Towards a MyMedia company* [Publicatie]. Geraadpleegd van PricewaterhouseCoopers: http://www.pwc.nl/nl/assets/documents/pwc-profitable-growth-digital-age.pdf

Van Lonkhuyzen, L. (2016, 27 april). Facebook ziet omzet weer flink groeien. *NRC-Handelsblad.* Geraadpleegd van https://www.nrc.nl/nieuws/2016/04/27/facebook-ziet-omzet-weer-flink-groeien-a1407613

Van Looveren, F. (2015). Internet, een enthousiast omhelsde dwingeland [Boekbespreking van *Het digitale proletariaat*]. Geraadpleegd van http://www.sintnorbertuskerk.be/sites/default/files/Het%20digitale%20proletariaat%20-%20Schnitzler.pdf

Waarschuwing voor grote internationale gijzelsoftware-campagne. (2017, 12 mei). *NOS*. Geraadpleegd van http://nos.nl/artikel/2172840-waarschuwing-voor-grote-internationale-gijzelsoftware-campagne.html

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16*(4), 479-500. http://dx.doi.org/10.1080/1369118X.2013.777757

Appendix A | Enquête

Hoe privacyproof ben jij?!

Beste dame/heer,

Graag nodig ik je uit om deel te nemen aan mijn afstudeeronderzoek over privacybewustzijn op het internet en verscheidene sociale media.

Deze vragenlijst is bedoeld voor personen vanaf 16 tot en met 29 jaar en het invullen ervan duurt ongeveer 5 à 10 minuten. Ik vraag je zo eerlijk mogelijk te antwoorden. De vragenlijst bevat ook een quiz met een eindscore, die je kennis over online privacy test en waar je ook wat van kan leren!

Er zijn geen risico's gebonden aan deelname van deze vragenlijst. Alle antwoorden worden anoniem verwerkt en individuele antwoorden worden niet gepubliceerd. De verkregen gegevens worden enkel gebruikt voor mijn afstudeeronderzoek. Je kunt elk moment stoppen door de pagina af te sluiten en later weer verder gaan.

Je deelname wordt zeer gewaardeerd en ik bedank je hier dan alvast voor!

Wanneer je vragen hebt, neem dan gerust contact met mij op via jessika.snel@student.eur.nl.

Met vriendelijke groet,

Jessika Snel

De volgende vragen gaan over algemene gegevens.
Selecteer het antwoord dat het meest voor jou van toepassing is.

Q1 Wat is je leeftijd?
Deze vragenlijst is alleen bedoeld voor personen vanaf 16 tot en met 29 jaar. Vul deze vragenlijst dus niet in wanneer je niet in deze leeftijdscategorie valt.
- ❍ 16 (1)
- ❍ 17 (2)
- ❍ 18 (3)
- ❍ 19 (4)
- ❍ 20 (5)
- ❍ 21 (6)
- ❍ 22 (7)
- ❍ 23 (8)
- ❍ 24 (9)
- ❍ 25 (10)
- ❍ 26 (11)
- ❍ 27 (12)
- ❍ 28 (13)
- ❍ 29 (14)

Q2 Wat is je geslacht?
- ❍ Man (1)
- ❍ Vrouw (2)

Q3 Wat is je hoogst afgeronde of huidige opleiding?
- ❍ Geen (1)
- ❍ Basisschool (2)
- ❍ Vmbo (3)
- ❍ Havo (4)
- ❍ Vwo (5)
- ❍ Mbo (6)
- ❍ Hbo (7)
- ❍ Wo (8)

Q4 Welk van onderstaande opties is voor jou van toepassing?
- ❍ Ik ben scholier/student (1)
- ❍ Ik ben werkende (2)
- ❍ Ik ben werkloos (3)
- ❍ Anders, namelijk: (4) _____

De volgende vragen gaan over sociale mediagebruik.
Met sociale mediagebruik wordt bedoeld het hebben van een account op een sociale netwerksite waarop sociaal contact kan worden onderhouden en waarop content, in de vorm van foto's, video's, comments et cetera, ook openbaar kan worden gedeeld. Berichtservices zoals WhatsApp worden niet als sociale media gezien.

Q5 Geef aan van welke sociale media je gebruikmaakt.
Meerdere antwoorden zijn mogelijk.
- ❑ Facebook (1)
- ❑ Instagram (2)
- ❑ Snapchat (4)
- ❑ Geen van bovenstaande (5)
- ❑ Ik maak geen gebruik van sociale media (6)

Condition: Ik maak geen gebruik van so... Is Selected. Skip To: Gepercipieerde privacy.

Q6 Van welk sociale medium maak je het meest gebruik op actieve wijze?
Met actieve wijze wordt bedoeld het zelf delen/posten van foto's, video's, statusupdates, comments, gevoel of locaties.
- ❍ Facebook (1)
- ❍ Instagram (2)
- ❍ Snapchat (3)
- ❍ Anders, namelijk: (4) _____
- ❍ Ik deel/post nooit iets op sociale media (5)

Voorwaarde: Ik deel/post nooit iets op ... is geselecteerd. Ga naar: Gepercipieerde privacy.

Q7 Hoe vaak deel/post je wel eens iets op jouw meest gebruikte sociale medium?
- ❍ 1 of meerdere keren per dag (1)
- ❍ Minder dan 1 keer per dag maar meer dan 1 keer per week (2)
- ❍ Minder dan 1 keer per week maar meer dan 1 keer per maand (3)
- ❍ Minder dan 1 keer per maand (4)

Q8 Geef aan in hoeverre je het eens of oneens bent met de volgende 6 stellingen.
Met persoonlijke gegevens wordt informatie bedoeld dat over jezelf gaat. Dat is feitelijke informatie, zoals je naam, geboortedatum en contactgegevens. Maar ook informatie zoals je geloof, interesses en content in de vorm van onder andere foto's, video's, comments, gevoel en locaties.

	Heel erg oneens (1)	Oneens (2)	Redelijk oneens (3)	Neutraal (4)	Redelijk eens (5)	Eens (6)	Heel erg eens (7)
Ik heb vertrouwen in hoe sociale media persoonlijke gegevens beschermen. (1)	❍	❍	❍	❍	❍	❍	❍
Sociale media, zoals Facebook, beschouw ik als privé omgevingen. (2)	❍	❍	❍	❍	❍	❍	❍
Ik maak sneller gebruik van een gratis online dienst in ruil voor persoonlijke gegevens dan een privacy vriendelijkere dienst waarvoor ik moet betalen. (3)	❍	❍	❍	❍	❍	❍	❍
Ik ben bang dat mijn persoonlijke gegevens voor ongewenste doeleinden worden gebruikt. (4)	❍	❍	❍	❍	❍	❍	❍
Ik vind het niet prettig wanneer ik persoonlijke gegevens moet geven aan online diensten om deze te kunnen gebruiken. (5)	❍	❍	❍	❍	❍	❍	❍
Ik heb het gevoel te worden gemonitord op het internet. (6)	❍	❍	❍	❍	❍	❍	❍

Q9 Geef aan welke opties voor jou van toepassing zijn.

Meerdere opties zijn mogelijk.

If Sociale media Facebook Is Selected

- ❑ Ik accepteer geen vriendschapsverzoeken van vreemden op Facebook (1)
- ❑ Ik gebruik wachtwoorden met speciale tekens en cijfers erin (2)
- ❑ Ik lees de privacyvoorwaarden van een online dienst voordat ik deze accepteer (3)

If Sociale media Facebook Is Selected

- ❑ Mijn Facebookberichten (statusupdates, foto's, video's, locatie, gevoel) staan ingesteld op 'alleen vrienden' (4)
- ❑ Ik verwijder en/of blokkeer cookies (5)

If Sociale media Snapchat Is Selected

- ❑ Ik maak geen gebruik van liveStories op Snapchat (6)
- ❑ Ik gebruik zoveel mogelijk verschillende wachtwoorden voor verschillende online diensten (7)

If Sociale media Facebook Is Selected

- ❑ Ik heb mijn e-mailadres op Facebook afgeschermd voor alleen mijzelf of alleen mijn vrienden (8)
- ❑ Mijn computer/laptop/telefoon is vergrendeld met een wachtwoord/pincode bij het opstarten (9)

If Sociale media Instagram Is Selected

- ❑ Mijn persoonlijke Instagram-profiel staat op privé (10)
- ❑ Voor al mijn apparaten installeer ik vrijwel altijd direct de beveiligingsupdates (11)

If Sociale media Facebook Is Selected

- ❑ Ik heb mijn mobiele telefoonnummer niet gedeeld met Facebook (12)
- ❑ Ik gebruik een firewall en/of virusscanner op mijn computer/laptop (13)
- ❑ De locatievoorziening op mijn telefoon staat compleet uit (14)

If Sociale media Snapchat Is Selected

- ❑ Ik stuur geen Snaps op Snapchat die niet voor iedereen zijn bedoeld om te zien (15)
- ❑ Ik laat mijn wachtwoorden niet door de browser onthouden (16)

Als Sociale media type Facebook is geselecteerd

- ❑ Ik ben geen lid van openbare groepen op Facebook (17)
- ❑ Ik internet niet op openbare wifi-hotspots of gebruik een VPN-dienst (18)

Er volgt nu een quiz met meerdere stellingen.
Geef aan of de stelling juist of onjuist is. Wanneer je twijfelt of het niet weet is dat niet erg en kun je dit aangeven via de optie 'Weet ik niet'. Aan het einde van de vragenlijst krijg je je eindscore.

