

IEDEREEN HEEFT HET OVER PRIVACY, MAAR WAAR HEBBEN ZE HET EIGENLIJK OVER?

Kwalitatief onderzoek naar de percepties van
Nederlandse internetgebruikers over internet privacy

Freshta Aslami

Masterscriptie Communicatiewetenschap



Iedereen heeft het over privacy, maar waar hebben ze het eigenlijk over?

Kwalitatief onderzoek naar de percepties van Nederlandse internetgebruikers
over internet privacy

Freshta Aslami
S1008756
F.aslami@student.ru.nl

22 juni 2019

Versie 1

Masterscriptie
Opleiding Communicatiewetenschap – Pro-sociale communicatie
Radboud Universiteit Nijmegen

Begeleider: Dr. Gabi Schaap
Tweede lezer: Daniëlle Bleize

Inhoudsopgave

Samenvatting	5
Hoofdstuk 1: Inleiding	6
Hoofdstuk 2: Theoretisch kader	9
2.1. Internet privacy.....	9
2.2. Aspecten van privacyproblemen	10
2.3. Gedrag van internetgebruikers en de onderliggende redenen	13
2.4. Internetgebruikers die zich geen zorgen maken	14
2.5. Probleemstelling	15
Hoofdstuk 3: Onderzoeksmethode	17
3.1. Onderzoeksopzet	17
3.2. Eenhedenselectie	17
3.3. Waarnemingsinstrument	18
3.4. Analyseprocedure	20
3.5. Kwaliteitseisen	21
Hoofdstuk 4: Resultaten	23
4.1. Vrijheid	25
4.2. Veiligheid.....	28
Hoofdstuk 5: Conclusie en discussie	35
5.1. Conclusie.....	35
5.2. Discussie	37
Literatuurlijst	40
Bijlagen	44
Bijlage 1. Topiclijst	44
Bijlage 2. Losse kaartjestechniek	49
Bijlage 3. Toestemmingsformulier.....	50
Bijlagen digitaal	
Bijlage 4. MAXQDA-bestand	
Bijlage 5. Transcripten	

Voorwoord

Mensen proberen te begrijpen, dat is voor mij als werknemer bij de geestelijke gezondheidszorg erg belangrijk. Een aantal cliënten van mij maakten zich zorgen over hun internet privacy. Toen ik daarop doorvroeg, vonden zij het moeilijk om te verwoorden waarom zij zich hier zorgen over maakten. Dezelfde week kregen we in de collegebanken les over internet privacy. Alhoewel een les werd geweid aan het belang van internet privacy in het huidige digitale tijdperk, werd niet besproken wat internet privacy precies betekent. Hoe is het dan eigenlijk mogelijk dat zoveel discussies worden gevoerd over internet privacy, als het niet eens duidelijk is wat mensen verstaan onder het concept? Dit riep zowel bij mijn scriptiebegeleider als bij mij de vraag op: wat betekent internet privacy? Uit die vraag is mijn scriptie voortgevloeid.

Een aantal mensen wil ik graag wil bedanken voor hun hulp tijdens het schrijven van deze masterscriptie. Ten eerste wil ik mijn begeleider Gabi Schaap bedanken voor zijn prettige manier van begeleiden. Objectief en met een luisterend oor heeft hij mij onder meer geleerd kritischer te kijken naar zowel mijn eigen studie als naar andere studies. Daarnaast wil ik mijn medeonderzoekers bedanken dat zij met mij meedachten gedurende dit onderzoeksproces. In het bijzonder wil ik Robin Brandes graag bedanken. Niet alleen als medeonderzoeker, maar ook als beste vriendin is zij er altijd voor mij geweest en heeft zij mij geholpen deze scriptie naar een hoger niveau te tillen. Tevens wil ik Marjan de Bie graag bedanken. Zij heeft met regelmaat mijn scriptie zorgvuldig doorgelezen en feedback gegeven op kromme zinnen en spelfouten. Tot slot wil ik mijn respondenten graag bedanken dat zij zo open zijn geweest en tijd hebben gemaakt om mij te helpen.

Na een uitdagende periode, ben ik trots om u deze masterscriptie te tonen. Ik wens u veel leesplezier toe.

Freshita Aslami, Mierlo, 19 juni 2019

Samenvatting

Ondanks dat de wetten over internet privacy en de discussies die het oproept laten zien dat internet privacy een urgent thema is geworden in het maatschappelijk debat, is het onduidelijk wat burgers onder privacy verstaan en waar de privacyzorgen inhoudelijk over gaan. Daarnaast zijn de percepties van de mensen die zich geen zorgen maken over hun privacy een onderbelicht thema in de wetenschap. Dit gaf aanleiding tot een kwalitatief onderzoek naar de percepties van Nederlandse internetgebruikers over hun privacy(zorgen). Uit de twaalf interviews die zijn afgenomen, blijkt dat privacy een manier is om je veilig en vrij te voelen. Onwetendheid bepaalt de mate waarin internetgebruikers zich zorgen maken, en heeft vooral betrekking op de vraag of hun persoonsgegevens veilig zijn op het internet. Concluderend kan gezegd worden dat veiligheid en vrijheid belangrijke waardes zijn voor zowel de internetgebruikers die zich zorgen maken over hun internet privacy als de internetgebruikers die zich geen zorgen maken. De mate van onwetendheid bepaalt of gebruikers zich zorgen maken over hun persoonsgegevens. Hoe minder men weet over de risico's, des te minder zorgen men zich maakt. Er zijn ook internetgebruikers die juist meer wil weten, zodat zij maatregelen kunnen nemen om de persoonsgegevens te beschermen.

Hoofdstuk 1: Inleiding

Het kan niemand ontgaan zijn dat privacy een veelbesproken onderwerp is met diverse percepties en attitudes jegens het belang ervan (DDMA, 2018; IIR, 2018). Met name door geavanceerde ontwikkelingen in de informatie- en communicatietechnologieën ligt de privacy onder vuur (Solove, 2008). Deze technologieën stellen bedrijven in staat om de digitale voetsporen van burgers op het internet te volgen (Boerman, Kruikemeier & Zuiderveen Borgesius, 2017). Zo krijgen bedrijven inzicht in het klik- en koopgedrag van internetgebruikers, waardoor zij onder andere te weten komen welke zoekopdrachten de gebruikers hebben uitgevoerd (Teunis, 2018). Voordat bedrijven persoonsgegevens van gebruikers verzamelen en analyseren, moeten internetgebruikers in Europa nadrukkelijk toestemming geven. Het bedrijf Facebook heeft hier geen rekening mee gehouden en kreeg veel aandacht nadat bleek dat zij privacygevoelige informatie gebruikt heeft, zonder de gebruikers daarover te informeren. Aan het licht kwam bijvoorbeeld dat gegevens met betrekking tot seksuele voorkeuren gebruikt werden om gepersonaliseerde content aan te bieden (Autoriteit Persoonsgegevens, 2017).

Dergelijke nieuwsberichten over privacyschendingen spelen een grote rol in het versterken van het bewustzijn van burgers over hun privacy op het internet (DDMA, 2018). Door dit bewustzijn denken internetgebruikers vaker kritisch na over de wijze waarop bedrijven gebruik maken van hun persoonsgegevens (TNO, 2015). Alhoewel bewustzijn gezien wordt als een positieve ontwikkeling, geldt voor gebruikers dat zij zich hierdoor ook meer zorgen maken ten aanzien van de privacybescherming (DDMA, 2018). Dit komt overeen met een onderzoek van de Autoriteit Persoonsgegevens (2019). Hieruit blijkt dat maar liefst 94 procent van de Nederlandse burgers zich zorgen maakt over hun privacybescherming op het internet. Maar maakt men zich daadwerkelijk zorgen en waar maakt zij zich precies zorgen over?

Het is namelijk opmerkelijk dat, ondanks het grote percentage van bezorgde burgers, sprake is geweest van een hoge verdeeldheid bij het referendum over de Wet op de Inlichtingen- en Veiligheidsdiensten. In de volksmond wordt de betreffende wet ook wel de Sleepwet genoemd (Hart van Nederland, 2018). De Sleepwet houdt in dat de inlichtingen- en veiligheidsdiensten vergaande bevoegdheden krijgen om de veiligheid in Nederland te waarborgen, door onder andere digitale informatie te verzamelen en te analyseren. Hoewel een kleine meerderheid van 49,5 procent van de Nederlandse stemmers tegen de Sleepwet heeft gestemd, is het cruciaal om op te merken dat ruim 46,5 procent voorstanders zijn geweest. De overige Nederlandse stemmers, stemden blanco (Hart van Nederland, 2018). De discussie tussen de voor- en tegenstanders gaat erover dat de tegenstanders beargumenteren dat de

privacy van burgers verloren gaat. In de zoektocht naar bepaalde informatie, wordt namelijk ook informatie van andere mensen ‘meegeslept’ die geen gevaar vormen voor de samenleving (Amnesty, z.d.; Hart van Nederland, 2018). De voorstanders daarentegen vinden de waarborging van de veiligheid in Nederland belangrijk, zelfs als dat ten koste gaat van hun privacy (Niemantsverdriet & Van den Dool, 2018).

Tegenstrijdigheid in houding en zorgen is bovendien terug te zien in het dubbelzinnige gedrag van internetgebruikers na de invoering van de Algemene Verordening Gegevensbescherming (AVG). Met deze wet, die in 2018 is doorgevoerd, hebben bedrijven meer verplichtingen om verantwoord en transparant met persoonsgegevens om te gaan (Autoriteit Persoonsgegevens, 2018). Hoewel bedrijven zich hieraan houden door privacyverklaringen op te stellen, vinden internetgebruikers dat de verklaringen verpakt zijn in lange en ingewikkelde teksten (TNO, 2015). De moeite om de privacyverklaringen te begrijpen is onder meer een reden waarom gebruikers, ondanks mogelijke zorgen, besluiten om alsnog hun persoonsgegevens te verstrekken (Choi, Park & Jung, 2018; Schermer, Custers & van der Hof, 2014). Deze discrepantie wordt de *privacy-paradox* genoemd (Norberg, Horne & Horne, 2007). Aangezien internetgebruikers moeite hebben om te begrijpen op welke wijze hun gegevens gebruikt worden, kan afgevraagd worden of gebruikers wel weten waar zij het over hebben wanneer gesproken wordt over de privacykwesaties.

Kortom, met de invoering van de AVG en de grote verdeeldheid bij de uitslag op de Sleepwet, is het duidelijk geworden dat burgers diverse attitudes hebben en tegenstrijdig gedrag vertonen met betrekking tot de privacyzorgen. Ondanks dat de discussies omtrent deze wetten laten zien dat internet privacy een urgent thema is geworden in het maatschappelijk debat, is het onduidelijk wat mensen precies onder privacy verstaan (Solove, 2008). Het is van belang duidelijk te maken wat privacy voor de internetgebruikers betekent, omdat dit kan bijdragen aan betere kennis en bewustwording onder burgers, overheid en bedrijven. Deze kennis kan relevant zijn in de discussie die gevoerd wordt over beleid betreffende privacykwesaties. Daarom richt dit onderzoek zich op het uitdiepen van de diverse percepties met betrekking tot internet privacy.

Alhoewel eerdere studies onderzoek hebben gedaan naar privacykwesaties, zijn deze vooral gericht op het spanningsveld tussen de zorgen omtrent de privacy en het verstrekken van de persoonsgegevens. Hierbij is voornamelijk aandacht geweest voor de verklaringen achter het verstrekken van persoonsgegevens ondanks de bestaande zorgen (Barth & De Jong, 2017; Li, Sarathy & Xu, 2010; Norberg et al., 2007), maar is het onduidelijk waarom en waarover men zich zorgen maakt. De studies die wel meer gericht waren op de privacyzorgen zijn veelal

kwantitatief van aard, waarbij de vragen of stellingen niet diepgaand genoeg zijn. Zo kunnen respondenten in de meeste onderzoeken louter aangeven in hoeverre zij bezorgd zijn over hun online privacy of in hoeverre zij vrezen voor misbruik van hun persoonsgegevens (Baek & Morimoto, 2012; Lwin, Wirtz & Williams, 2007; Smit, Van Noort & Voorveld, 2014). Bij deze kwantitatieve studies hebben gebruikers niet de mogelijkheid gekregen vanuit hun eigen belevingswereld de percepties ten aanzien van de inhoud van de privacyzorgen op het internet onder woorden te brengen. Daardoor is het ook niet mogelijk geweest om door te vragen wat zij verstaan onder internet privacy. Dit roept de vraag op wat de betekenis is van privacy en of mensen daadwerkelijk bezorgd zijn over hun privacy of dat de situatie genuanceerder ligt. Bovendien zijn voor zover bekend nauwelijks studies die de diverse percepties en attitudes omtrent de privacyzorgen hebben uitgediept. In de meeste studies wordt namelijk gesproken over de mensen die zich zorgen maken, maar daarbij is de kant van de gebruikers die zich nauwelijks zorgen maken of andere percepties hebben, onderbelicht.