Q10.1 Een website die begint met 'http://' is een website die gebruikmaakt van een onbeveiligde verbinding.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Http Onjuist is geselecteerd
Of Http Weet ik niet is geselecteerd

Deze stelling is juist.
'http' geeft een onbeveiligde verbinding aan en is daarmee kwetsbaar voor spionageaanvallen. Een webadres met een beveiligde verbinding begint met 'https' en is ook te herkennen aan het slot icoon voor het webadres. Let hier dus op wanneer je bijvoorbeeld bankgegevens verstuurt via een website.

Display This Question:
Als Http Juist is geselecteerd

Deze stelling is inderdaad juist.
'http' geeft een onbeveiligde verbinding aan en is daarmee kwetsbaar voor spionageaanvallen. Een webadres met een beveiligde verbinding begint met 'https' en is ook te herkennen aan het slot icoon voor het webadres. Let hier dus op wanneer je bijvoorbeeld bankgegevens verstuurt via een website.

Q10.2 Banken en verzekeringsmaatschappijen kunnen om je persoonlijke gegevens vragen per e-mail.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:

Als Banken en verzekeringsmaatschappijen kunnen om je persoonlijke gegevens vragen per e-mail. Juist is geselecteerd

Of Banken en verzekeringsmaatschappijen kunnen om je persoonlijke gegevens vragen per e-mail. Weet ik niet is geselecteerd

Deze stelling is onjuist.

Banken en verzekeringsmaatschappijen doen dit niet. Wanneer je toch een dergelijke mail krijgt is dit hoogstwaarschijnlijk een poging van een kwaadwillende om je inloggegevens te verkrijgen. Volg links in dergelijk mails dan ook nooit op.

Display This Question:

Als Banken en verzekeringsmaatschappijen kunnen om je persoonlijke gegevens vragen per e-mail. Onjuist is geselecteerd

Deze stelling is inderdaad onjuist.

Banken en verzekeringsmaatschappijen doen dit niet. Wanneer je toch een dergelijke mail krijgt is dit hoogstwaarschijnlijk een poging van een kwaadwillende om je inloggegevens te verkrijgen. Volg links in dergelijk mails dan ook nooit op.

Display This Question:
If Sociale media type Facebook Is Selected

Q10.3 Je bepaalt zelf wie er toegang heeft tot de inhoud en informatie op je Facebookprofiel.

- Juist (1)
- Onjuist (2)
- Weet ik niet (3)

Display This Question:
Als Facebook toegang Juist is geselecteerd
Of Facebook toegang Weet ik niet is geselecteerd

Deze stelling is onjuist.

In de privacyvoorwaarden van Facebook staat dat ze de inhoud en andere gegevens van hun gebruikers verzamelen en deze delen met verschillende partijen die zich moeten houden aan overeenkomsten. Maar wie die partijen precies zijn en wat die overeenkomsten inhouden staat er niet bij. Daarnaast kunnen anderen in wiens vriendenlijst je staat ook (ongewild) gegevens over je delen, zoals je contactgegevens, wanneer zij ingaan met bepaalde diensten, zoals spelletjes.

Display This Question:
Als Facebook toegang Onjuist is geselecteerd

Deze stelling is inderdaad onjuist.

In de privacyvoorwaarden van Facebook staat dat ze de inhoud en andere gegevens van hun gebruikers verzamelen en deze delen met verschillende partijen die zich moeten houden aan overeenkomsten. Maar wie die partijen precies zijn en wat die overeenkomsten inhouden staat er niet bij. Daarnaast kunnen anderen in wiens vriendenlijst je staat ook (ongewild) gegevens over je delen, zoals je contactgegevens, wanneer zij ingaan met bepaalde diensten, zoals spelletjes.

Q10.4 Wanneer je voor een apparaat dat gekoppeld is aan het internet, zoals een printer, het wachtwoord gebruikt dat de fabrikant meegeeft, is deze moeilijk te hacken.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Apparaat hacken Juist is geselecteerd
Of Apparaat hacken Weet ik niet is geselecteerd

Deze stelling is onjuist.

Hackers kunnen apparaten die gekoppeld zijn aan het internet, zoals printers, beveiligingscamera's, externe harde schijven en webcams opsporen. Wachtwoorden van de fabrikant zijn vaak bekend, omdat deze vaak voor een type product hetzelfde zijn. Hackers hoeven maar een paar van deze standaard wachtwoorden uit te proberen en kunnen vervolgens in je apparaat komen. Een standaard wachtwoord kan je vaak herkennen aan 'admin'.

Display This Question:
Als Apparaat hacken Onjuist is geselecteerd

Deze stelling is inderdaad onjuist.

Hackers kunnen apparaten die gekoppeld zijn aan het internet, zoals printers, beveiligingscamera's, externe harde schijven en webcams opsporen. Wachtwoorden van de fabrikant zijn vaak bekend, omdat deze vaak voor een type product hetzelfde zijn. Hackers hoeven maar een paar van deze standaard wachtwoorden uit te proberen en kunnen vervolgens in je apparaat komen. Een standaard wachtwoord kan je vaak herkennen aan 'admin'.

Q10.5 Sociale media kunnen geen bescherming van persoonlijke gegevens garanderen.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Sociale media bescherming Onjuist is geselecteerd
Of Sociale media bescherming Weet ik niet is geselecteerd

Deze stelling is juist.

Sociale media kunnen niet garanderen dat derde partijen, zoals externe apps, websites of diensten die aanwezig zijn op sociale media, op betrouwbare en veilige wijze omgaan met persoonlijke gegevens. Facebook en Snapchat verwijzen je daarbij door om het privacybeleid te lezen van de desbetreffende partij.

Display This Question:
Als Sociale media bescherming Juist is geselecteerd

Deze stelling is inderdaad juist.

Sociale media kunnen niet garanderen dat derde partijen, zoals externe apps, websites of diensten die aanwezig zijn op sociale media, op betrouwbare en veilige wijze omgaan met persoonlijke gegevens. Facebook en Snapchat verwijzen je daarbij door om het privacybeleid te lezen van de desbetreffende partij.

Q10.6 Wanneer je een openbaar wifi-netwerk wil gebruiken en er komen meerdere wifi-namen naar voren moet je altijd het wifi-netwerk nemen waarin de naam van de desbetreffende locatie wordt genoemd dan een wifi-netwerk met een naam bestaande uit willekeurige letters en cijfers.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Openbaar wifinetwerk Juist is geselecteerd
Of Openbaar wifinetwerk Weet ik niet is geselecteerd

Deze stelling is onjuist.

Veel openbare wifi-netwerken hebben een naam die bestaat uit willekeurige letters en cijfers. Maar voor mensen is een bekende naam een logischere keuze dan een willekeurige combinatie. Hackers maken hier gebruik van door een eigen netwerk beschikbaar te stellen met de naam van de desbetreffende locatie waar je als bezoeker vervolgens gebruik van maakt en daarmee wellicht gevoelige informatie prijsgeeft, zoals inlogcodes. Daarom kan je beter ook altijd voor de zekerheid om de naam van het wifi-netwerk vragen.

Display This Question:
Als Openbaar wifinetwerk Onjuist is geselecteerd

Deze stelling is inderdaad onjuist.

Veel openbare wifi-netwerken hebben een naam die bestaat uit willekeurige letters en cijfers. Maar voor mensen is een bekende naam een logischere keuze dan een willekeurige combinatie. Hackers maken hier gebruik van door een eigen netwerk beschikbaar te stellen met de naam van de desbetreffende locatie waar je als bezoeker vervolgens gebruik van maakt en daarmee wellicht gevoelige informatie prijsgeeft, zoals inlogcodes. Daarom kan je beter ook altijd voor de zekerheid om de naam van het wifi-netwerk vragen.

Q10.7 Cookies volgen je surfgedrag en informatie over je computer/laptop/smartphone om een persoonlijk dossier over jou op te bouwen.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Cookies Onjuist is geselecteerd
Of Cookies Weet ik niet is geselecteerd

Deze stelling is juist.

Cookies zorgen er niet alleen voor dat websites effectief werken, maar bouwen dus ook een persoonlijk dossier over jou op. Per website kunnen het aantal cookies tot in de tientallen oplopen. De verzamelde informatie wordt door adverteerders bijvoorbeeld gebruikt om effectievere advertenties naar je toe te sturen, maar ook door vele andere bedrijven met een vaak onduidelijk doel.

Display This Question:
Als Cookies Juist is geselecteerd

Deze stelling is inderdaad juist.

Cookies zorgen er niet alleen voor dat websites effectief werken, maar bouwen dus ook een persoonlijk dossier over jou op. Per website kunnen het aantal cookies tot in de tientallen oplopen. De verzamelde informatie wordt door adverteerders bijvoorbeeld gebruikt om effectievere advertenties naar je toe te sturen, maar ook door vele andere bedrijven met een vaak onduidelijk doel.

Display This Question:
Als Sociale media type Instagram is geselecteerd

Q10.8 Wanneer je Instagram-account op privé staat en je gebruikt hashtags kunnen alleen jouw eigen volgers die foto’s op de desbetreffende hashtag-pagina's zien.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Instagram hashtags Onjuist is geselecteerd
Of Instagram hashtags Weet ik niet is geselecteerd

Deze stelling is juist.

Privéfoto’s zijn niet zichtbaar voor een openbaar publiek, zelfs wanneer deze een hashtag hebben. Alleen je volgers kunnen deze foto's op de desbetreffende hashtag-pagina's zien.

Display This Question:
Als Instagram hashtags Juist is geselecteerd

Deze stelling is inderdaad juist.

Privéfoto’s zijn niet zichtbaar voor een openbaar publiek, zelfs wanneer deze een hashtag hebben. Alleen je volgers kunnen deze foto's op de desbetreffende hashtag-pagina's zien.

Display This Question:
If Sociale media type Snapchat Is Selected

Q10.9 Snapchat is privacy veiliger dan andere sociale media zoals Facebook of Instagram, omdat Snapchat je Snap maar enkele seconden laat zien en vervolgens weer verwijdert.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Snap verwijdert Juist is geselecteerd
Of Snap verwijdert Weet ik niet is geselecteerd

Deze stelling is onjuist.

Snaps worden tijdelijk opgeslagen in het bestandssysteem van telefoontoestellen, waarmee deze Snaps toch opgeslagen zouden kunnen worden. Daarnaast geeft Snapchat in zijn privacyvoorwaarden aan dat ze niet kunnen beloven dat Snaps binnen een bepaald tijdsbestek worden verwijderd van hun servers. Ook wanneer je een Snap aan LiveStories toevoegt bewaart Snapchat deze zo lang als dat voor hen nodig is en kan deze opnieuw worden uitgezonden door hun zakenpartners zonder dat je hierop aanspraak kan maken. Deel dus geen berichten waarvan je niet wil dat iemand anders deze opslaat of deelt.

Display This Question:
Als Snap verwijdert Onjuist is geselecteerd

Deze stelling is inderdaad onjuist.

Snaps worden tijdelijk opgeslagen in het bestandssysteem van telefoontoestellen, waarmee deze Snaps toch opgeslagen zouden kunnen worden. Daarnaast geeft Snapchat in zijn privacyvoorwaarden aan dat ze niet kunnen beloven dat Snaps binnen een bepaald tijdsbestek worden verwijderd van hun servers. Ook wanneer je een Snap aan LiveStories toevoegt bewaart Snapchat deze zo lang als dat voor hen nodig is en kan deze opnieuw worden uitgezonden door hun zakenpartners zonder dat je hierop aanspraak kan maken. Deel dus geen berichten waarvan je niet wil dat iemand anders deze opslaat of deelt.

Display This Question:
If Sociale media type Instagram Is Selected

Q10.10 Wanneer je Instagram-profiel op openbaar staat, is je profiel ook opgenomen in zoekmachines zoals Google en Bing.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Instagram openbaar Onjuist is geselecteerd
Of Instagram openbaar Weet ik niet is geselecteerd

Deze stelling is juist.

Wanneer je niet wil dat je Instagram-profiel gevonden kan worden in zoekmachines moet je deze op privé zetten.

Display This Question:
Als Instagram openbaar Juist is geselecteerd

Deze stelling is inderdaad juist.

Wanneer je niet wil dat je Instagram-profiel gevonden kan worden in zoekmachines moet je deze op privé zetten.

Display This Question:
If Sociale media type Snapchat Is Selected

Q10.11 Snapchat geeft altijd een melding wanneer en door wie er een screenshot is gemaakt van je Snap.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Snapchat screenshot Juist is geselecteerd
Of Snapchat screenshot Weet ik niet is geselecteerd

Deze stelling is onjuist.

Ondanks deze melding bestaan er apps die te downloaden zijn waarmee je screenshots kan maken zonder dat daar een melding voor wordt gegeven. Deel dus geen berichten waarvan je niet wil dat iemand anders deze opslaat of deelt.

Display This Question:
Als Snapchat screenshot Onjuist is geselecteerd

Deze stelling is inderdaad onjuist.

Ondanks deze melding bestaan er apps die te downloaden zijn waarmee je screenshots kan maken zonder dat daar een melding voor wordt gegeven. Deel dus geen berichten waarvan je niet wil dat iemand anders deze opslaat of deelt.

Display This Question:
If Sociale media type Facebook Is Selected

Q10.12 Wanneer je Facebook opzegt kan Facebook je niet meer volgen.

- ❍ Juist (1)
- ❍ Onjuist (2)
- ❍ Weet ik niet (3)

Display This Question:
Als Facebook opzeggen Juist is geselecteerd
Of Facebook opzeggen Weet ik niet is geselecteerd

Deze stelling is onjuist.

Meer dan 10 miljoen websites hebben een vind-ik-leuk-knop geïnstalleerd gelinkt naar Facebook, waardoor de bezoeker automatisch een cookie krijgt van Facebook waarmee hij of zij wordt gevolgd.

Display This Question:
Als Facebook opzeggen Onjuist is geselecteerd

Deze stelling is inderdaad onjuist.

Meer dan 10 miljoen websites hebben een vind-ik-leuk-knop geïnstalleerd gelinkt naar Facebook, waardoor de bezoeker automatisch een cookie krijgt van Facebook waarmee hij of zij wordt gevolgd.

Q11 Ben je van plan anders om te gaan met het delen van jouw persoonlijke gegevens na het invullen van deze vragenlijst?

- ❍ Ja (1)
- ❍ Misschien (2)
- ❍ Nee (3)

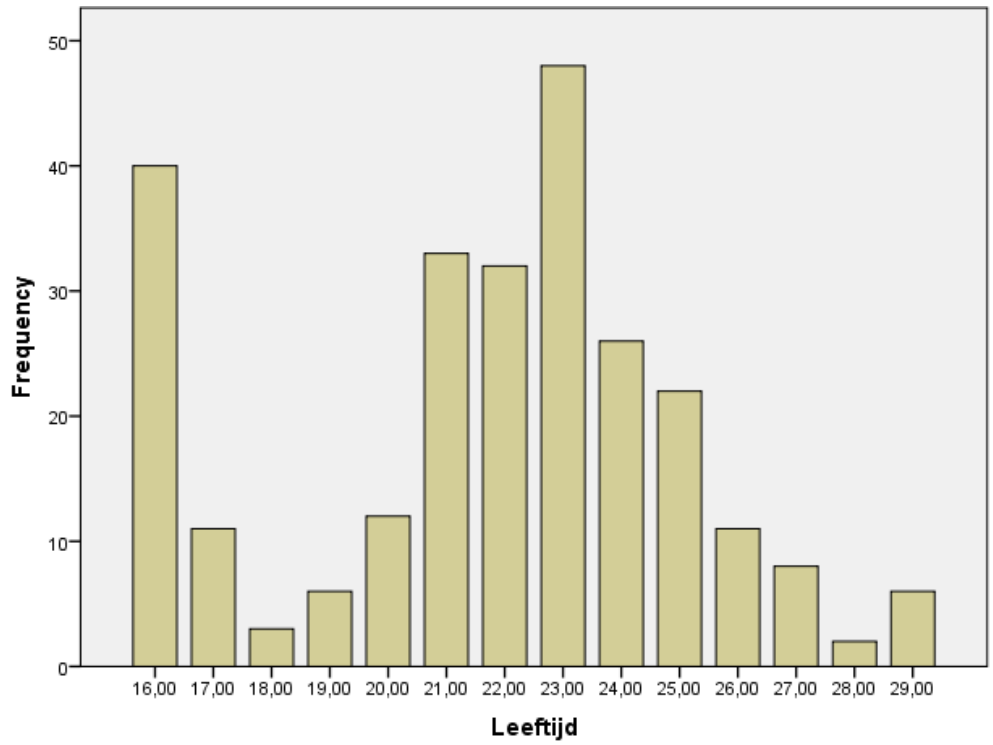
Q12 Heb je verder nog op of aanmerkingen?