Samenvattend kan gezegd worden dat voorgaande onderzoeken naar de privacyzorgen op het internet beperkt inzicht geven in de belevingswereld van de internetgebruikers. Om beter inzicht te krijgen in de belevingswereld van internetgebruikers omtrent hun privacyzorgen op het internet, wordt gebruik gemaakt van kwalitatief onderzoek. Kwalitatief onderzoek is namelijk een geschikte methode om de belevingen en de percepties van mensen aan het licht te brengen (Braun & Clarke, 2013). Ten behoeve van het uitdiepen van percepties over privacyzorgen, wordt de volgende onderzoeksvraag behandeld: *Welke percepties hebben Nederlanders ten aanzien van hun privacy en privacyzorgen op het internet?*

Door de ontbrekende kennis aan te vullen, wordt gepoogd met deze studie een bijdrage te leveren aan wetenschappelijke inzichten op het gebied van privacy op het internet. Zo kan het als basis dienen voor een kwantitatief vervolgonderzoek, waarbij de onderzoekers gerichter hypothesen en vragen over het concept privacy kunnen opstellen. Ook kan het leidend zijn in een survey over het thema privacybeleving. Tevens kan het een bijdrage leveren aan het kritischer kijken naar de privacykwesties in de samenleving. De interviews die ten behoeve van dit onderzoek worden gehouden, dragen daar allereerst al aan bij. Door met respondenten over hun online privacypercepties te praten, reflecteren zij mogelijk kritischer op bestaande percepties, waardoor zij zich meer bewust worden van het al dan niet verstrekken van persoonsgegevens. Bovendien kunnen de resultaten die voortkomen uit dit onderzoek gebruikt worden om andere gebruikers bewust te maken van de heersende privacy discussies, zodat zij kritischer gaan kijken naar de manier waarop zij zelf met hun gegevens op het internet omgaan. Tot slot kan deze kennis meegenomen worden bij de wetgeving omtrent de privacykwesties.

Hoofdstuk 2: Theoretisch kader

Uit de aanleiding blijkt dat eerdere onderzoeken naar privacyzorgen op het internet beperkt inzicht geven in de percepties van internetgebruikers. Dit onderzoek richt zich daarom op de verkenning van de percepties ten aanzien van internet privacy. In dit hoofdstuk wordt eerst toegelicht wat wetenschappers verstaan onder internet privacy. Vervolgens wordt aan de hand van inzichten uit eerder onderzoek besproken wat al bekend is over privacyzorgen. Daarna wordt gekeken naar het gedrag van gebruikers op het internet en naar de redenen waarom zij besluiten om hun persoonsgegevens al dan niet te verstrekken. Vervolgens wordt behandeld wat bekend is over de percepties van mensen die zich geen zorgen maken over hun online privacy. Dit hoofdstuk wordt afgesloten met de onderzoeksvraag en de bijbehorende deelvragen.

2.1. Internet privacy

“It seems as though everybody is talking about “privacy”, but it is not clear exactly what they are talking about” (Solove, 2008). Dit citaat illustreert dat privacy een veelbesproken onderwerp is, maar dat het onduidelijk is wat mensen ermee bedoelen. Om de diverse percepties ten aanzien van (internet) privacyzorgen uit te diepen, is het noodzakelijk eerst te begrijpen wat privacy in het algemeen inhoudt door verscheidene definities van het concept uiteen te zetten.

Voor diverse wetenschappers is het lastig een duidelijke definitie te geven voor een complex begrip als privacy. Dit komt doordat de context en tijd waarin het concept privacy gebruikt wordt een belangrijke rol spelen bij de betekenisgeving van het begrip (Cuijpers, 2007). Een voorbeeld hiervan is dat onderzoekers naar privacy verwijzen als de persoonlijke levenssfeer van een individu. Buitenstaanders hebben niet het recht inbreuk te maken op deze persoonlijke levenssfeer. Echter, in de context van bijvoorbeeld gedetineerden, is het vanwege veiligheidsbelangen gerechtvaardigd om inbreuk te maken in hun persoonlijke levenssfeer (Blok, 2002).

Een tweede verklaring waarom onduidelijkheid over het begrip bestaat, heeft te maken met de reikwijdte van het concept (Cuijpers, 2007). Zo pleiten Warren en Brandeis (1890) dat privacy het recht van een individu is om alleen gelaten te worden. Bij deze definitie worden vraagtekens gezet bij wat ‘alleen laten’ precies betekent. ‘Alleen laten’ heeft namelijk niet louter betrekking op het concept privacy. Iemand die ongewenst aangeraakt wordt, wordt ook niet alleen gelaten. Desalniettemin wordt dit niet gezien als een ‘privacy’ probleem, maar als iemand die ongewenst fysiek contact ondervindt (Solove, 2008).

Tot slot wordt privacy gedefinieerd in termen van controle (Westin, 1968). Hoewel dit los staat van de redenen waarom er onduidelijkheid bestaat over het concept, is het belangrijk om deze definitie te benoemen. Het is namelijk een veelgebruikte definitie in verscheidene onderzoeken (TNO, 2015). Zo wordt in diverse studies naar privacy verwezen als het vermogen van een persoon om te controleren welke informatie door welke personen of bedrijven verkregen en gebruikt worden (Westin, 1968).

Opvallend bij bovenstaande definiëringen is dat geen duidelijk onderscheid wordt gemaakt in offline en online privacy. Enerzijds kan dit komen doordat het internet gedurende enkele van deze studies nog niet bestond, maar anderzijds is het onduidelijk of hier een verschil tussen bestaat. Zo zijn studies die online privacy omschrijven als de manier waarop persoonsgegevens verzameld en geanalyseerd worden op het internet (Pavlou, 2011), maar er wordt ook gepleit dat de privacy norm ondanks de opkomst van technologische ontwikkelingen niet veranderd is (Nissenbaum 2011). Activiteiten die offline gedaan kunnen worden, kunnen tegenwoordig ook online plaatsvinden. Mensen boeken hun vlucht online, maken gebruik van internetbankieren, shoppen online en ga zo maar door. Doordat nauwelijks verschil is tussen online en offline handelingen, wordt online en offline privacy als hetzelfde concept beschouwd (Nissenbaum, 2011). Dit roept de vraag op of internetgebruikers zelf een onderscheid maken tussen online en offline privacy.

Al met al mag het duidelijk zijn dat privacy een subjectief concept is dat op verscheidene manieren geïnterpreteerd wordt. Zo associëren wetenschappers privacy met persoonlijke levenssfeer, met het hebben van controle en met 'alleen gelaten' worden. Desondanks zijn alle definities tot op heden bedacht door wetenschappers, terwijl nooit aan internetgebruikers is gevraagd wat internet privacy voor hen betekent. Het is dus nog niet bekend of gebruikers het eens zijn met de huidige definiëringen van wetenschappers of dat zij er een andere gedachtegang op nahouden.

2.2. Aspecten van privacyproblemen

Zoals besproken maakt een groot deel van de Nederlanders zich zorgen over hun privacy op het internet. Op zoek naar het antwoord op de vraag waarom mensen zich zorgen maken, is het belangrijk om in kaart te brengen uit welke aspecten *internet* privacy bestaat volgens wetenschappers.

Solove (2006) maakt geen duidelijk onderscheid tussen offline en online privacy, maar geeft wel aan dat nieuwe technologieën ertoe leiden dat privacy op een hele reeks nieuwe manieren geschaad kan worden. Hij achtte het hierdoor nodig om een *Taxonomy of Privacy* te

ontwikkelen. In dit model wordt gepoogd de aspecten van privacyproblemen aan te duiden. Het onderscheidt vier algemene categorieën, te weten informatieverzameling, informatieverwerking, informatieverspreiding en het indringen in iemands leven (Solove, 2006). In het licht van dit onderzoek dienen de privacyproblemen als basis voor het in kaart brengen van de privacyzorgen die Nederlandse internetgebruikers mogelijk beleven. Een cruciale vraag die het model oproept is of de privacyproblemen die verondersteld worden door wetenschappers, door de internetgebruikers zelf ervaren worden als privacyzorgen. Daarnaast is het maar de vraag of het model volledig is en of er nog andere privacyzorgen zijn die internetgebruikers hebben.

Informatieverzameling betreft de manier waarop persoonsgegevens verzameld worden. Het verzamelen van informatie is problematisch, omdat men zich hierdoor bekeken en ongemakkelijk voelt (Solove, 2006). Dat gevoel van toezicht heeft een remmende werking op het gedrag van gebruikers, waardoor het een vorm van sociale controle is die het gevoel van vrijheid beperkt (Solove, 2006). Ondanks deze bewering is niet aan internetgebruikers gevraagd of zij zich daadwerkelijk bekeken en ongemakkelijk voelen wanneer zij online rondsurfen. Zelfs indien dit wel het geval is, is het onduidelijk wat de achterliggende reden is voor het ongemakkelijke gevoel dat ontstaat bij het verzamelen van persoonsgegevens.

Informatieverwerking heeft betrekking op het opslaan, analyseren en zelfs het manipuleren van persoonsgegevens. Gebruikers verwachten dat zij op het internet slechts een klein deel van hun persoonsgegevens online achterlaten, maar deze verwachtingen worden verstoord doordat met informatieverwerking gegevens samengevoegd worden (Solove, 2006). Hierdoor is het voor bedrijven mogelijk een uitgebreid profiel op te zetten van individuele internetgebruikers. Vervolgens gebruiken bedrijven persoonsgegevens, zonder dat gebruikers daar (bewust) toestemming voor geven (Solove, 2006). Ondanks de veronderstelling dat internetgebruikers denken dat zij slechts een deel van zichzelf op het internet blootleggen, is niet bekend of zij daadwerkelijk het idee hebben dat zij slechts een deel van zichzelf op het web achterlaten. Het is onduidelijk hoe gebruikers het online rondsurfen beleven als zij ervan op de hoogte zijn dat bedrijven een uitgebreid profiel van hen opzetten.

Informatieverspreiding betreft de mogelijkheid waarin iedere internetgebruiker tegenwoordig gemakkelijk informatie kan delen met derden. Het nadeel hiervan is dat er mogelijk incomplete informatie over gebruikers verspreid wordt, waardoor een vertekend beeld van de internetgebruikers ontstaat. Aan de andere kant wordt ook correcte informatie verspreid, maar willen internetgebruikers dit alsnog liever voor zichzelf houden vanwege veiligheidsbelangen (Solove, 2006). Hoewel op basis van bovenstaande punten wordt

verondersteld dat dataverspreiding volgens internetgebruikers een vervelende activiteit is, hebben internetgebruikers nooit zelf benoemd wat zij hiervan vinden. Zelfs als zij dataverspreiding inderdaad zorgwekkend vinden, is het onbekend wat de achterliggende reden van internetgebruikers is om correcte informatie voor zichzelf te houden wanneer zij zich wel veilig voelen.

Indringen in iemands leven is het inbreuk maken op het recht om ‘alleen’ te zijn, waardoor iemands rust wordt verstoord (Solove, 2006; Warren & Brandeis, 1890). Vooral als internetgebruikers persoonlijke content ontvangen, versterkt dit het gevoel dat er ingedrongen wordt in hun leven (Van Doorn & Hoekstra, 2013). Het verschil met de overige drie aspecten van de *Taxonomy of Privacy* is dat het indringen in iemands leven rechtstreeks invloed heeft op het individu. Dit hoeft bij dataverzameling, dataverwerking en dataverspreiding niet altijd het geval te zijn (Solove, 2006). Het is de vraag of internetgebruikers dit verschil ook zien of dat zij indringen in iemands leven op een andere manier beleven. Bovendien zijn het louter veronderstellingen: krijgt iemand daadwerkelijk het gevoel dat ingedrongen wordt in zijn/haar leven als inbreuk gemaakt wordt op het recht om ‘alleen’ te zijn? En beleeft iemand op dat moment een verstoring van zijn/haar rust? Wat wel duidelijk is, is dat het indringen in iemands leven een bedreiging vormt voor de autonomie van een persoon (Solove, 2006). Wanneer internetgebruikers worden vastgepind op een profiel door persoonlijke content te ontvangen, beperkt dit namelijk de keuzemogelijkheden (Becker, 2015). Ondanks deze bewering is niet eenduidig bepaald of het verliezen van de autonomie een onderdeel is van ervaren privacyzorgen (Solove, 2006). De vraag die dit oproept is waar volgens internetgebruikers het onderscheid en de overeenkomst ligt tussen het verliezen van autonomie en het ervaren van privacyzorgen.

Al met al is het duidelijk geworden dat de *Taxonomy of Privacy* een aantal privacyzorgen aankaart. Desondanks is onbekend of de problemen die opgesteld zijn door wetenschappers ook door internetgebruikers worden ervaren als privacyzorgen. Zelfs als dat wel het geval is, roept de *Taxonomy* diverse inhoudelijke vragen op. Waarom voelen internetgebruikers zich ongemakkelijk als zij bekeken worden? Hoe komt het dat mensen correcte informatie voor zichzelf willen houden? En wanneer hebben gebruikers het gevoel dat ingedrongen wordt in hun leven en wanneer is dit minder een probleem? Dit zijn onder meer belangrijke vragen om beter inzicht te krijgen in de percepties van internetgebruikers.

2.3. Gedrag van internetgebruikers en de onderliggende redenen

In de vorige paragraaf kwam naar voren dat de verscheidene aspecten van privacyproblemen mogelijke zorgen met zich meebrengen bij internetgebruikers. Desondanks is het opvallend dat maar een kleine groep in lijn handelt met hun privacyzorgen en actie onderneemt om de persoonsgegevens te beschermen door advertenties te vermijden of cookies te verwijderen (McDonald & Cranor, 2010). De rest van de internetgebruikers verstrekt de persoonsgegevens ondanks eventuele privacyzorgen. Deze discrepantie wordt de *privacy-paradox* genoemd (Norberg et al., 2007). Diverse studies hebben dit tegenstrijdige gedrag van internetgebruikers onderzocht (Aguirre, Mahr, Grewal, Ruyter & Wetzels, 2015; Barth & De Jong, 2017; Norberg, et al., 2007). Doordat er zoveel studies zijn die verklaren dat mensen niet in lijn handelen met hun privacyzorgen, kan worden afgevraagd of mensen zich daadwerkelijk zorgen maken over hun privacy. Over welke privacykwesties maken zij zich dan zorgen en over welke niet? En waarom maken zij zich zorgen? Om dit verder uit te diepen is het van belang te kijken welke factoren een belangrijke rol spelen in de *privacy-paradox* en wat voor vragen deze oproepen.