Dit is het einde van de vragenlijst.
Nogmaals bedankt voor je tijd!

Hieronder staat je eindscore van de quiz.
Benieuwd hoe jouw vrienden hierop zouden scoren? Daag hen dan uit en deel deze vragenlijst met je vrienden door ze de volgende link te sturen:
https://erasmusuniversity.eu.qualtrics.com/jfe/form/SV_25JzD7CmJC9E4jb

Tip: Kijk ook op onderstaande website voor meerdere tips om jezelf beter te beschermen op het internet.
https://decorrespondent.nl/5243/de-digitale-zelfverdedigingsgids-bescherm-jezelf-op-het-web/282193989-b5ee7af1

Appendix B | Tabellen en figuren



Appendix B1.

Staafdiagram met de frequentie van alle leeftijden (*N* = 260)

Appendix B2.

Correlatiematrix*

		Item 1	Item 2	Item 3	Item 4	Item 5	Item 6
Correlatie	Item 1	**1.000**	**.323**	.104	**.304**	.198	.281
	Item 2	**.323**	**1.000**	.136	-.012	-.067	-.013
	Item 3	.104	.136	**1.000**	.135	.112	.071
	Item 4	**.304**	-.012	.135	**1.000**	**.570**	**.379**
	Item 5	.198	-.067	.112	**.570**	**1.000**	**.328**
	Item 6	.281	-.013	.071	**.379**	**.328**	**1.000**

*De correlatiematrix geeft de sterkte van de relaties weer tussen de variabelen (.3 - .5 = matige relatie, .5 - .8 = sterke relatie, .8 - .99 = zeer sterke relatie).

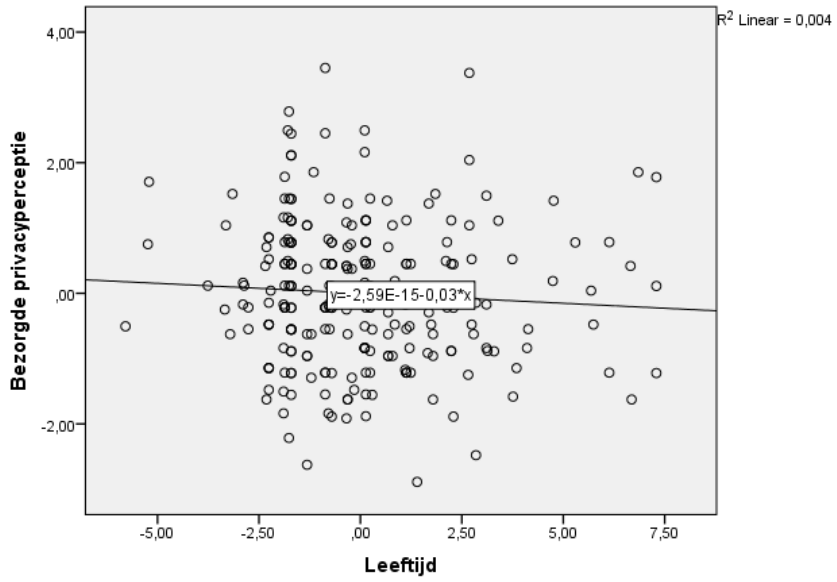
Let op: Correlatiecoëfficiënten met een waarde van .3 of hoger zijn dikgedrukt.

Appendix B3.

Factor- en betrouwbaarheidsanalyse voor schalen van bezorgde en vertrouwende privacypercepties (N = 260)

Item	*Bezorgde privacypercepties*		*Vertrouwende privacypercepties*	
	Pattern coëfficiënten	Structure coëfficiënten	Pattern coëfficiënten	Structure coëfficiënten
Ik heb vertrouwen in hoe sociale media persoonlijke gegevens beschermen.	.275	.406	**.676**	**.730**
Sociale media, zoals Facebook, beschouw ik als privé omgevingen.	-.298	-.129	**.874**	**.817**
Ik maak sneller gebruik van een gratis online dienst in ruil voor persoonlijke gegevens dan een privacy vriendelijkere dienst waarvoor ik moet betalen.	.091	.171	.414	.432
Ik ben bang dat mijn persoonlijke gegevens voor ongewenste doeleinden worden gebruikt.	**.826**	**.835**	.050	.209
Ik vind het niet prettig wanneer ik persoonlijke gegevens moet geven aan online diensten om deze te kunnen gebruiken.	**.826**	**.810**	-.086	.073
Ik heb het gevoel te worden gemonitord op het internet.	**.663**	**.677**	.074	.202
R^2	11.81		5.04	
Cronbach's α	.687		.488	
Eigenwaarde	2.11		1.27	

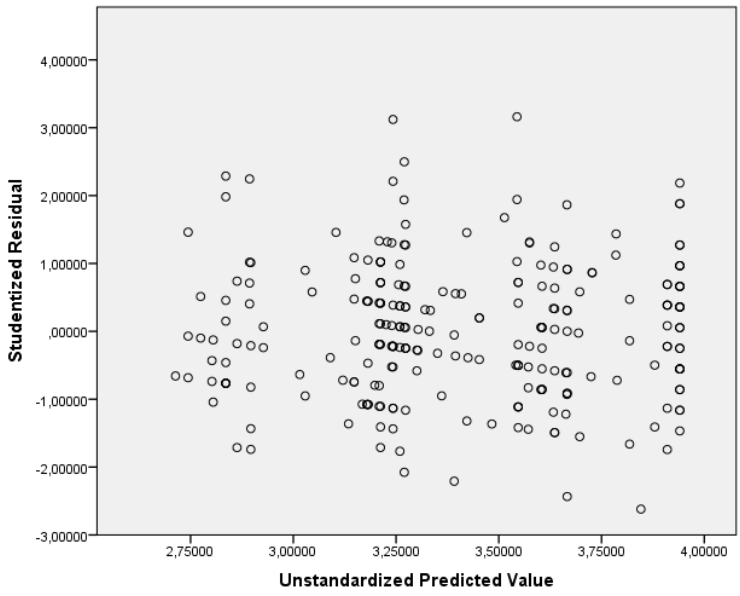
Let op: Factorladingen van .5 of hoger zijn dikgedrukt, omdat deze een sterke correlatie aangeven.



Appendix B4.

Partiële regressieplot om lineariteit aan te tonen tussen bezorgde privacyperceptie en leeftijd (*N* = 248*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.



Appendix B5.

Scatterplot om lineariteit aan te tonen tussen bezorgde privacyperceptie en onafhankelijke variabelen gezamenlijk en om homoscedasticiteit te controleren (*N* = 248*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.

Appendix B6.

Correlaties van meervoudige regressie analyse met bezorgde privacyperceptie als afhankelijke variabele om multicollineariteit te controleren (*N* = 248*)

		B. privacy perceptie	Leeftijd	Geslacht	Actief sociale mediagebruik	Hbo	Wo
Pearson's r	B. privacyperceptie	1.000	-.196	.051	.221	-.193	-.026
	Leeftijd	-.196	1.000	-.370	-.279	.236	.450
	Geslacht	.051	-.370	1.000	.165	-.021	-.143
	A. sociale mediagebruik	.221	-.279	.165	1.000	-.121	-.132
	Hbo	-.193	.236	-.021	-.121	1.000	-.495
	Wo	-.026	.450	-.143	-.132	-.495	1.000
Sig. (1-tailed)	B. privacyperceptie	.	.001	.214	.000	.001	.344
	Leeftijd	.001	.	.000	.000	.000	.000
	Geslacht	.214	.000	.	.005	.370	.012
	A. sociale mediagebruik	.000	.000	.005	.	.028	.019
	Hbo	.001	.000	.370	.028	.	.000
	Wo	.344	.000	.012	.019	.000	.

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.

Appendix B7.

Collineariteit voor bezorgde privacyperceptie, privacy-aandacht en privacykennis (*N* = 248*)

	Tolerantie	VIF
Leeftijd	.449	2.226
Geslacht	.842	1.187
Actief sociale mediagebruik	.908	1.101
Hbo	.479	2.087
Wo	.408	2.449

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.

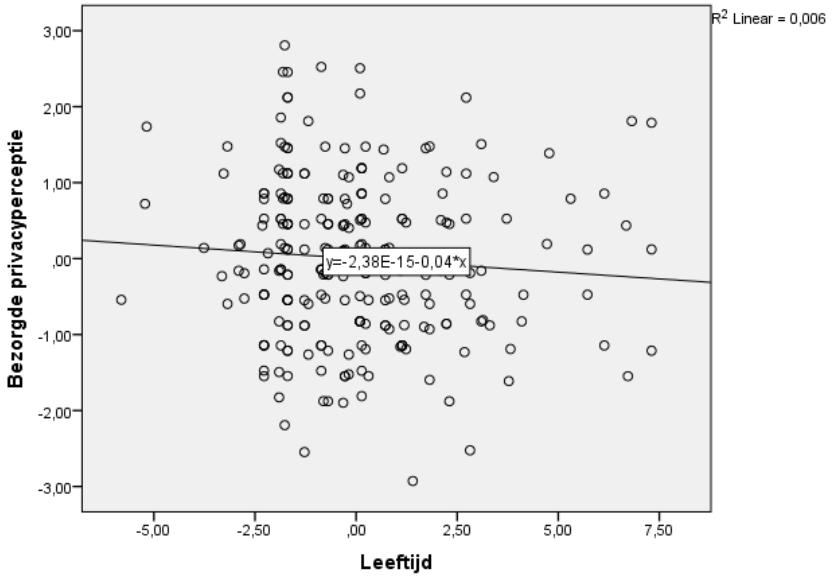
Let op: Tolerantiewaarden die kleiner zijn dan .1 of VIF-waarden die groter zijn dan 10 tonen collineariteit aan.

Appendix B8.

Casewise Diagnostics geeft significante uitschieters (Std. residu) aan voor bezorgde privacyperceptie (*N* = 248*)

Case nr.	Std. residu	B. Privacyperceptie	Voorspelde waarde	Residu
127	3.10	6.67	3.24	3.42
254	3.13	7.00	3.54	3.46

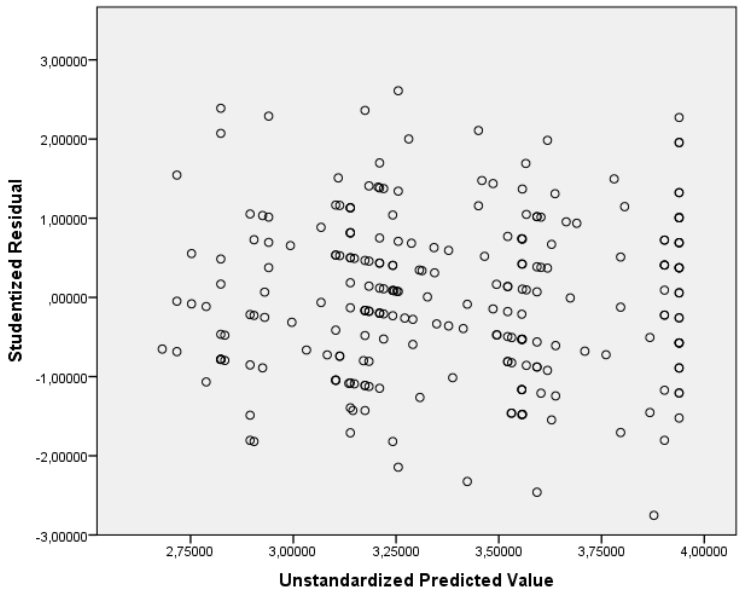
*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.



Appendix B9.

Partiële regressieplot om lineariteit aan te tonen tussen bezorgde privacyperceptie en leeftijd (*N* = 246*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieters.



Appendix B10.

Scatterplot om lineariteit aan te tonen tussen bezorgde privacyperceptie en onafhankelijke variabelen gezamenlijk en om homoscedasticiteit te controleren (*N* = 246*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieters.

Appendix B11.

Correlaties van meervoudige regressie analyse met bezorgde privacyperceptie als afhankelijke variabele om multicollineariteit te controleren (*N* = 246*)

		B. privacy perceptie	Leeftijd	Geslacht	Actief sociale mediagebruik	Hbo	Wo
Pearson's r	B. privacyperceptie	1.000	-.218	.037	.228	-.187	-.053
	Leeftijd	-.218	1.000	-.374	-.285	.239	.448
	Geslacht	.037	-.374	1.000	.166	-.019	-.149
	A. sociale mediagebruik	.228	-.285	.166	1.000	-.122	-.134
	Hbo	-.187	.239	-.019	-.122	1.000	-.493
	Wo	-.053	.448	-.149	-.134	-.493	1.000
Sig. (1-tailed)	B. privacyperceptie	.	.001	.281	.000	.002	.204
	Leeftijd	.001	.	.000	.000	.000	.000
	Geslacht	.281	.000	.	.005	.385	.010
	A. sociale mediagebruik	.000	.000	.005	.	.028	.018
	Hbo	.002	.000	.385	.028	.	.000
	Wo	.204	.000	.010	.018	.000	.

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieters.

Appendix B12.

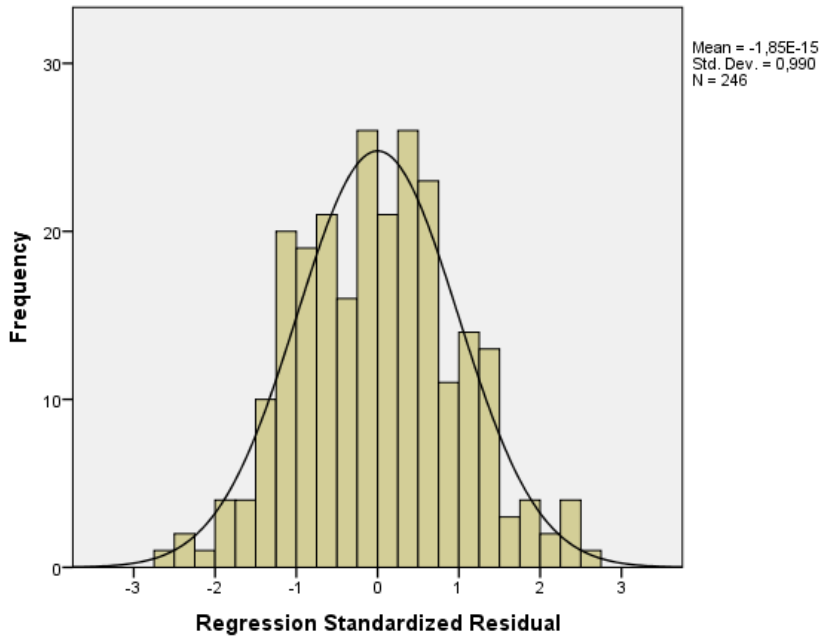
Collineariteit voor bezorgde privacyperceptie

(*N* = 246*)

	Tolerantie	VIF
Leeftijd	.448	2.231
Geslacht	.840	1.191
Actief sociale mediagebruik	.906	1.104
Hbo	.480	2.084
Wo	.411	2.435

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieters.

Let op: Tolerantiewaarden die kleiner zijn dan .1 of VIF-waarden die groter zijn dan 10 tonen collineariteit aan.

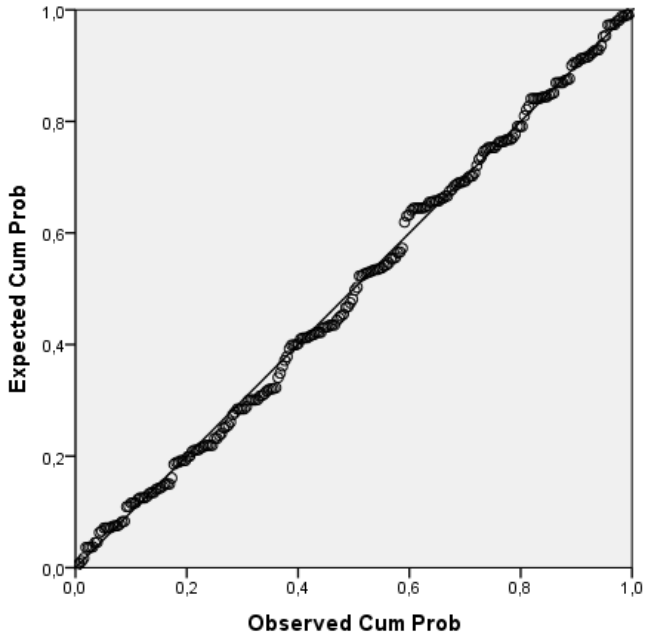


Appendix B13.