De *Privacy Calculus Theory* stelt dat individuen de potentiële voordelen en risico's tegen elkaar opwegen als zij overwegen de persoonsgegevens te verstrekken (Li et al., 2010). Zo is het een voordeel dat gebruikers bruikbare informatie verkrijgen bij het verstrekken van persoonsgegevens en omdat daarmee de behoefte om bepaalde content te zien onmiddellijk bevredigd wordt (Acquisti, 2004; Li, Sarathy & Xu, 2010). Deze voordelen wegen internetgebruikers af tegen een aantal factoren, zoals de mate waarin zij een website vertrouwen en de mate waarin zij gepercipieerde controle over hun persoonsgegevens ervaren (Barth & De Jong, 2017; Dinev & Hart, 2006). Eigendom en dus ook de persoonsgegevens zijn volgens de *ownership theory* namelijk belangrijk voor gebruikers (Avey, Avolio, Crossley & Luthans, 2009). Wanneer internetgebruikers niet weten wat met hun persoonsgegevens gebeurt voelen zij zich kwetsbaar en machteloos (Solove, 2006). Daarom is het belangrijk om internetgebruikers op een open en transparante manier te informeren over de wijze waarop met hun persoonsgegevens wordt omgegaan (Aguirre et al., 2015; Bleier & Eisenbeiss, 2015; Boerman et al., 2017; Dinev, Xu, Smith & Hart, 2013; Miyazaki, 2008). Desalniettemin zijn gebruikers niet tevreden over de manier waarop zij geïnformeerd worden (Schermer et al., 2014). Het blijkt dat onwetendheid bestaat over de manier waarop bedrijven met de persoonsgegevens omgaan, omdat het cognitieve capaciteit vergt voor internetgebruikers om bij te houden hoe zij de persoonsgegevens kunnen beschermen (Choi, et al., 2018; Schermer et al., 2014; Ur, Leon, Cranor, Shay, & Wang, 2012). Doordat het vermoeiend is om de lange

privacyverklaringen te lezen en te begrijpen, nemen internetgebruikers daar niet de moeite voor en zijn zij geneigd de verklaringen te accepteren (Choi et al., 2018).

Concluderend kan gesteld worden dat internetgebruikers controle en transparantie willen, maar dat zij de cognitieve inspanning tot een minimum willen beperken. Dit roept de vraag op wat transparantie voor gebruikers betekent en hoe zij de juiste situatie met betrekking tot het transparant omgaan met persoonsgegevens voor zich zien. Bovendien is het relevant om op te merken dat de *Privacy Calculus Theory* duidelijk weergeeft wat de potentiële voordelen en risico's zijn bij het al dan niet verstrekken van de persoonsgegevens, maar dat het niet duidelijk is hoe internetgebruikers de voordelen en nadelen tegen elkaar afwegen. Wanneer wegen de nadelen zwaarder dan de voordelen, of andersom? Hoe wordt rationeel een afweging gemaakt als sprake is van onwetendheid met betrekking tot de privacykwesties? En als diverse studies bevestigen dat mensen niet in lijn handelen met hun privacyzorgen, maken mensen zich dan wel echt zorgen? Dit zijn belangrijke vragen die nader onderzocht moeten worden, om te kunnen achterhalen of mensen zich daadwerkelijk zorgen maken over hun online privacy.

2.4. Internetgebruikers die zich geen zorgen maken

In de vorige paragrafen is gesproken over de problematische aspecten van privacy en hoe mensen zich gedragen wanneer zij zich zorgen maken over hun privacy. Desalniettemin zijn er ook mensen die zich geen zorgen maken over hun privacy. Om inzicht te krijgen in de volledige belevingswereld van internetgebruikers, wordt besproken wat in de literatuur bekend is over de percepties van mensen die zich geen zorgen maken over hun privacy.

Hoewel hierover relatief weinig bekend is, is wel duidelijk dat er twee redenen zijn waarom mensen zich geen zorgen maken over de online privacy. Ten eerste hechten mensen meer waarde aan de nationale veiligheid dan aan hun eigen privacy. Aangezien burgers denken dat criminelen gemakkelijker opgespoord worden als de overheid toegang heeft tot persoonsgegevens van burgers, maken zij zich geen zorgen wanneer persoonsgegevens worden gevraagd (Solove, 2008). Ten tweede gebruiken mensen veelal het argument dat zij niets illegaals doen en dus niets te verbergen hebben (Solove, 2008).

Echter, het 'niets-te-verbergen' argument is vooral gericht op het verbergen van illegale activiteiten (Solove, 2008). Dus hoe zit het dan met het verbergen van privacygevoelige informatie waar geen illegale activiteiten bij betrokken zijn? Zo blijkt uit onderzoek dat creditcardgegevens meer worden beschouwd als privacygevoelige informatie dan een emailadres (Cranor, Reagle & Ackerman, 1999). Desalniettemin is het onduidelijk waarom internetgebruikers bepaalde informatie privacygevoeliger vinden dan andere informatie en of

gebruikers nog steeds standvastig bij hun mening blijven dat zij niets te verbergen hebben wanneer om meer privacygevoelige informatie wordt gevraagd. De veronderstelling is namelijk dat iedereen zich op de één of ander manier onprettig voelt als bedrijven privacygevoelige informatie vragen (Flaherty, 1999). Flaherty (1999) stelt daarover dat internetgebruikers geen waarde hechten aan hun privacy op het moment dat gebruikers het goedkeuren wanneer privacygevoelige informatie wordt gevraagd en het argument gebruiken dat zij toch niets te verbergen hebben. Maar is het inderdaad zo dat mensen geen waarde hechten aan hun privacy hebben wanneer zij zeggen dat zij niets te verbergen hebben?

Vanuit rationeel oogpunt kunnen bovenstaande beweringen ontkracht worden, omdat men wellicht verwacht dat niet alle informatie vastgelegd wordt. Zelfs wanneer dat wel gebeurt, zouden internetgebruikers ervanuit kunnen gaan dat de privacygevoelige informatie louter door enkele functionarissen van de wetshandhaving zal worden gezien of door een computer (Solove, 2008). Desondanks zijn dit veronderstellingen en dient onderzocht te worden hoe gebruikers het online surfen beleven als zij weten dat hun persoonsgegevens niet alleen door wetshandhavers worden bekeken, maar ook in handen van commerciële bedrijven komen die niets van doen hebben met de nationale veiligheid. Hoeveel waarde hechten internetgebruikers dan aan hun internet privacy? En wat weten zij eigenlijk van de wijze waarop bedrijven met hun persoonsgegevens omgaan?

Concluderend kan gezegd worden dat een deel van de mensen zich geen zorgen maakt over hun privacy, omdat zij vinden dat zij niets te verbergen hebben of omdat zij de veiligheid belangrijker vinden dan de privacy. Ondanks deze beweringen is het een cruciale vraag om te stellen hoe mensen hier tegenaan kijken als de overheid privacygevoelige informatie vraagt of wanneer commerciële bedrijven privacygevoelige informatie vragen. Tot slot is het belangrijk om op te merken dat slechts enkele studies gekeken hebben naar de percepties van mensen die zich geen zorgen maken. Dit roept de vraag op of er meerdere redenen zijn dat zij zich geen zorgen maken en waar dit dan mee te maken heeft.

2.5. Probleemstelling

Uit literatuur en empirisch onderzoek blijkt dat diverse definities worden aangehouden omtrent het concept internet privacy. Desondanks is niet gekeken naar wat internetgebruikers er zelf onder verstaan en waarom men zich zorgen maakt over hun internet privacy. Het zijn namelijk veelal veronderstellingen die worden gedaan over de redenen waarom internetgebruikers zich zorgen maken. Tevens is relatief weinig bekend over de percepties van internetgebruikers die zich geen zorgen maken over hun internet privacy. Het doel van dit onderzoek is daarom inzicht

te krijgen in de belevingswereld van internetgebruikers ten aanzien van de privacyzorgen op het internet. Daarop aansluitend is de volgende onderzoeksvraag opgesteld: *Welke percepties hebben Nederlandse internetgebruikers ten aanzien van privacy(zorgen) op het internet?*

Om de onderzoeksvraag te beantwoorden zijn een aantal deelvragen opgesteld. Deze deelvragen zijn opgesteld aan de hand van het theoretisch kader:

1. Wat betekent internet privacy voor Nederlandse internetgebruikers?
2. Welke privacyzorgen ervaren Nederlandse internetgebruikers?
3. Waarom maken Nederlandse internetgebruikers zich wel of geen zorgen over hun internetprivacy?

Hoofdstuk 3: Onderzoeksmethode

In dit hoofdstuk wordt beargumenteerd waarom voor een kwalitatieve onderzoeksmethode is gekozen, gevolgd door een uitleg over de manier waarop het onderzoek is uitgevoerd. Tot slot wordt de waarborging van de kwaliteitseisen uiteengezet.

3.1. Onderzoeksopzet

Het doel van deze studie is inzicht te krijgen in de belevingswereld van internetgebruikers ten aanzien van hun privacy(zorgen) op het internet. Hiervoor wordt een kwalitatieve onderzoeksmethode toegepast, omdat het hiermee mogelijk is complexe fenomenen in kaart te brengen, zoals de paradoxale percepties en houdingen jegens internet privacy (Boeije, 2014). Een tweede reden waarom gekozen is voor kwalitatief onderzoek, is dat gepoogd wordt inzicht te verkrijgen in een niet-geëxploreerde verschijnsel (Hijmans & Wester, 2006). Zo zijn binnen het onderzoeksveld de percepties van internetgebruikers die zich geen zorgen maken over hun internet privacy onderbelicht.

Om de respondenten de ruimte te geven om hun interpretatie en betekenis over internet privacy in eigen woorden te delen, is gekozen voor diepte-interviews. Bij deze interviews is het mogelijk diepgaande informatie te krijgen over de leefwereld van de Nederlandse internetgebruikers wat betreft internet privacy (Hijmans & Wester, 2006). Bovendien is er rekening mee gehouden dat privacygevoelige onderwerpen aan bod kunnen komen tijdens de interviews. Respondenten vinden het wellicht prettiger om dit soort informatie één op één te bespreken dan in een groep. Het doel van de analyse van de interviews is een conceptueel model te ontwikkelen die gaat over de percepties van privacy(zorgen) van Nederlandse internetgebruikers.

3.2. Eenhedenselectie

Aangezien het onderzoek zich richt op Nederlandse internetgebruikers, zijn de respondenten gekozen middels een doelgerichte steekproef. Voor de werving van de respondenten is gebruik gemaakt van het netwerk van de onderzoeker, maar is ook gebruik gemaakt van de sneeuwbalmethode: sommige respondenten zijn geworven middels het netwerk van de respondenten (Wester, Renckstorf & Scheepers, 2012). Bij het werven van de respondenten is niet gestreefd naar een representatieve steekproef van de Nederlandse bevolking, maar het was wel van belang een representatief en volledig beeld te krijgen van het verschijnsel dat onderzocht wordt (Hijmans & Wester, 2006). Dit betreft de percepties omtrent internet privacy

van een zo breed mogelijk publiek. Zie Tabel 1 voor een weergave van de respondenten die deel hebben genomen aan het onderzoek:

Tabel 1

Kenmerken geïnterviewde respondenten.

Code	Geslacht	Leeftijd	Opleidingsniveau	Etnische achtergrond
G1	Vrouw	35	HBO	Indonesisch
G2	Vrouw	58	MBO	Nederlands
G3	Vrouw	23	HBO	Nederlands
G4	Man	25	WO	Nederlands
G5	Man	24	WO	Turks
G6	Vrouw	37	WO	Afghaans
G7	Man	44	MBO	Nederlands
G8	Man	33	HBO	Nederlands
G9	Vrouw	24	MBO	Nederlands
G10	Man	61	HBO	Nederlands
G11	Vrouw	22	MBO	Indonesisch
G12	Vrouw	27	WO	Afghaans

Bovenstaande respondenten hebben *active consent* verleend om deel te nemen aan het onderzoek, door de toestemmingsverklaring te ondertekenen (zie bijlage 3). Gedurende de interviews is sprake geweest van *theoretical sampling*. Zo is gekeken naar mogelijke afwijkende percepties en is gestreefd naar saturatie (Braun & Clarke, 2013). Een voorbeeld van de *theoretical sampling* en de nastreving van saturatie is dat gedurende de interviews door een aantal respondenten werd benoemd dat zij zich geen zorgen maken, omdat zij geen bekend persoon zijn en daardoor niet denken dat iemand misbruikt maakt van hun persoonsgegevens. Vervolgens is besloten om een internetgebruiker te interviewen met maar liefst 22.000 volgers op haar Instagram. Uiteindelijk is tijdens het laatste interview geen sprake geweest van nieuwe perspectieven en is saturatie bereikt.