Histogram van de normale verdeling van bezorgde privacyperceptie

(*N* = 246*)

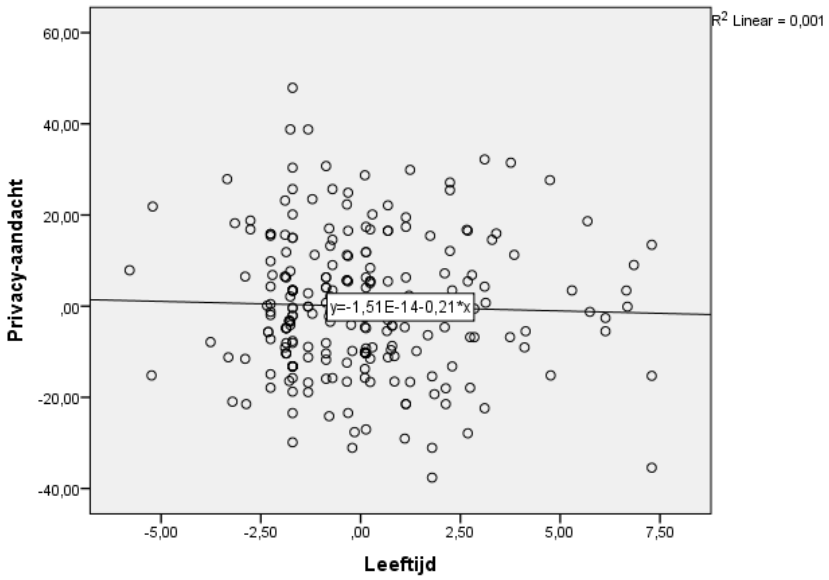
*Exlcusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieters.



Appendix B14.

P-P Plot om de normale verdeling van bezorgde privacyperceptie aan te tonen (*N* = 246*)

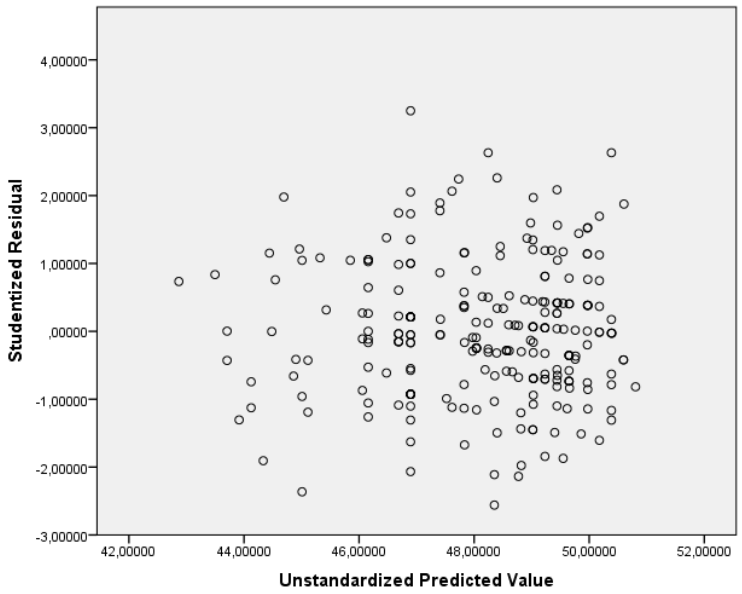
*Exlcusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieters.



Appendix B15.

Partiële regressieplot om lineariteit aan te tonen tussen privacy-aandacht en leeftijd (*N* = 248*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.



Appendix B16.

Scatterplot om lineariteit aan te tonen tussen privacy-aandacht en onafhankelijke variabelen gezamenlijk en om homoscedasticiteit te controleren (*N* = 248*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.

Appendix B17.

Correlaties van meervoudige regressie analyse met privacy-aandacht als afhankelijke variabele om multicollineariteit te controleren (*N* = 248*)

		Privacy-aandacht	Leeftijd	Geslacht	Actief sociale mediagebruik	Hbo	Wo
Pearson's r	Privacy-aandacht	1.000	.031	.027	.008	.029	.066
	Leeftijd	.031	1.000	-.370	-.279	.236	.450
	Geslacht	.027	-.370	1.000	.165	-.021	-.143
	A. sociale mediagebruik	.008	-.279	.165	1.000	-.121	-.132
	Hbo	.029	.236	-.021	-.121	1.000	-.495
	Wo	.066	.450	-.143	-.132	-.495	1.000
Sig. (1-tailed)	Privacy-aandacht	.	.312	.334	.448	.326	.152
	Leeftijd	.312	.	.000	.000	.000	.000
	Geslacht	.334	.000	.	.005	.370	.012
	A. sociale mediagebruik	.448	.000	.005	.	.028	.019
	Hbo	.326	.000	.370	.028	.	.000
	Wo	.152	.000	.012	.019	.000	.

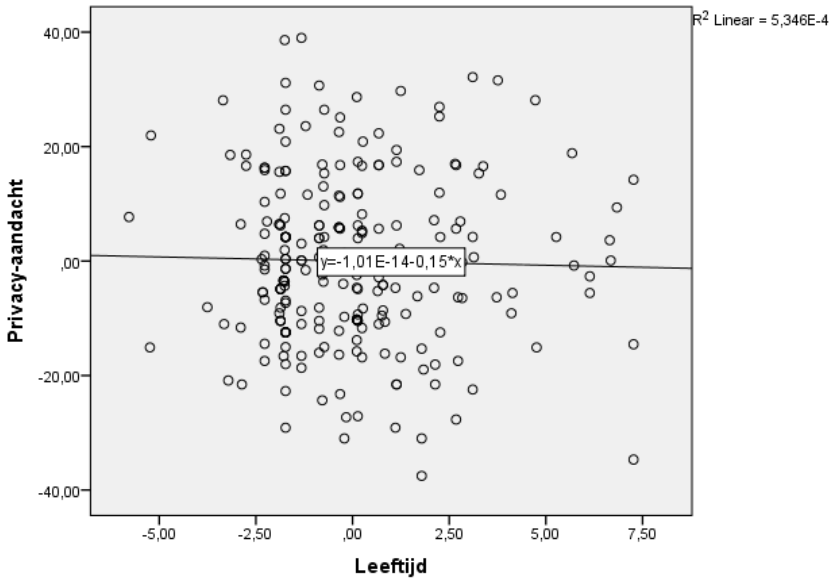
*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.

Appendix B18.

Casewise Diagnostics geeft significante uitschieters (Std. residu) aan voor privacy-aandacht (*N* = 248*)

Case nr.	Std. residu	Privacy-aandacht	Voorspelde waarde	Residu
35	3.22	94.44	46.90	47.55

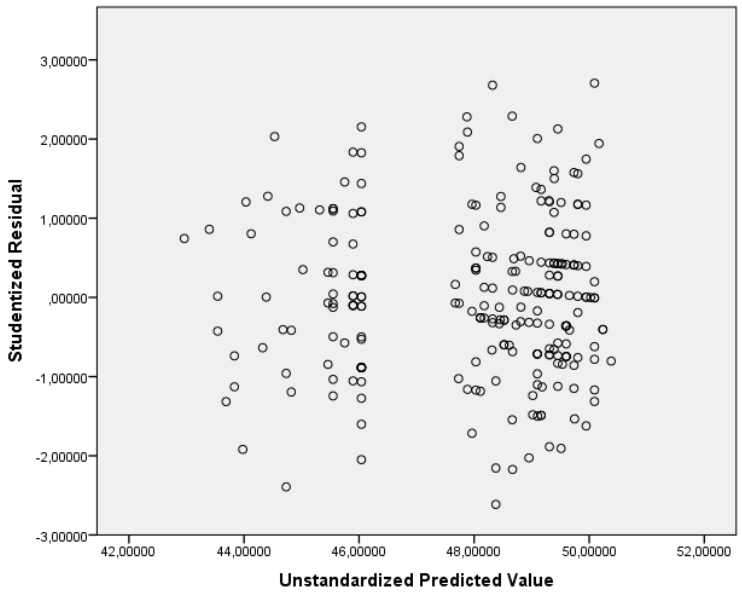
*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.



Appendix B19.

Partiële regressieplot om lineariteit aan te tonen tussen privacy-aandacht en leeftijd (*N* = 247*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.



Appendix B20.

Scatterplot om lineariteit aan te tonen tussen privacy-aandacht en onafhankelijke variabelen gezamenlijk en om homoscedasticiteit te controleren (*N* = 247*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.

Appendix B21.

Correlaties van meervoudige regressie analyse met privacy-aandacht als afhankelijke variabele om multicollineariteit te controleren (*N* = 247*)

		Privacy-aandacht	Leeftijd	Geslacht	Actief sociale mediagebruik	Hbo	Wo
Pearson's r	Privacy-aandacht	1.000	.054	.020	-.005	.036	.080
	Leeftijd	.054	1.000	-.368	-.274	.234	.446
	Geslacht	.020	-.368	1.000	.163	-.020	-.141
	A. sociale mediagebruik	-.005	-.274	.163	1.000	-.120	-.129
	Hbo	.036	.234	-.020	-.120	1.000	-.498
	Wo	.080	.446	-.141	-.129	-.498	1.000
Sig. (1-tailed)	Privacy-aandacht	.	.198	.378	.466	.286	.106
	Leeftijd	.198	.	.000	.000	.000	.000
	Geslacht	.378	.000	.	.005	.377	.014
	A. sociale mediagebruik	.466	.000	.005	.	.030	.022
	Hbo	.286	.000	.377	.030	.	.000
	Wo	.106	.000	.014	.022	.000	.

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.

Appendix B22.

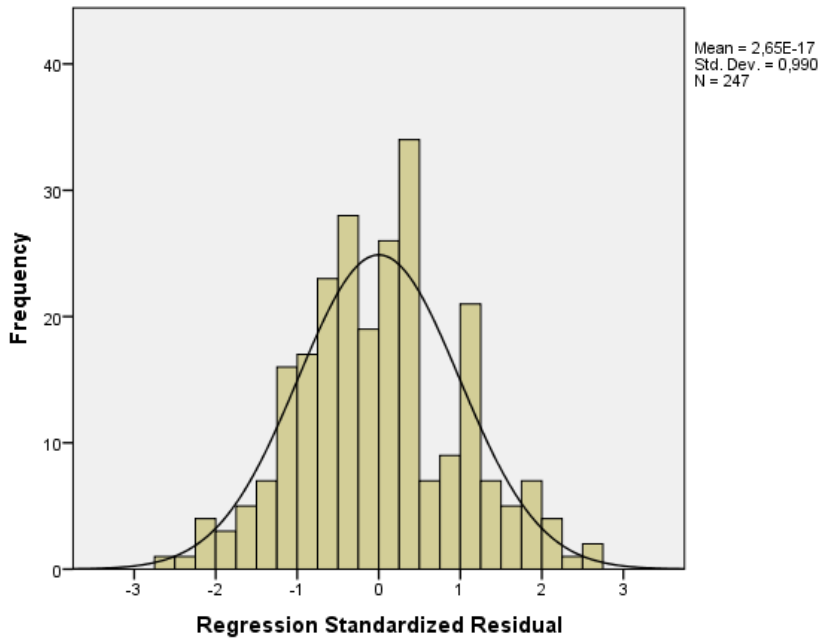
Collineariteit voor privacy-aandacht

(*N* = 247*)

	Tolerantie	VIF
Leeftijd	.453	2.206
Geslacht	.844	1.185
Actief sociale mediagebruik	.911	1.097
Hbo	.479	2.086
Wo	.410	2.441

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.

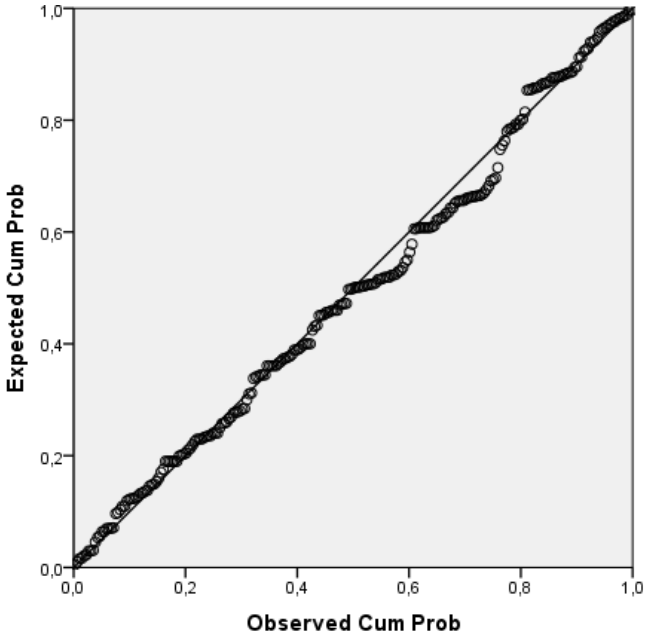
Let op: Tolerantiewaarden die kleiner zijn dan .1 of VIF-waarden die groter zijn dan 10 tonen collineariteit aan.



Appendix B23.

Histogram van de normale verdeling van privacy-aandacht (*N* = 247*)

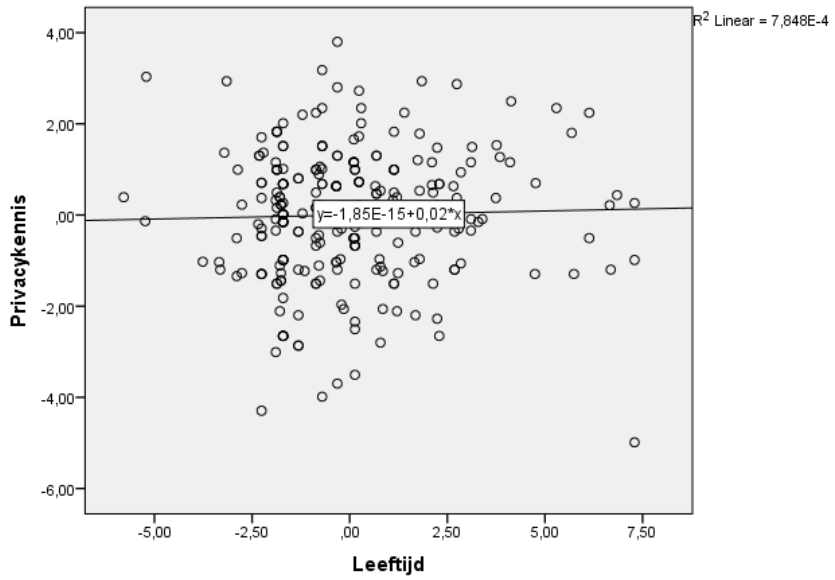
*Exlcusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.



Appendix B24.

P-P Plot om de normale verdeling van privacy-aandacht aan te tonen (*N* = 247*)

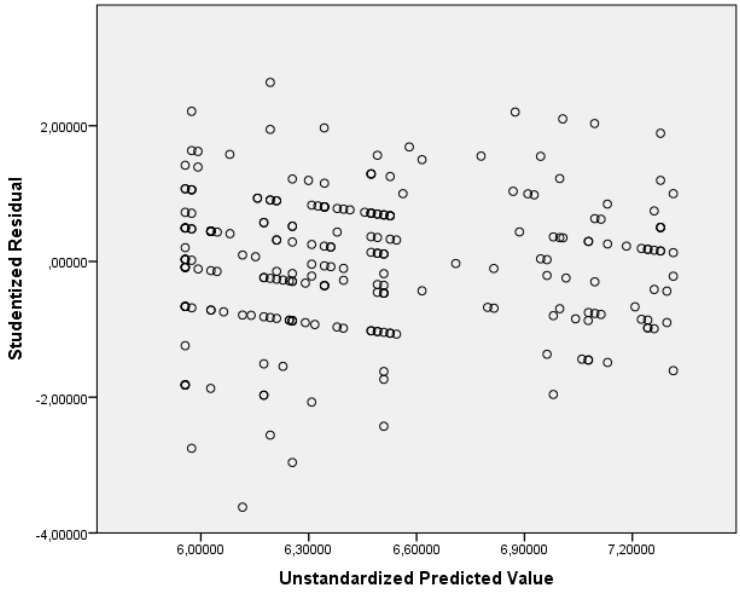
*Exlcusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.



Appendix B25.

Partiële regressieplot om lineariteit aan te tonen tussen privacykennis en leeftijd (*N* = 248*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.



Appendix B26.

Scatterplot om lineariteit aan te tonen tussen privacykennis en onafhankelijke variabelen gezamenlijk en om homoscedasticiteit te controleren (*N* = 248*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.

Appendix B27.

Correlaties van meervoudige regressie analyse met privacykennis als afhankelijke variabele om multicollineariteit te controleren (*N* = 248*)

		Privacy kennis	Leeftijd	Geslacht	Actief sociale mediagebruik	Hbo	Wo
Pearson's r	Privacykennis	1.000	.165	-.255	-.151	-.005	.110
	Leeftijd	.165	1.000	-.370	-.279	.236	.450
	Geslacht	-.255	-.370	1.000	.165	-.021	-.143
	A. sociale mediagebruik	-.151	-.279	.165	1.000	-.121	-.132
	Hbo	-.005	.236	-.021	-.121	1.000	-.495
	Wo	.110	.450	-.143	-.132	-.495	1.000
Sig. (1-tailed)	Privacykennis	.	.005	.000	.009	.470	.042
	Leeftijd	.005	.	.000	.000	.000	.000
	Geslacht	.000	.000	.	.005	.370	.012
	A. sociale mediagebruik	.009	.000	.005	.	.028	.019
	Hbo	.470	.000	.370	.028	.	.000
	Wo	.042	.000	.012	.019	.000	.