3.3. Waarnemingsinstrument

Middels het theoretische kader zijn *sensitizing concepts* tot stand gekomen. Dit zijn onderwerpen uit de literatuur die handvatten geven om de interviews te leiden (Blumer, 1954). Voorbeelden hiervan zijn het concept ‘internet privacy’ en ‘aspecten van privacyzorgen’. De

sensitizing concepts zijn omgezet in diverse open vragen die gesteld zijn aan de respondenten. Met behulp van de open vragen worden de internetgebruikers namelijk gestimuleerd om vanuit hun eigen referentiekader te redeneren (Braun & Clarke, 2013). De open vragen zijn verwerkt in de topiclijst (zie bijlage 1). De topiclijst vormde een leidraad tijdens het afnemen van de interviews (Wester & Peters, 2009). Deze topiclijst is verdeeld in vijf delen, waarvan vier gebaseerd zijn op de subparagrafen uit het theoretische kader. In het eerste deel kregen de respondenten namelijk de ruimte om zichzelf voor te stellen. Hierbij werd ook gevraagd of de respondenten het nieuws kijken of de krant lezen. Aangezien uit de literatuur bleek dat mediaberichten over privacyschendingen invloed hebben op het bewustzijn, had dit wellicht invloed op hun belevingswereld. Daarna zijn de percepties van de respondenten behandeld. Voordat hier dieper op in werd gegaan, begon elk deel van de topiclijst met een startvraag. Een voorbeeld hiervan is dat gepoogd werd om de betekenis van internet privacy te achterhalen door te beginnen met de startvraag: ‘Wat roept het concept privacy bij je op?’. Voor de respondenten die moeite hadden om deze vraag te beantwoorden, is de losse kaartjestechniek ingezet (zie bijlage 2). Dit waren een aantal kaartjes met definities van privacy bedacht door de wetenschappers, zoals ‘controle’, ‘persoonlijke levenssfeer’ en ‘alleen gelaten worden’. Met deze techniek werd het voor respondenten gemakkelijker om antwoord te geven op de vraag (Ketelaar, Hentenaar & Kooter, 2011). Vervolgens is doorgevraagd op de antwoorden die de respondenten gaven. Een voorbeeld van een *follow-up* vraag is dat wanneer respondenten benoemden dat zij aan controle moeten denken bij internet privacy, de onderzoeker heeft gevraagd of zij willen toelichten waarom zij dan aan controle moeten denken.

Het middelste deel van de topiclijst ging over de aspecten van de privacyzorgen. Hierin kwamen de vier aspecten van *Taxonomy of privacy* in terug. Het doel was te achterhalen wat zij verstaan onder privacyzorgen en waarom respondenten zich zorgen maken over hun privacy. Het onderwerp autonomie kwam ook terug in dit deel. Bij deze vraag is in de topiclijst genoteerd dat eerst gecontroleerd moest worden of de respondenten begrijpen wat autonomie betekent. Dit was om te voorkomen dat de vragen verkeerd begrepen werden. Vervolgens werd nagegaan of autonomie-zorgen ervaren werden als privacyzorgen en waar dat mee te maken had.

In het laatste deel zijn vooral vragen opgesteld over het ‘niets-te-verbergen’ argument. Dit deel begon met de startvraag of de respondenten ooit het idee hadden dat het niet slim was om de persoonsgegevens te verstrekken. Daarna kon doorgevraagd worden wat de redenen hiervan waren en of bepaalde informatie privacygevoeliger werd ervaren en waar dat aan lag. In de topiclijst is een kanttekening gemaakt om goed te letten op de non-verbale houding, voor het geval de respondenten zich ongemakkelijk voelden wanneer zij vertelden over de

privacygevoelige onderwerpen (Ketelaar, Hentenaar & Kooter, 2011). De onderzoeker hield op deze manier in de gaten of de respondenten minder open vertelden en kon daarop anticiperen, door bijvoorbeeld nogmaals te benoemen dat de gegevens anoniem verwerkt werden.

Alhoewel in de topiclijst alle delen op de volgorde van het theoretisch kader zijn weergegeven, is deze volgorde niet altijd aangehouden tijdens de interviews. Als de respondenten bijvoorbeeld benoemden dat zij zich geen zorgen maakten over hun privacy of benoemden dat zij meer transparantie wilden, werd eerst hierop ingegaan. Ook was er ruimte voor onverwachte onderwerpen die niet op de topiclijst stonden. Aangezien kwalitatief onderzoek een flexibele methode is, was het mogelijk het interview hierop aan te passen (Braun & Clarke, 2013).

Voordat de topiclijst gebruikt werd bij de respondenten, heeft de onderzoeker een oefensessie gehouden met een medestudent die zich ook verdiept had in het onderzoek. Hierdoor kon de onderzoeker vertrouwd raken met het meetinstrument. Door middel van deze oefensessie is de topiclijst aangescherpt, waardoor de kwaliteit van de vragen is toegenomen. Een voorbeeld hiervan is dat tijdens de oefensessie naar voren kwam dat de vragen naar zorgen door een 'vertekend beeld' onduidelijk waren. Met de medestudent is bedacht om het onderwerp in te leiden met een concreet voorbeeld: aan de respondenten werd gevraagd of zij zich zorgen zouden maken over een mogelijk vertekend beeld, als zij een zoekopdracht op Google zouden uitvoeren naar wapens.

3.4. Analyseprocedure

Voor de analyse van de transcripten is gebruik gemaakt van het computerprogramma MAXQDA. Middels deze software is het mogelijk om op een systematische manier codes toe te kennen aan de interviews en uiteindelijk kernthema's te ontwikkelen die de onderzoeksvraag beantwoorden. Om tot deze thema's te komen zijn eerst een aantal fases doorlopen.

De eerste fase van data-analyse is de exploratiefase (Braun & Clarke, 2013), waarbij de onderzoeker de transcripten heeft doorgenomen en stukken tekst gemarkeerd heeft die haar opvielen. Een voorbeeld hiervan is dat sommige respondenten zich juist geen zorgen maakten over hun privacy, door een gebrek aan kennis. Daarna is sprake geweest van open codering: fragmenten die gingen over de percepties omtrent internet privacy kregen een code. Een aantal voorbeelden van de open codering zijn 'niets illegaals te verbergen' en 'kwetsbaar voelen'. De volgende fase is de specificatiefase (Braun & Clarke, 2013), waarbij concepten en thema's tot stand kwamen. Hierbij heeft de onderzoeker gekeken of er bepaalde patronen te zien waren in de antwoorden van de respondenten. De onderzoeker merkte bijvoorbeeld op dat het onderwerp

onwetendheid en controle vaak met elkaar samenhangen. Ook merkte de onderzoeker op dat ‘persoonlijke kwetsbaarheid’ regelmatig gepaard ging met ‘interessant doelwit’. De patronen en thema’s zijn systematisch en regelmatig met elkaar vergeleken. Dit is een cyclisch en iteratief proces geweest. Dit wil zeggen dat de onderzoeker controleerde of de codes onder de juiste concepten stonden. Een voorbeeld hiervan is dat de code ‘internetervaring’ eerst onder ‘persoonlijke kwetsbaarheid’ stond. Bij het controleren van de codes en concepten, kwam de onderzoeker tot de conclusie dat ‘internetervaring’ vooral de mate van onwetendheid liet zien. Daarom is besloten om deze code onder het concept ‘onwetendheid’ te plaatsen. Vervolgens is wel een stippellijn weergegeven tussen ‘internetervaring’ en ‘persoonlijke kwetsbaarheid’. Tot slot vond de reductiefase plaats (Braun & Clarke, 2013). In deze fase zijn de kernthema’s ‘vrijheid’ en ‘veiligheid’ ontwikkeld. Bovenstaande fases zijn meerdere malen doorlopen om te kijken of de thema’s nog steeds van toepassing waren bij de gecodeerde fragmenten. Het resultaat van de uiteindelijke codes en thema’s is op een heldere manier gepresenteerd middels een concept-indicator model in de resultatensectie.

3.5. Kwaliteitseisen

Om de kwaliteit van het onderzoek te verhogen, zijn een aantal stappen ondernomen om de validiteit van het onderzoek te waarborgen.

Tijdens de interviews is sprake geweest van *member checking*, doordat de onderzoeker regelmatig het antwoord van de internetgebruikers samenvatte en vroeg of dit goed begrepen was. Op deze manier werd een verkeerde interpretatie van het antwoord voorkomen en konden de respondenten de samenvatting zo nodig verbeteren of bijstellen (Braun & Clarke, 2013). Naast *member checking*, is sprake geweest van triangulatie doordat de onderzoeker naar stabiliteit in de antwoorden van de respondenten zocht (Braun & Clarke, 2013). De onderzoeker heeft dit gedaan door op diverse manieren en invalshoeken een vraag te stellen. De eerdergenoemde losse kaartjestechniek is toegepast, maar de triangulatie is ook bevorderd door te controleren of het antwoord van de respondenten constant bleef, door op een later moment de vragen op een andere manier te stellen. Zo werd eerst een vraag gesteld waarin de term autonomie werd gebruikt en daarna werd dezelfde vraag opnieuw gesteld met de term ‘zelf bepalen’. Daarnaast is sprake geweest van *begripsvalidatie* (Wester, Renckstorf & Scheepers, 2012) door aan de respondenten te vragen wat zij verstaan onder privacy of ‘indringen in iemands leven’. Dit zijn subjectieve concepten die iedereen op een ander manier kan interpreteren. Nadat de interviews zijn afgenomen, is de validiteit verhoogd doordat sprake is geweest van *peer debriefing*. De conceptualisering van de codes en thema’s zijn voorgelegd

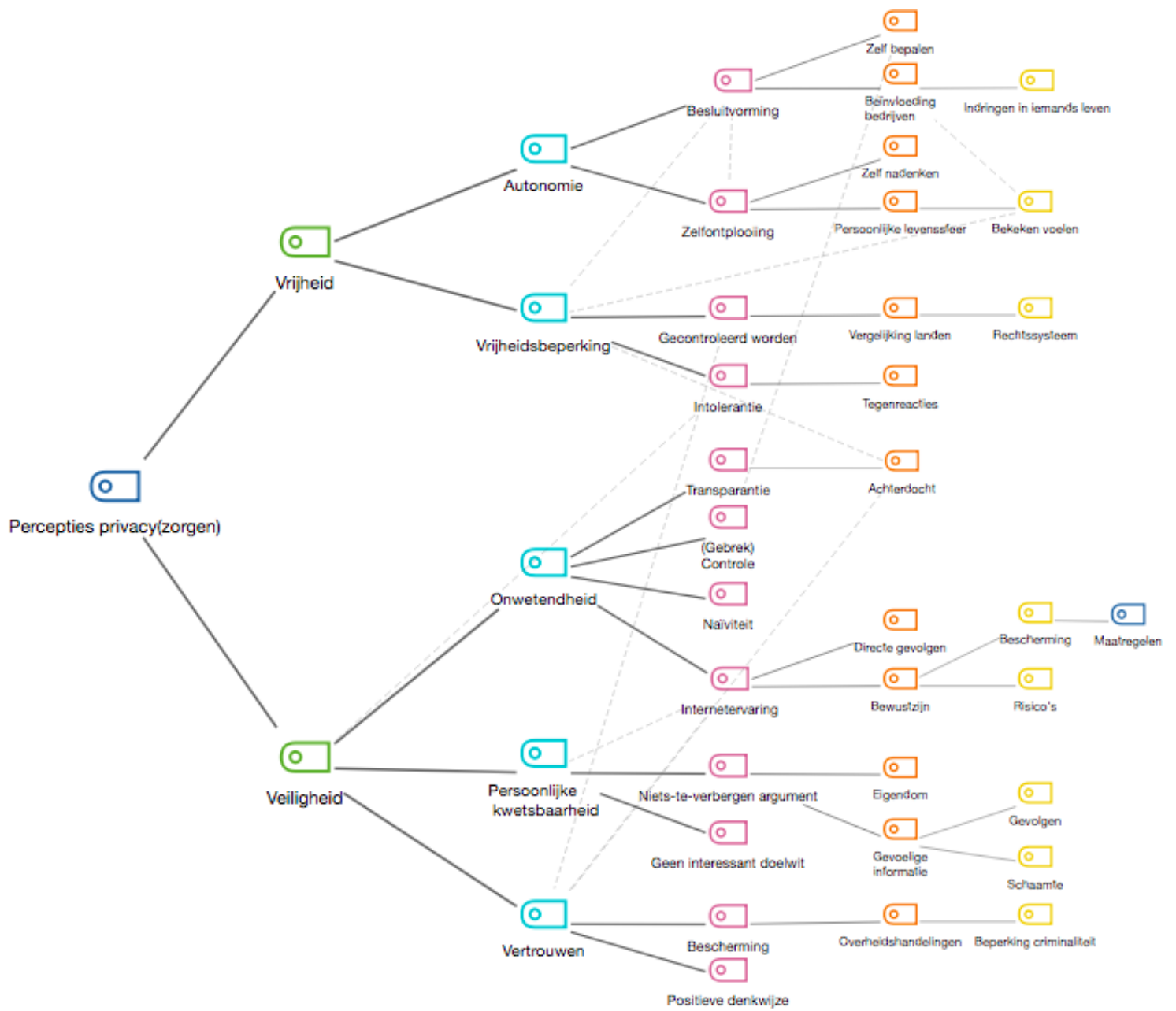
aan een medeonderzoeker. Hiermee is gecontroleerd of de onderzoeker de resultaten op een correcte manier geïnterpreteerd heeft (Peters, 2006). Er kwam onder andere naar voren dat de code ‘persoonlijke relevantie’ op verschillende manieren geïnterpreteerd kon worden. Daarom is deze code veranderd naar ‘persoonlijke kwetsbaarheid’.

Tot slot is gepoogd het onderzoek navolgbaar te maken. Allereerst kunnen de vijf delen van de topiclijst gecontroleerd worden (zie bijlage 1). Deze topiclijst kan gebruikt worden voor een vervolgonderzoek. Daarnaast zijn de interviews opgenomen en getranscribeerd. Hierdoor kan ook de manier waarop de vragen zijn gesteld worden nagegaan. Vervolgens is bij de analyse van de interviews gebruik gemaakt van memo’s, waarbij uitgebreid beschreven en gereflecteerd is waarom bepaalde codes of thema’s gekozen zijn en waarom een verband is weergegeven met andere codes of thema’s (zie bijlage 4). Zo is in de memo’s uitgelegd waarom controle zowel onder vrijheidsbeperking valt als onder onwetendheid. Dit komt niet alleen ten goede aan de navolgbaarheid van het onderzoek (Hijmans & Wester, 2006), maar ook aan de validiteit van het onderzoek. Er wordt namelijk gecontroleerd of de conclusies juist zijn getrokken en geformuleerd.

Hoofdstuk 4: Resultaten

In dit hoofdstuk worden de onderzoeksresultaten uiteengezet. Aan de hand van de analyse van twaalf interviews met Nederlandse internetgebruikers is het concept-indicator model tot stand gekomen (zie Figuur 1). Het model geeft inzicht in de privacypercepties van de twaalf respondenten. De betekenis en het belang van privacy wordt uitgedrukt in termen als: ‘vrijheid’ en ‘veiligheid’. Privacy wordt namelijk gezien als de vrijheid die gebruikers ervaren of als een manier om de vrijheid of veiligheid te beschermen. In het eerste deel van dit hoofdstuk worden de concepten en deelconcepten besproken die onder de themacode ‘vrijheid’ vallen.

Figuur 1. Concept-indicator model



4.1. Vrijheid

Privacy wordt gezien als de ervaren vrijheid van internetgebruikers. Met vrijheid wordt bedoeld dat de internetgebruikers ongestoord en ongezien op een website informatie kunnen opzoeken of hun mening kunnen plaatsen, zonder dat zij daarin beïnvloed worden. Vrijheid is belangrijk, omdat dit een waarde is waar de internetgebruikers in de westerse samenleving mee zijn opgegroeid. Om deze vrijheid te ervaren, is het voor de internetgebruikers belangrijk dat zij zich een autonoom persoon voelen én dat zij niet beperkt worden in hun vrijheid.

4.1.1. Autonomie

Om zich een autonoom persoon te voelen, moet sprake zijn van een gevoel van keuzevrijheid op het internet. Dit betekent dat de internetgebruikers niet altijd persoonlijke content willen ontvangen. Door persoonlijke content te ontvangen hebben de internetgebruikers namelijk het gevoel dat bedrijven bepalen welke informatie aansluit bij hun interesses en dat zij hier minder keuze in hebben. Hierdoor wordt minder autonomie ervaren. Dit wordt door de internetgebruikers als een privacyzorg gezien, aangezien persoonlijke gegevens verzameld worden om het internetgedrag te beïnvloeden. Deze beïnvloeding is vervolgens storend, omdat zowel iemands besluitvorming als zijn/haar zelfontplooiing onder druk komt te staan. Dit heeft weer zijn weerslag op de autonomie en de vrijheid.

4.1.1.1. Besluitvorming

Er zijn meerdere redenen waarom de internetgebruikers het vervelend vinden als de besluitvorming en daarmee ook de autonomie onder druk komt te staan. Allereerst voelt het voor de internetgebruikers alsof er ingedrongen wordt in hun leven als bedrijven anticiperen op hun zoekgedrag. Dit kan middels gerichte advertenties. Met ‘indringen in iemands leven’ wordt bedoeld dat bedrijven informatie krijgen over de gebruikers. Dit voelt voor de gebruikers alsof de bedrijven te dichtbij komen in hun leven. Er zijn ook internetgebruikers die vinden dat ‘indringen in iemands leven’ pas van toepassing is als sprake is van menselijk contact. Dit geldt dus niet voor internetgebruik. Waar de internetgebruikers wel eenduidig over zijn, is dat het ‘indringen in iemands leven’ aan de orde is als ongevraagd dingen gebeuren. Een voorbeeld hiervan is als gebruikers ongevraagd reclame aangeboden krijgen. Dit voelt frustrerend. Ten eerste omdat internetgebruikers hier niet op zitten te wachten, aangezien zij niet zelf de keuze hebben gemaakt omtrent het ontvangen van ongewenste reclame. Ten tweede hebben gebruikers het gevoel dat zij de controle verliezen. Vanwege deze redenen is een link gemaakt tussen ‘zelf bepalen’ en ‘controle’. Het ervaren van controle draagt eraan bij dat gebruikers

autonomie en daarmee vrijheid ervaren. In het volgende citaat legt de gebruiker de betekenis van privacy uit in termen van controle. Als wordt gevraagd waarom dit zo belangrijk voor haar is, legt zij uit dat zij door de controle, vrijheid ervaart.

G12: Het woordje controle, dat jij controle hebt en niet iemand anders macht over jou heeft. Dat vind ik wel privacy, dat jij daar controle over hebt en kan doen en kan gaan staan en dat niemand je daarin kan beïnvloeden eigenlijk.

I: Vind je dat belangrijk?

G12: Ja dat vind ik wel heel belangrijk.

I: Waarom vind je dat belangrijk?

G12: Dat is vrijheid en vrijheid is één van de belangrijkste dingen, voor mij (vrouw, 27 jaar).

Als bedrijven geen rekening houden met deze principes en de internetgebruikers beïnvloeden, voelt het voor de internetgebruikers alsof een inbreuk wordt gemaakt op de controle die zij hebben. Dat komt omdat internetgebruikers hierdoor het gevoel krijgen dat zij niet serieus genomen worden. Hieraan ligt ten grondslag dat zij niet de mogelijkheid hebben zelf beslissingen te kunnen nemen met betrekking tot de informatie die zij wel of niet willen ontvangen. Bedrijven doen dit immers al voor hen. Daarnaast geeft dit het gevoel alsof zij niet zelf kunnen nadenken. Het zelf nadenken is belangrijk, omdat dit een manier is om tot zelfontplooiing te komen.

4.1.1.2. Zelfontplooiing

Met zelfontplooiing wordt bedoeld dat internetgebruikers zelf kunnen en willen nadenken om zichzelf te ontwikkelen. Dit hoeven bedrijven niet voor hen te doen, wat zij volgens de internetgebruikers nu wel doen met gerichte advertenties die hun autonomie beperken. Dit is dan ook onder andere de reden waarom gebruikers waarde hechten aan hun persoonlijke levenssfeer. Persoonlijke levenssfeer wil zeggen dat gebruikers de ruimte hebben om op het internet rond te surfen, zonder dat hun internetgedrag gevolgd wordt door bedrijven. Het is dus een ruimte waarin zij alleen kunnen zijn. Wanneer zij zich beïnvloed voelen door bedrijven met gerichte advertenties voelt dit alsof de persoonlijke levenssfeer beperkt wordt. Dit gaat ten koste van de zelfontplooiing en de vrijheid die iemand ervaart:

G7: Privacy dat er respect en ruimte is om jezelf, als identiteit te ontplooiën en daar heb je die ruimte voor nodig, die vrijheid nodig (man, 44 jaar).

4.1.2. Vrijheidsbeperking

Ondanks dat de vrijheid zo belangrijk is voor de internetgebruikers, ervaren zij soms dat hun vrijheid beperkt wordt. Bijvoorbeeld wanneer zij gecontroleerd worden door de commerciële bedrijven of door de overheid, maar ook als zij hun mening niet durven te uiten op het internet, omdat zij in hun beleving leven in een intolerante samenleving.

4.1.2.1. Gecontroleerd worden

Opmerkelijk is dat de perceptie van de internetgebruikers ten aanzien van hun internet privacy, gedeeltelijk tot stand komt door de mate waarop Nederland sociale controle uitoefent op de internetgebruikers. Zij nemen dit land als uitgangspunt voor hun perceptie, maar benoemen dat deze perceptie nog weleens anders kan zijn als ze woonden in landen als China of Rusland. Dit zijn volgens de internetgebruikers namelijk landen waarin de internet privacy nog meer beperkt wordt dan in Nederland, omdat de overheid de burgers daar meer controleert. In het volgende citaat legt een internetgebruiker uit dat de privacy en dus ook de vrijheid zodanig belangrijk voor hem is, dat hij niet bereid is om naar China te gaan. Hij denkt dat hij daar meer het risico loopt om gecontroleerd te worden op zijn online gedrag.

G8: Dat is voor mij al een reden om niet naar China te reizen, je weet dat je daar de grotere kans loopt om gecheckt te worden of je doet wat je hoort te doen. En gewoon het idee dat mensen je mening kunnen bepalen of onderdrukken. Niet zozeer nu in Nederland (man, 33 jaar).

4.1.2.2. Intolerantie

Hoewel sommige internetgebruikers vinden dat meer sprake is van internet privacy in Nederland vergeleken met andere landen, ervaren andere gebruikers juist minder internet privacy doordat zij wonen in Nederland. Sommige internetgebruikers zien Nederland namelijk als een intolerante samenleving. Hiermee wordt bedoeld dat zij polarisatie ervaren. Zij vrezen dat er groepen mensen zijn die hun mening niet zullen accepteren. Deze gebruikers zijn bang voor onprettige reacties en durven daardoor niet alles wat zij denken en voelen zomaar op het internet te gooien. Dit is dan ook de reden waarom zij waarde hechten aan hun privacy. Privacy is een manier om hun mening te beschermen:

G7: Ja en die privacy die beschermt dan in wezen dat die mening die ik heb dat die niet de hele wereld rond gaat (man, 44 jaar).

De internetgebruikers voelen zich door de mogelijke tegenreacties kwetsbaar op het moment dat zij hun mening wel op het internet publiceren. Het kwetsbare gevoel dat het teweegbrengt,

zorgt ervoor dat de internetgebruikers zich onveilig voelen. Om deze reden is in het concept-indicator model een verband weergegeven tussen ‘intolerantie’ en ‘veiligheid’.

4.2. Veiligheid

Naast dat de internetgebruikers hun vrijheid belangrijk vinden, vinden zowel de internetgebruikers die zich geen zorgen maken over hun privacy als de internetgebruikers die zich wel zorgen maken, hun veiligheid erg belangrijk. Met veiligheid wordt bedoeld dat zij willen dat hun persoonsgegevens veilig gewaarborgd zijn en niet in handen komen van onbevoegden, zoals criminelen. Met andere woorden willen zij dat correct wordt omgegaan met hun persoonsgegevens. Als zij weten dat dit niet gebeurt, zorgt dit ervoor dat de internetgebruikers zich onveilig voelen. Dit heeft te maken met de gevolgen die het mogelijk teweegbrengt. De mate waarin de internetgebruikers dit onveilige gevoel ervaren, zorgt ervoor dat zij zich wel of geen zorgen maken over hun privacy. De gepercipieerde veiligheid hangt af van de onwetendheid, de persoonlijke kwetsbaarheid en het vertrouwen dat de internetgebruikers hebben in bedrijven.

4.2.1. Onwetendheid

Opvallend is dat de internetgebruikers zelf aankaarten dat zij zich onwetend voelen. Onwetendheid betekent ten eerste dat internetgebruikers niet weten wat bedrijven met hun persoonsgegevens doen en ten tweede dat internetgebruikers niet weten hoe zij hun persoonsgegevens moeten beschermen. Wanneer de internetgebruikers benoemen hoeveel kennis zij hebben, baseren zij hun kennis veelal op verhalen van vrienden of verhalen die zij in de media lezen. Zij vinden het belangrijk om op de hoogte te zijn van deze verhalen, omdat zij zich door de onwetendheid achterdochtig voelen en het gevoel krijgen dat zij de controle uit handen geven. Dit zorgt voor een onveilig gevoel. Anderzijds zijn er ook internetgebruikers die juist minder willen weten en het niet erg vinden naïef te zijn. Niet omdat zij geen waarde hechten aan hun gevoel van veiligheid, maar juist omdat zij denken zich onveilig te voelen wanneer zij meer kennis hebben over de risico's die gepaard gaan met online handelingen.

4.2.1.1. Controle

Eerder werd besproken dat internetgebruikers het gevoel hebben dat zij gecontroleerd worden door bedrijven, maar dat wordt niet met deze vorm van controle bedoeld. Controle betekent in de context van veiligheid dat internetgebruikers controle over de eigen persoonsgegevens willen hebben, omdat dit een gevoel van veiligheid geeft. Controle geeft namelijk overzicht

over de manier waarop de persoonsgegevens beschermd zijn en dat is belangrijk, omdat het internet als grenzeloos wordt ervaren. Grenzeloos kan in dit onderzoek op twee manieren geïnterpreteerd worden. Allereerst wordt met grenzeloos bedoeld dat privacy voor internetgebruikers een breed concept is en niet uit te leggen is in eenduidige termen. Ten tweede wordt met grenzeloos bedoeld dat de technologie zo snel gaat, dat de gebruikers minder grip hebben op hun online privacy dan op de offline privacy. Deze internetgebruikers die een verschil zien tussen online en offline privacy, vinden vooral dat online meer risico is op misbruik van de persoonsgegevens. Dit roept een onveilig gevoel op bij de internetgebruikers. Opmerkelijk is dat dit gebrek aan controle voortkomt uit onwetendheid. Wanneer onwetendheid is over de manier waarop internetgebruikers controle kunnen hebben over hun persoonsgegevens, ontstaan zorgen over hun internet privacy. De gebruikers die ervan overtuigd zijn dat zij wel voldoende kennis hebben om zichzelf te beschermen, maken zich daarentegen minder zorgen. Het volgende citaat illustreert dat een internetgebruiker zich geen zorgen maakt over de veiligheid van zijn persoonsgegevens op het internet, omdat hij het idee heeft dat hij zijn gegevens voldoende beschermt:

G5: Als diegene op mijn naam bepaalde financiële transacties uit zou willen voeren, dan kan dat met die gegevens. En dat zullen alleen mensen doen met de verkeerde bedoeling.

I: Maak je je daar zorgen over dat dat gebeurt?

G5: Nee, eigenlijk helemaal niet. Omdat ik denk dat ik alles goed heb beveiligd met wachtwoorden en gegevens.

4.2.1.2. Transparantie

Om de controle en kennis te verhogen is het voor de internetgebruikers belangrijk dat bedrijven meer open zijn over hoe met hun gegevens wordt omgegaan. Hierdoor wordt het gemakkelijker om eventuele maatregelen te nemen als zij weten dat bedrijven op een onprettige en onveilige manier met hun gegevens omgaan. Door de onderzoeker is gevraagd of dit betekent dat zij meer transparantie willen, maar opvallend is dat door een internetgebruiker benoemd werd dat zij juist geen transparantie wil. Transparantie betekent voor deze internetgebruiker namelijk dat zij geïnformeerd wordt over alle details van de gegevensbehandeling van een bedrijf.