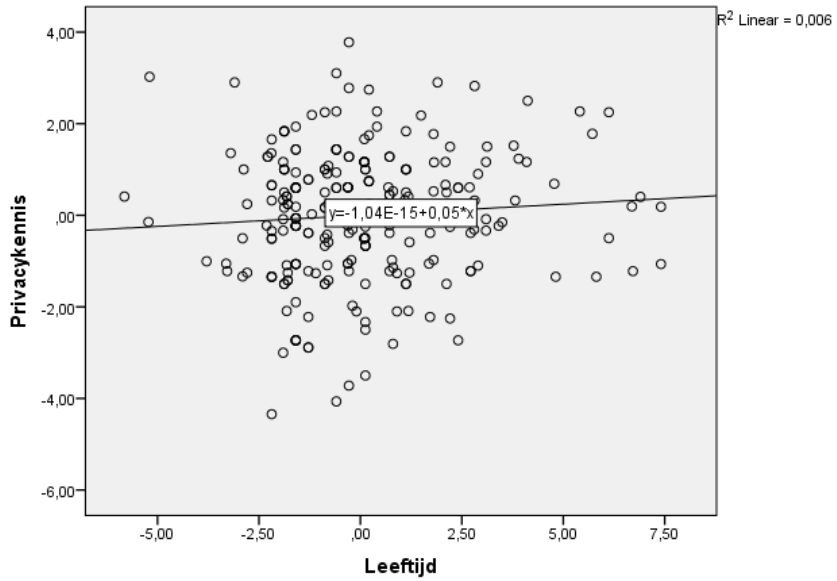
*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.

Appendix B28.

Casewise Diagnostics geeft significante uitschieters (Std. residu) aan voor privacykennis (*N* = 248*)

Case nr.	Std. residu	Privacykennis	Voorspelde waarde	Residu
122	-3.52	1.00	6.12	-5.12

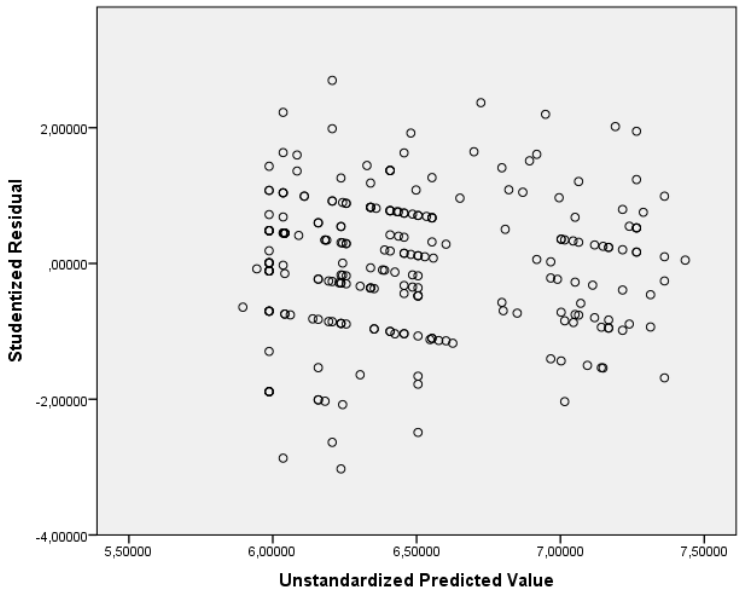
*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken.



Appendix B29.

Partiële regressieplot om lineariteit aan te tonen tussen privacykennis en leeftijd (*N* = 247*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.



Appendix B30.

Scatterplot om lineariteit aan te tonen tussen privacykennis en onafhankelijke variabelen gezamenlijk en om homoscedasticiteit te controleren (*N* = 247*)

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.

Appendix B31.

Correlaties van meervoudige regressie analyse met privacykennis als afhankelijke variabele om multicollineariteit te controleren (*N* = 247*)

		Privacy kennis	Leeftijd	Geslacht	Actief sociale mediagebruik	Hbo	Wo
Pearson's r	Privacykennis	1.000	.185	-.253	-.139	-.013	.099
	Leeftijd	.185	1.000	-.373	-.285	.238	.455
	Geslacht	-.253	-.373	1.000	.163	-.020	-.141
	A. sociale mediagebruik	-.139	-.285	.163	1.000	-.120	-.129
	Hbo	-.013	.238	-.020	-.120	1.000	-.498
	Wo	.099	.455	-.141	-.129	-.498	1.000
Sig. (1-tailed)	Privacykennis	.	.002	.000	.014	.421	.061
	Leeftijd	.002	.	.000	.000	.000	.000
	Geslacht	.000	.000	.	.005	.377	.014
	A. sociale mediagebruik	.014	.000	.005	.	.030	.022
	Hbo	.421	.000	.377	.030	.	.000
	Wo	.061	.000	.014	.022	.000	.

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.

Appendix B32.

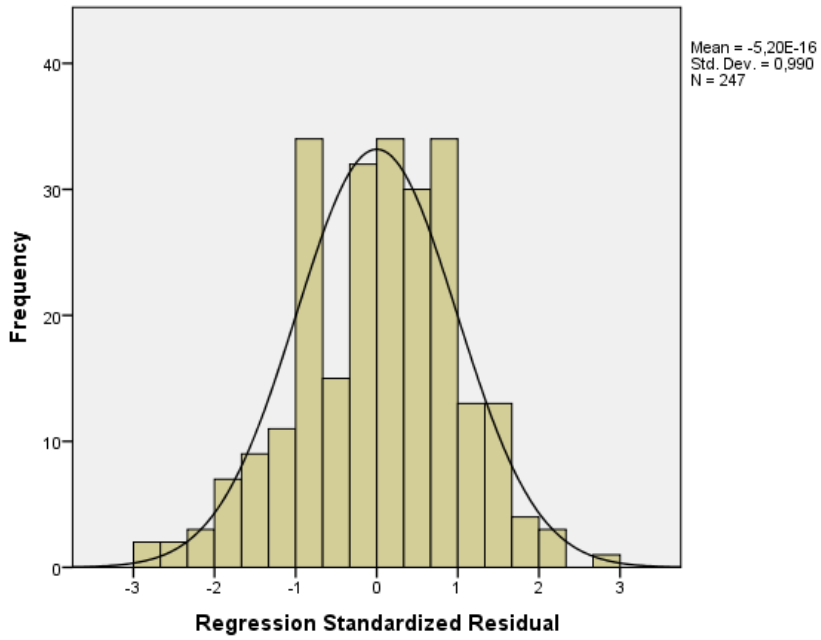
Collineariteit voor privacykennis

(*N* = 247*)

	Tolerantie	VIF
Leeftijd	.432	2.315
Geslacht	.837	1.194
Actief sociale mediagebruik	.908	1.101
Hbo	.466	2.145
Wo	.395	2.531

*Exclusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.

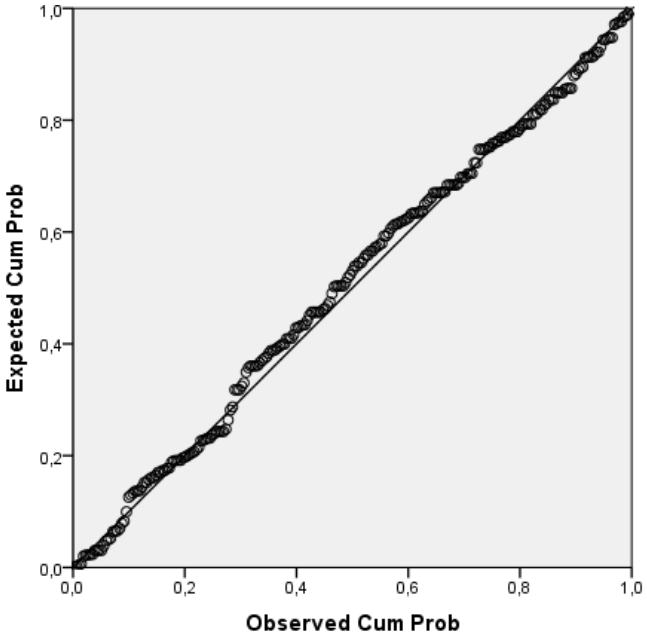
Let op: Tolerantiewaarden die kleiner zijn dan .1 of VIF-waarden die groter zijn dan 10 tonen collineariteit aan.



Appendix B33.

Histogram van de normale verdeling van privacykennis (*N* = 247*)

*Exlcusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.



Appendix B34.

P-P Plot om de normale verdeling van privacykennis aan te tonen (*N* = 247*)

*Exlcusief ontbrekende waarden, welke de respondenten betreffen die niet op actieve wijze van sociale media gebruikmaken en de uitschieter.