I: Je zegt dus: ik vind het belangrijk om te weten wat bedrijven met mijn gegevens doen, maar transparantie vind je niet belangrijk. (...). Waar ligt dan voor jou het onderscheid tussen weten wat bedrijven met jouw gegevens doen en transparantie?

G12: Transparantie is alles, ook tot elk millimeter detail laten zien wat ze doen (vrouw, 27 jaar).

De reden dat de bovenstaande internetgebruiker geen transparantie wil, is omdat zij dit te veel informatie vindt om op te nemen. Niet alle respondenten zijn het eens met de bovenstaande internetgebruiker en willen wél meer transparantie. Echter, zij definiëren transparantie op een andere manier. Deze internetgebruikers verstaan onder transparantie dat bedrijven globaal laten weten hoe de verzameling en verwerking van persoonsgegevens werkt. Dit is dan ook de reden waarom de privacyverklaringen niet transparant worden ervaren, maar juist gebruiksonvriendelijk. Het kost tijd en energie om dit te lezen en te begrijpen, waardoor de internetgebruikers geen idee hebben wat met hun persoonsgegevens gebeurt. De gebruiksonvriendelijke verklaringen maken de internetgebruikers achterdochtig. Zij denken dat deze met opzet lang en ingewikkeld zijn, omdat in die verklaringen wellicht informatie staat waarvan bedrijven liever niet willen dat internetgebruikers het gaan lezen. Om te zorgen dat de internetgebruikers meer het gevoel krijgen dat hun persoonsgegevens veilig zijn op het internet, waarderen de gebruikers een korte samenvatting van een half A4'tje. In deze verklaringen moet vooral duidelijk worden gemaakt waar de gegevens terecht komen. Dit draagt eraan bij dat zij zich minder onwetend voelen.

4.2.1.3. Naïviteit

Het is opmerkelijk dat er ook een groep internetgebruikers is die zich juist minder zorgen maakt door de onwetendheid. Zij willen juist niet weten wat de risico's zijn, omdat zij zich hierdoor meer zorgen maken over hun online privacy. De volgende quote geeft weer hoe een internetgebruiker dit ervaart:

I: En zou jij graag willen weten wat bedrijven met jouw gegevens doen?

G1: Ik denk dat ik het liever niet wil weten. Nou ja, het is misschien heel naïef. Maar soms moet je gewoon dingen niet willen weten. Nou ja, omdat hoe meer je weet, hoe meer je ziet, hoe meer je je druk gaat maken en dan wordt het een ding en dan ga je er last van krijgen (vrouw, 35 jaar).

De gebruikers die hun ogen sluiten voor de risico's, benoemen wel dat ze zich naïef voelen. Een aantal van hen ziet dit niet als een positieve ontwikkeling, omdat zij hierdoor het gevoel hebben dat zij niet de verantwoordelijkheid nemen voor de veiligheid van hun persoonsgegevens. Zij benoemen dat zij niet onbezonnen door het leven willen. Er is niet voldoende doorgevraagd wat hiermee bedoeld wordt.

4.2.2.1. Internetervaring

Tot slot komt de onwetendheid terug wanneer de internetgebruikers spreken over hun ervaringen op het internet. Met internetervaringen worden zowel de eigen ervaringen bedoeld, als de ervaringen van vrienden of de mediaberichten die zij lezen. Het zijn meestal negatieve ervaringen die zij gehoord hebben. Alhoewel uit de interviews niet duidelijk naar voren komt in hoeverre zij zich verdiept hebben in deze verhalen, krijgen zij hierdoor wel het gevoel dat hun persoonsgegevens onveilig zijn. Dit zorgt voor een verhoogd bewustzijn over de manier waarop met de persoonsgegevens wordt omgegaan. Door dit bewustzijn hebben sommige internetgebruikers maatregelen genomen om hun privacy te beschermen, zoals het afschermen van de webcam. Ook wordt soms informatie incognito opgezocht. Dit betekent dat op een anonieme browser informatie op wordt gevraagd. Bij de vraag of het een reële kans is dat hun persoonsgegevens onveilig zijn als zij de maatregelen niet nemen, benoemen sommige internetgebruikers dat zij, wanneer zij rationeel nadenken, de kans irreëel inschatten dat iets gebeurt met hun persoonsgegevens. De reden dat zij alsnog de maatregelen nemen, is uit voorzorg om de mogelijke risico's te voorkomen:

I: Maar als je het rationeel toch niet waarschijnlijk vindt?

G8: Ja dat zijn hele goede vragen. Maar met heel veel dingen is het zo dat de kans dat het gebeurt niet zo groot is, maar toch verzeker je ervoor. De kans dat mijn huis in brand komt is heel klein, maar toch verzeker je ervoor (man, 33 jaar).

Er bestaan vele mogelijke risico's omtrent het misbruik van persoonsgegevens op het internet, zoals dat onbevoegden toegang krijgen tot de gegevens of dat een vertekend beeld ontstaat wanneer zij bepaalde informatie opzoeken. Zij vrezen dat, indien zij informatie over bijvoorbeeld wapens opzoeken, het verkeerd geïnterpreteerd wordt door de overheid. Ondanks dat zij niet weten hoe het allemaal precies zit, bestaat volgens hen de mogelijkheid dat zij geprofileerd worden tot een terrorist als zij informatie uit nieuwsgierigheid opzoeken. Vooral de internetgebruikers met een islamitische achtergrond achten de kans groot dat op een negatieve manier een vertekend beeld van hen ontstaat. Zij zijn eerder geneigd de hiervoor genoemde maatregelen te nemen om hun gevoel van veiligheid te waarborgen.

Aan de andere kant zijn er ook internetgebruikers die hun internetgedrag niet aanpassen, omdat zij dit onnodig vinden als zij geen verkeerde intenties hebben of omdat zij de directe gevolgen niet ondervinden. Onderstaande citaat illustreert dat de mediaverhalen zorgen voor een hoger bewustzijn. Desondanks is dit voor de gebruiker niet voldoende om zich daadwerkelijk zorgen te maken of zich onveilig te voelen:

G3: Maar aan de andere kant geef ik er ook te weinig om er echt dagelijks bij stil te staan, maar zo af en toe... Toevallig als je het erover hebt of ergens voorbij ziet komen. Maar het is niet dat ik er echt bij stil sta van oh shit nu hebben ze het weer hoeveel gegevens van me. Dat ook weer totaal niet eigenlijk (vrouw, 23 jaar).

4.2.3. Persoonlijke kwetsbaarheid

Naast de mate van onwetendheid die bepaalt hoe (on)veilig de internetgebruikers zich voelen, wordt de persoonlijke kwetsbaarheid ook meegenomen wanneer de internetgebruikers uitleggen of ze denken dat hun internet privacy al dan niet gewaarborgd is. Met persoonlijke kwetsbaarheid wordt bedoeld in hoeverre internetgebruikers denken dat er een vergrote kans is dat misbruik van hun persoonsgegevens wordt gemaakt. Zo denken de internetgebruikers dat dit meer het geval is als zij iets te verbergen zouden hebben of als zij om diverse redenen mogelijk een interessant doelwit zijn voor criminelen. Als de internetgebruikers ervaren dat zij een interessant doelwit zijn voor criminelen, voelen zij zich minder veilig.

4.2.2.2. Niets-te-verbergen argument

Als het gaat om het niets-te-verbergen argument, nuanceren de internetgebruikers dat zij geen illegale zaken te verbergen hebben. Als wordt doorgevraagd of dit dus betekent dat het hen niet uitmaakt als legale informatie, zoals de rekeninggegevens, openbaar wordt gesteld, blijkt dat er wel informatie is die zij liever voor zichzelf willen houden. Ten eerste heeft dat ermee te maken dat zij waarde hechten aan hun eigendom en dus ook aan hun persoonsgegevens. Het volgende citaat geeft weer dat de gebruiker er niet op zit te wachten dat iedereen haar persoonsgegevens ziet:

I: Maar als je dan toch niets te verbergen hebt, waarom wil je weten wat mensen wel en niet over jou weten?

G11: Omdat dat van mij is. Dat gaat over mij, dus ik vind niet dat iedereen dat hoeft te zien of te weten (vrouw, 22 jaar).

Ten tweede willen de internetgebruikers met name de privacygevoelige informatie voor zichzelf houden, omdat dit negatieve gevolgen met betrekking tot hun veiligheid teweeg kan brengen. Of iets als privacygevoelig wordt ervaren, heeft niet alleen te maken met de negatieve gevolgen, maar ook met het gevoel van schaamte. Medische gegevens worden bijvoorbeeld als privacygevoelig ervaren, omdat zij zich daarvoor kunnen schamen als dit aan iedereen wordt blootgesteld. Wat betreft de gevolgen, worden de reeds besproken intolerantie en de negatieve

tegenreacties bedoeld, maar ook de fysieke veiligheid. Een aantal internetgebruikers werkt in de zorg met criminele cliënten. Zij vrezen dat wanneer hun adresgegevens openbaar worden gesteld, het door de cliënten tegen hen gebruikt kan worden. Mogelijkerwijs heeft dit uiteindelijk gevolgen voor de fysieke veiligheid. Hieruit blijkt dat de werksector de perceptie ook beïnvloedt.

4.2.2.3. Interessant doelwit

Bovendien denken de internetgebruikers die in de zorgbranche werken dat een grotere kans bestaat dat mensen hun persoonsgegevens op het internet controleren. Met andere woorden, zij voelen zich eerder een interessant doelwit dan de mensen die niet in de zorg werken. Met interessant doelwit wordt bedoeld dat internetgebruikers de kans groter achten dat de overheid of criminelen hun persoonsgegevens natrekken, omdat zij bijvoorbeeld veel geld op hun bankrekening hebben staan. Ook kunnen internetgebruikers zich eerder een interessant doelwit voelen, omdat zij denken dat zij aan een aantal kenmerken van een crimineel voldoen. Zoals reeds besproken schatten internetgebruikers met een islamitische achtergrond de kans groter in dat zij een interessant doelwit zijn om nagetrokken te worden. Om deze reden is een verband weergegeven tussen persoonlijke kwetsbaarheid en de eigen ervaringen. Wanneer internetgebruikers deze kans groter schatten, voelen zij zich onveiliger op het internet.

Daarentegen zijn er ook internetgebruikers die er juist van overtuigd zijn dat de kans klein is dat hun gegevens misbruikt worden. Onderstaande citaat geeft een duidelijk voorbeeld weer van een internetgebruiker die niet denkt dat haar persoonsgegevens misbruikt worden door een gebrek aan persoonlijke kwetsbaarheid:

G5: (...), maar ik denk ook niet dat het bij mij zo snel kan gebeuren, ook omdat ik, het is niet dat ik ruzie heb met mensen of mensen kwaad heb gedaan waardoor ze het bij mij kunnen doen. En ik ben ook niet een interessant doelwit om het zo maar te zeggen, dus geen belangrijk of bekend persoon (man, 24 jaar).

De respondent heeft er voldoende vertrouwen in dat hij geen interessant doelwit is, waardoor hij zich veilig voelt.

4.2.3. Vertrouwen

Vertrouwen is een belangrijk aspect wanneer de internetgebruikers een afweging maken of hun persoonsgegevens op het internet veilig zijn. Met vertrouwen wordt bedoeld dat internetgebruikers geloven dat andere internetgebruikers, bedrijven en/of de overheid op een veilige en correcte manier met hun persoonsgegevens omgaan. De internetgebruikers

benoemen wel dat zij vooral vertrouwen hebben in de overheid, omdat zij denken dat de overheid de burgers wil beschermen en de criminaliteit wil beperken. Dit maakt dat de internetgebruikers eerder bereid zijn hun persoonsgegevens te verstrekken aan de overheid. Zelfs als de gebruikers privacygevoelige informatie moeten verstrekken, zullen zij dit doen voor het belang van de veiligheid. De internetgebruikers benoemen namelijk dat de veiligheid als meer belangrijk wordt ervaren dan de internet privacy.

Desondanks zijn er wel een aantal internetgebruikers die zich naïef voelen als zij zeggen dat zij denken dat de overheid de veiligheid waarborgt. Dit gevoel van naïviteit komt ook terug als internetgebruikers benoemen dat zij uitgaan van het goede in de mens en denken dat er een kleine groep is die misbruik wil maken van de persoonsgegevens. Aangezien het vertrouwen dat de internetgebruikers hebben vaak gepaard gaat met het gevoel van naïviteit, is er een verband weergegeven tussen 'vertrouwen' en 'naïviteit'.

Hoofdstuk 5: Conclusie en discussie

In dit hoofdstuk wordt aan de hand van de deelvragen de onderzoeksvraag beantwoord. Vervolgens wordt gereflecteerd op het huidige onderzoek, gevolgd door een aantal aanbevelingen voor vervolgonderzoek.

5.1. Conclusie

Het doel van deze studie is inzicht te krijgen in de belevingswereld van internetgebruikers ten aanzien van hun privacyzorgen op het internet. Hierop aansluitend is de volgende onderzoeksvraag opgesteld: *Welke percepties hebben Nederlandse internetgebruikers ten aanzien van privacy(zorgen) op het internet?* Om deze onderzoeksvraag te beantwoorden, zijn verschillende deelvragen opgesteld.

De eerste deelvraag van dit onderzoek heeft betrekking op de betekenis van internet privacy voor de internetgebruikers. Op basis van de analyse van twaalf interviews komt naar voren dat internet privacy een subjectief concept is, omdat het uitgedrukt wordt in diverse betekenissen. Privacy wordt namelijk beschreven als de controle of de autonomie die de internetgebruikers hebben over hun persoonsgegevens, maar het wordt ook gezien als de ruimte en vrijheid om alleen te zijn zonder bemoeienis van anderen. Dat privacy een subjectief concept is, komt overeen met eerdere onderzoeken waarin wetenschappers privacy op verscheidene manieren definiëren (Blok, 2002; Cuijpers, 2007; Westin, 1968). Desondanks is in dit onderzoek het verschil tussen online en offline privacy uitgediept wat in eerdere onderzoeken nog niet is gedaan. Zo blijkt dat de kans groter wordt geschat dat de online privacy in het geding komt dan de offline privacy, omdat internetgebruikers minder grip ervaren op hun online privacybescherming. Echter, er kan niet direct geconcludeerd worden dat de betekenis van privacy hierdoor verandert. Er kan louter geconcludeerd worden dat de internetgebruikers meer mogelijke risico's ervaren op het internet. Dit komt gedeeltelijk overeen met de studie van Nissenbaum (2011). Volgens zijn studie verandert de betekenis van privacy niet door de technologische ontwikkelingen. Desalniettemin nuanceert hij niet dat internetgebruikers wel het gevoel hebben dat er online vaker diverse risico's voorkomen.

De tweede deelvraag en de derde deelvraag worden tegelijkertijd behandeld, omdat uit de analyse van de interviews blijkt dat deze twee deelvragen met elkaar overlappen. De tweede deelvraag heeft namelijk betrekking op de ervaren privacyzorgen en de derde deelvraag heeft betrekking op de redenen waarom de internetgebruikers zich wel of geen zorgen maken over hun internet privacy. Het blijkt dat er twee belangrijke privacyzorgen zijn. De eerste privacyzorg is dat sommige internetgebruikers vrezen dat zij door een gebrek aan privacy

onvoldoende vrijheid ervaren op het internet. De redenen waarom de internetgebruikers zich wel of geen zorgen maken over hun vrijheid, hangt ten eerste af van de mate waarop zij vrezen voor vrijheidsbeperking. Dit kan in de vorm van negatieve reacties van buitenstaanders die het niet eens zijn met de mening van de internetgebruikers, waardoor de internetgebruikers het gevoel hebben dat hun meningsvrijheid in het geding komt. De tweede reden waarom de internetgebruikers zich wel of geen zorgen maken over hun vrijheid, hangt af van de mate van de autonomie die zij ervaren op het internet. Als zij onvoldoende keuzevrijheid ervaren, maken zij zich meer zorgen. Alhoewel in de *Taxonomy of Privacy* betwijfeld wordt of een inbreuk op de autonomie beschouwd moet worden als een privacyzorg (Solove, 2006), blijkt uit de huidige studie dat een inbreuk op de autonomie een duidelijk onderdeel is van de privacyzorgen. Wanneer bedrijven namelijk persoonsgegevens verzamelen en de keuzes beperken door persoonlijke content aan te bieden, wordt inbreuk gemaakt op de autonomie. Dit wil dus zeggen dat de twee problemen niet los van elkaar kunnen worden gezien, omdat het verzamelen en verwerken van de persoonsgegevens een voorwaarde is om inbreuk op de autonomie te ervaren.

De tweede privacyzorg is dat sommige internetgebruikers vrezen dat zij door een gebrek aan privacy onvoldoende veiligheid ervaren. De redenen waarom de internetgebruikers zich zorgen maken over hun veiligheid op het internet, is omdat zij onvoldoende vertrouwen hebben in bedrijven of omdat zij denken dat zij een interessant doelwit zijn voor de overheid door hun (etnische) achtergrond. Hierdoor kunnen de internetgebruikers zich kwetsbaar voelen. Als er voldoende vertrouwen en een gebrek aan kwetsbaarheid ervaren wordt, maken de internetgebruikers zich minder zorgen over hun internet privacy. Dat de persoonlijke kwetsbaarheid een reden is om zich wel of geen zorgen te maken over de internet privacy, is voor zover bekend nooit eerder aangekaart in eerder onderzoek. Daarnaast ervaren internetgebruikers onvoldoende veiligheid als zij onwetend zijn omtrent de omgang van bedrijven met hun persoonsgegevens. De reden dat de internetgebruikers zich door de onwetendheid onveilig voelen, komt doordat zij een gebrek aan controle ervaren. Het belang van controle voor internetgebruikers is in de literatuur al eerder aangekaart (Barth & De Jong, 2017). Desondanks is nooit duidelijk geworden waarom het hebben van controle zo belangrijk is voor de internetgebruikers. Uit het huidige onderzoek blijkt dat controle belangrijk is, omdat controle hebben, zorgt voor overzicht over wat er met hun persoonsgegevens gebeurt. Overzicht geeft vervolgens een gevoel van veiligheid.

Hierop aansluitend zou een vervolgonderzoek zich kunnen richten op hoe de kennis van de Nederlandse internetgebruikers omtrent de privacykwesties verhoogd kan worden, zodat zij meer controle en daarmee meer veiligheid ervaren. Hierbij moet wel de kanttekening gemaakt

worden dat niet alle internetgebruikers behoefte hebben aan meer kennis. Onwetendheid kan er namelijk ook voor zorgen dat internetgebruikers geneigd zijn te denken dat hun persoonsgegevens op het internet veilig zijn. Dit komt omdat zij niet op de hoogte zijn van de mogelijke risico's, waardoor zij zich hier ook geen zorgen over maken. Dat onwetendheid met betrekking tot de persoonsgegevens bijdraagt aan gevoelens van veiligheid, is nergens in eerdere onderzoeken terug te vinden.

Bij bovenstaande twee deelvragen moet de nuance gemaakt worden dat 'zorgen' een breed concept is. In de interviews lopen de termen zorgen en bewustzijn door elkaar. Er kan geen antwoord op de vraag gegeven worden waar het onderscheid precies ligt, maar het zet wel twijfels bij de vraag of de hele privacydiscussie daadwerkelijk gaat over zorgen, of dat het meer een bewustzijn is dat af en toe komt opdagen over wat er nu eigenlijk precies met de persoonsgegevens gebeurt.

Samengevat kan geconcludeerd worden dat de perceptie van de Nederlandse internetgebruikers met betrekking tot internet privacy veelal geleid wordt door onwetendheid. Deze onwetendheid speelt een grote rol in de mate waarop internetgebruikers vrijheid en veiligheid ervaren op het internet. De betekenis van internet privacy wordt vooral beschreven in de vrijheid die ervaren wordt. De term vrijheid komt ook terug als de Nederlandse internetgebruikers het belang van internet privacy benadrukken: door de privacy voelen internetgebruikers zich vrij, maar ook veilig. Dit is een bevinding die niet expliciet naar voren is gekomen in eerder onderzoek.

5.2. Discussie

Het onderzoek kent een aantal beperkingen die mogelijk de resultaten gedeeltelijk gevormd hebben. Allereerst is er te weinig sprake geweest van onderzoekertriangulatie (Wester, Renckstorf & Scheepers, 2012). Alhoewel een medestudente mee heeft gekeken naar een aantal gecodeerde fragmenten en het concept-indicator model, zou de validiteit van het onderzoek beter gewaarborgd zijn als meerdere onderzoekers betrokken waren bij de analyse van de onderzoeksresultaten. In een vervolgonderzoek wordt daarom aangeraden om met meerdere medeonderzoekers samen te werken.

Een tweede beperking van het onderzoek heeft betrekking op de steekproef: de Nederlandse internetgebruikers. Het is van belang geweest een zo breed mogelijk publiek te interviewen om een representatief beeld te krijgen van het verschijnsel dat onderzocht is (Hijmans & Wester, 2006), namelijk de percepties van deze internetgebruikers omtrent hun internet privacy. Desondanks zijn er nauwelijks senioren geïnterviewd. Mogelijkerwijs is er een

verschil tussen de percepties van jongeren en de percepties van burgers die niet zijn opgegroeid in het digitale tijdperk. Dit haakt aan op het volgende punt: deze studie heeft zich louter gericht op internetgebruikers, maar wellicht zijn er burgers die geen internet gebruiken omdat zij er niet mee zijn opgegroeid of omdat zij dit niet willen door mogelijke privacyzorgen. Het kan interessant zijn om deze doelgroep in een vervolgonderzoek mee te nemen. Ten eerste brengt hun perceptie mogelijk nieuwe inzichten met zich mee, maar ten tweede horen zij bij de Nederlandse samenleving en hebben zij ook een stem in het doorvoeren van privacywetten en in discussies over privacy.

Een ander punt met betrekking tot de geïnterviewde respondenten, is dat het opmerkelijk is geweest dat het ‘niets-te-verbergen’ argument een aantal keer werd aangekaart. Vooral als de internetgebruikers niets illegaals te verbergen hebben, maken zij zich minder zorgen over hun privacy. Dit roept de vraag op of deze perceptie ook geldt voor mensen met bijvoorbeeld een strafblad. Maken zij zich meer zorgen over hun internet privacy, omdat zij illegale activiteiten hebben ondernomen? Een suggestie voor vervolgonderzoek is om deze doelgroep ook mee te nemen. Dit kan bijdragen aan een volledig beeld van de percepties van de Nederlandse internetgebruikers met betrekking tot internet privacy.

De laatste beperking van dit onderzoek gaat over de reikwijdte van het onderwerp. Privacy is een complex concept met diverse elementen (Cuijpers, 2007). Alhoewel de onderzoeker gepoogd heeft zoveel mogelijk relevante elementen van privacyaspecten mee te nemen, bleek dat dit zou leiden tot te veel topics voor de interviews. Zo is het door tijdsgebrek niet gelukt om de *Privacy Calculus Theory* (Li et al., 2010) voldoende uit te diepen. Daarom kan geen antwoord worden gegeven op de vraag hoe internetgebruikers de potentiële voordelen en risico's tegen elkaar afwegen bij het verstrekken van de persoonsgegevens of wanneer de voordelen zwaarder wegen dan de nadelen. Het wordt daarom aangeraden om in een vervolgonderzoek meer duidelijkheid te krijgen over de werking van de *Privacy Calculus Theory*.

Ondanks de beperkingen, is deze studie zowel relevant voor de wetenschap als voor de samenleving. Doordat er gebruik is gemaakt van een kwalitatieve onderzoeksmethode, is het duidelijk geworden wat de burgers zelf verstaan onder internet privacy, wat het belang ervan is en wat ervoor zorgt dat zij zich al dan niet zorgen maken over hun internet privacy. Dit zijn onderwerpen die in eerder onderzoek over internet privacy nog niet waren uitgediept. Niet alleen kan deze kennis meegenomen worden voor vervolgonderzoek, maar het heeft ook een bijdrage geleverd aan de maatschappij. Zo heeft dit onderwerp bij de respondenten geleid tot meer bewustzijn over de eigen percepties met betrekking tot de internet privacy. Daarnaast kan

de kennis over de percepties van de internetgebruikers de vorm van de privacydiscussies veranderen. De discussies over internet privacy geven de indruk geven dat de percepties van de internetgebruikers die zich geen zorgen maken verschillen van de percepties van de internetgebruikers die zich wel zorgen maken. Desondanks blijkt uit dit onderzoek dat zij dezelfde waarden delen. Beide groepen vinden namelijk hun vrijheid en veiligheid belangrijk. Wellicht moet het daarom geen discussie meer zijn tussen de ‘voorstanders’ en ‘tegenstanders’, maar moet het een samenwerking worden naar meer veiligheid en vrijheid.

Literatuurlijst

- Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce*, 1(1), 21-29. doi: 10.1145/988772.988777
- Aguirre, E., Mahr, E., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 9(1), 34-49. doi: 10.1016/j.jretai.2014.09.005
- Amnesty. (z.d). *Sleepwet bedreiging voor mensenrechten*. Geraadpleegd op 17 februari 2019, van <https://www.amnesty.nl/mensenrechten-in-nederland/veiligheid-en-mensenrechten/sleepwet>
- Autoriteit Persoonsgegevens. (2017). *Onderzoek naar het verwerken van persoonsgegevens van betrokkenen in Nederland door het Facebook-concern*. Geraadpleegd op 8 maart 2019, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_faceboo.k.pdf
- Autoriteit Persoonsgegevens. (2018). *Algemene verordening gegevensbescherming*. Geraadpleegd op 7 december 2018, van <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg>
- Autoriteit Persoonsgegevens. (2019). *Nederland maakt zich zorgen over privacy*. Geraadpleegd op 16 februari 2019, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/resultaten_enquete_privacyzorgen_jan_2019.pdf
- Avey, J. B., Avolio, B. J., Crossley, C. D., & Luthans, F. (2009). Psychological ownership: Theoretical extensions, measurement and relation to work outcomes. *Journal of Organizational Behavior*, 30(2), 173-191. doi: 10.1002/job.583
- Baek, T. H., & Morimoto, M. (2012). Stay away from me: Examining the determinants of consumer avoidance of personalized advertising. *Journal of Advertising*, 41(1), 59–76. doi: 10.2753/JOA0091-3367410105
- Barth, S., & De Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038-1058. doi: 10.1016/j.tele.2017.04.013

- Becker, M. (2015). *Ethiek van de digitale media*. Amsterdam: Boom.
- Bleier, A. & Eisenbeiss, M. (2015). The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, 91(3), 390–409. doi: 10.1016/j.jretai.2015.04.001
- 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.
- Blumer, H. (1954). What is wrong with social theory? *American Sociological Review*, 19(1), 3-10. doi: 10.2307/2088165
- Boeije, H. (2014). *Analyseren in kwalitatief onderzoek: denken en doen*. Den Haag: Boom.
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, 46(3), 363-376. doi: 10.1080/00913367.2017.1339368
- Braun, V., & Clarke, V. (2013). *Successful Qualitative Research: A practical guide for beginners* (1th ed.). London: Sage Publishing.
- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81(1), 42-51. doi: 10.1016/j.chb.2017.12.001
- Cuijpers, C. M. K. C. (2007). Privacy in context. In J. E. J. Prins, & J. M. A. Berkvens (Eds.), *Privacyregulering in theorie en praktijk* (pp. 7-24). Deventer: Kluwer.
- Cranor, L. F., Reagle, J., & Ackerman, M.S. (1999). Beyond Concern: Understanding Net User's Attitudes About Online Privacy. *AT&T Labs-Research Technical Report*, 1(1), 1-25.
- DDMA. (2018). *Privacy Monitor 2018: Wat consumenten denken*. Geraadpleegd op 19 februari 2019, van <https://ddma.nl/privacy-monitor/>
- Dinev, T., & Hart, C. (2006). An extended privacy calculus model for e-commerce. *Information System Transactions Research*, 17(1), 61-80. doi: 10.1287/isre.1060.0080
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295–316. doi: 10.1057/ejis.2012.23
- Flaherty, D. H. (1999) Visions of Privacy: Past, Present, and Future. In C. J. Bennett & R. Grant (Eds.), *Visions of Privacy: Policy Choices for the Digital Age* (pp. 19-38). Toronto: Toronto Press.
- Hart van Nederland. (2018). *De Sleepwet: hoe zit het nu precies?* Geraadpleegd op 16 februari 2019, van <https://www.hartvannederland.nl/nieuws/2018/de-sleepwet-hoe-zit-het-nu-precies/>

- Hart van Nederland. (2018). *Uitslag referendum sleepwet: meerderheid is tegen*.
Geraadpleegd op 16 februari 2019, van
<https://www.hartvannederland.nl/nieuws/2018/de-sleepwet-hoe-zit-het-nu-precies/>
- Hijmans, E., & Wester, F. (2006). De kwalitatieve interviewstudie. In Wester, F., Renckstorf, K. & Scheepers, P. (Eds.), *Onderzoekstypen in de communicatiewetenschap* (pp. 507-532). Alphen aan de Rijn: Kluwen.
- IIR. (2018). *Vier inspirerende visies op de AVG*. Geraadpleegd op 5 juni 2019, van
<https://iir.nl/blog/vier-inspirerende-visies-op-de-avg/>
- Ketelaar, P.E., Hentenaar, F., & Kooter, M. (2011). *Groepen in focus: in vier stappen naar toegepast focusgroeponderzoek*. Den Haag: Boom.
- Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), 62-71.
doi: 10.1080/08874417.2010.11645450
- Li, H., Sarathy, R., & Xu, H. (2010). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, 51(3), 434-445. doi: 10.1016/j.dss.2011.01.017
- Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power – responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4), 572-585. doi: 10.1007/s11747-006-0003-3
- McDonald, A.M., Cranor, L.F. (2010). Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. *TPRC 2010*, 1(1), 1-28.
- Miyazaki, A. D. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy and Marketing*, 27(1), 19–33. doi: 10.1509/jppm.27.1.19
- Niemantsverdriet, T., & Van den Dool, P. *Ik heb niets te verbergen*. Geraadpleegd op 4 maart 2019, van <https://www.nrc.nl/nieuws/2018/03/17/ik-heb-niets-te-verbergen-a1596044>
- Nissenbaum, H. (2011). Contextual Approach to Privacy Online. *Daedalus*, 140(4), 32-48.
doi: 10.1162/DAED_a_00113
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-120. doi: 10.1111/j.1745-6606.2006.00070.x
- Pavlou, P.A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 35(4), 977-988. doi: 10.2307/41409969
- Peters, V. (2006). De case-studie. In Wester, F., Renckstorf, K. & Scheepers, P. (Eds.),

- Onderzoekstypen in de communicatiewetenschap* (pp. 615-642). Alphen aan de Rijn: Kluwen.
- Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, 16(2), 171-182. doi: 10.1007/s10676-014-9343-8
- Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, 32(1), 15-22. doi: 10.1016/j.chb.2013.11.008
- Solove, D.J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477-560. doi: 10.2307/40041279
- Solove, D. J. (2008). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, 44(289), 745-772.
- Solove, D. J. (2008). *Understanding Privacy*. Londen: Harvard University Press.
- Teunis, H. (2018). *Dit is wat Google en Facebook over jou weten (en zo pas je het aan)*. Geraadpleegd op 22 februari 2019, van <https://www.rtlnieuws.nl/tech/artikel/3909436/dit-wat-google-en-facebook-over-jou-weten-en-zo-pas-je-het-aan>
- TNO. (2015). *Privacy beleving op het internet in Nederland*. Geraadpleegd 22 februari 2019, van <https://repository.tudelft.nl/view/tno/uuid:9ea8a097-d17d-4f50-a910-76059d46aedb>
- Ur, B., Leon, P.G., Cranor, L.F., Shay, R., & Wang, Y. (2012). Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 4(1), 1-11. doi:10.1145/2335356.2335362
- Van Doorn., & Hoekstra, J.C. (2013). Customization of Online Advertising: The Role of Intrusiveness. *Marketing Letters*, 24(4), 339-51. doi: 0.1007/s11002-012-9222-1
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *The Harvard Law Review Association*, 4(5), 193-220. doi: 10.2307/1321160
- Wester, F., & Peters, V. (2009). *Kwalitatieve analyse: Uitgangspunten en procedures (1th ed.)*. Bussum: Coutinho.
- Wester, F., Renckstorf, K. & Scheepers, P. (2012). *Onderzoekstypen in de communicatiewetenschap* Alphen aan de Rijn: Kluwen.
- Westin, A. F. (1968). *Privacy and Freedom*. Geraadpleegd op 11 maart 2019, van <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlu>

Bijlagen

Bijlage 1. Topiclijst

Sensitizing concept: percepties van mensen over de privacyzorgen op het internet.

Hoofdtopics:

- (Internet)privacy
- Aspecten privacyzorgen
- Gedrag van internetgebruikers en achterliggende redenen
- Percepties van mensen die zich geen zorgen maken

Materialen

- Pen en papier
- Laptop
- Opnameapparatuur
- Snacks en drinken

1. Inleiding

- Mezelf voorstellen.
- Benoemen dat het fijn is dat zij meewerken aan mijn onderzoek.
- Benadrukken dat er geen foute antwoorden mogelijk zijn.
- Respondenten op de hoogte stellen dat:
 - Het interview wordt opgenomen voor onderzoeksdoeleinden.
 - Er zullen geen namen gebruikt worden bij het transcriberen.
 - De geluidsopnamen en video-opnamen worden gewist na het onderzoek.
 - Er zullen aantekeningen gemaakt worden over onderwerpen waar ik graag nog meer over wil weten.
 - De respondent mag vragen stellen wanneer iets onduidelijk is.
- Toestemmingsformulier laten ondertekenen.

2. Kennismaking respondent

<p>Doel: De respondent beter leren kennen. Door de respondent beter te leren kennen, geeft dit de mogelijkheid om later door te vragen.</p> <p>Hoofdvraag: Wat voor persoon ben ik aan het interviewen?</p> <p>Startvraag: Om je beter te leren kennen, ben ik benieuwd naar wat je in het dagelijkse leven doet.</p>	Ruimte voor aantekeningen:
<p>Doorvragen:</p> <ul style="list-style-type: none">- Hoe oud ben je?- Wat is je hoogst genoten opleiding?- Waar kom je oorspronkelijk vandaan?- Wat doe je in het dagelijkse leven?- Kijk je veel naar het nieuws of lees je regelmatig de krant? (<i>Wellicht heeft dit invloed op hun belevingswereld</i>).	

3. (Internet)privacy

<p>Doel: Het onderwerp inleiden door te zeggen dat door de technologische ontwikkelingen privacy een veelbesproken onderwerp is in het nieuws. Achterhalen wat het concept privacy bij hen oproept.</p> <p>Hoofdvraag: Wat betekent (internet)privacy voor jou?</p> <p>Startvraag: Wat roept het concept privacy bij je op?</p> <ul style="list-style-type: none">• Losse kaartjestechniek: trefwoorden internet-privacy	Ruimte voor aantekeningen:
<p>Doorvragen:</p> <ul style="list-style-type: none">- Waarom roept het concept (internet)privacy <i>dit</i> bij je op?- Is er een verschil tussen online en offline privacy?	

4. Aspecten privacyzorgen

<p>Doel: Achterhalen wat de privacyzorgen zijn en waarom mensen zich wel of geen zorgen maken over hun internet privacy</p> <p>Hoofdvraag: Welke zorgen ervaren de respondenten als privacyzorgen en waarom zijn deze zorgen er?</p> <p>Startvraag: Kun jij je voorstellen dat mensen zich zorgen maken om hun privacy?</p>	Ruimte voor aantekeningen:
<p>Doorvragen:</p>	

- Percepties dataverzameling:
 - Voelen mensen zich bekeken of ongemakkelijk wanneer zij informatie opzoeken? Waarom voelen mensen zich bekeken of ongemakkelijk?
- Percepties dataverwerking/ data-analyse:
 - Denken mensen dat zij slechts een deel van zichzelf op het internet achterlaten? Hoe ervaren zij dit?
- Percepties dataverspreiding: *ik ga dit uit een voorbeeld uit mezelf uitleggen. Moletov cocktail.*
 - Vinden mensen het problematisch wanneer er een vertekend beeld van hen ontstaat? Waarom?
 - Willen mensen ‘correcte’ informatie voor zichzelf houden? Waarom?
- Percepties ‘indringen in iemands leven’:
 - Hebben mensen het gevoel dat er ingedrongen wordt in hun leven? Wanneer? Hoe wordt dit ervaren?
 - Wat bedoelen zij wanneer zij het hebben over ‘indringen in iemands leven’?
 - Hebben mensen het gevoel dat er inbreuk wordt gemaakt op het ‘recht om alleen te zijn’? Wat bedoelen zij met ‘het recht om alleen te zijn’?
- Wat roept het bij mensen op wanneer data verzameld, geanalyseerd of verspreid wordt?
- Percepties autonomie **Let op: eerst duidelijk krijgen of mensen begrijpen wat autonomie betekent.*
 - Waar ligt het onderscheid tussen autonomie en privacy? Is dit een privacyzorg?

**Wanneer mensen zich zorgen maken is het mogelijk dat ze hierbij benoemen dat zij niet gemotiveerd zijn om er iets mee te doen. Overgang volgende deel.*

5. Gedrag van internetgebruikers en achterliggende redenen

Doel: Achterhalen of mensen zich daadwerkelijk zorgen maken om de privacy of dat situatie genuanceerder ligt.

Hoofdvraag: Maken mensen zich daadwerkelijk zorgen om hun privacy?

Ruimte voor aantekeningen:

<p>Startvraag: Worden de persoonsgegevens verstrekt wanneer mensen zich zorgen maken?</p>	
<p>Doorvragen:</p> <ul style="list-style-type: none"> • <i>Privacy calculus theory</i> <ul style="list-style-type: none"> - Hoe maken mensen de afweging wanneer zij de persoonsgegevens verstrekken? Wanneer wegen de voordelen zwaarder dan de nadelen of andersom? - Hebben mensen genoeg zicht op de voordelen en nadelen? - Is controle belangrijk voor mensen? Waarom wel of niet? Wat roept het verlies van controle over persoonsgegevens op? • <i>Transparantie</i> <ul style="list-style-type: none"> - Wat betekent transparantie voor mensen? - Hoe zien zij de juiste situatie met betrekking tot transparant omgaan met de persoonsgegevens voor zich? 	

6. Percepties van mensen die zich geen zorgen maken

<p>Doel: Achterhalen waarom mensen zich geen zorgen maken om de privacy op het internet.</p> <p>Hoofdvraag: Maken mensen zich daadwerkelijk geen zorgen en waar heeft dit mee te maken?</p> <p>Startvraag: Heb je ooit een keer het idee gehad dat het niet slim was om je persoonsgegevens te verstrekken?</p> <p>*Let op non-verbale houding van de respondenten.</p>	<p>Ruimte voor aantekeningen:</p>
<p>Doorvragen:</p> <ul style="list-style-type: none"> • <i>Privacygevoelige informatie</i> <ul style="list-style-type: none"> - Wat zijn de redenen waarom mensen zich geen zorgen maken om hun privacy? - Wordt bepaalde informatie privacygevoeliger ervaren? Waarom? - Hebben mensen gebrek voor hun privacy wanneer zij niets te verbergen hebben? • <i>Nationale veiligheid</i> <ul style="list-style-type: none"> - Hoe wordt het ervaren als de overheid privacygevoelige informatie verzameld? 	

7. Afronding

Vragen of er nog dingen onduidelijk zijn of dat er vragen zijn waar ze nog op terug willen komen. De respondenten bedanken en benadrukken dat alle gegevens vernietigd worden na het onderzoek.

Bijlage 2. Losse kaartjestechniek

Persoonlijke levenssfeer

Geen sprake van bemoeienis buitenstaanders

Alleen gelaten worden

Controle of autonomie over intimiteit en identiteit

Controle over wie toegang heeft tot welke informatie

Bijlage 3. Toestemmingsformulier

Toestemmingsverklaring

voor deelname aan empirisch onderzoek over
de percepties ten aanzien van de privacyzorgen op het internet.

Ik ben voldoende geïnformeerd over het onderzoek omtrent privacyzorgen op het internet. Ik heb de gelegenheid gehad om vragen te stellen. Mijn vragen zijn naar tevredenheid beantwoord. Ik heb de tijd gehad om na te denken of ik mee zal doen aan dit onderzoek. Ik ben ervan op de hoogte dat het interview wordt opgenomen en dat deze geluidsopnamen en video-opnamen vernietigd zullen worden na het onderzoek. Ik weet dat mijn gegevens anoniem zullen blijven. Ik kan op ieder moment beslissen om niet mee te doen met het onderzoek en ik ben ervan op de hoogte dat ik hier geen reden voor hoeft op te geven. Ik doe vrijwillig mee aan dit onderzoek.

Met dit formulier geef ik toestemming om deel te nemen aan het onderzoek.

Naam respondent:

Handtekening:

Datum: __/__/__