Radboud Universiteit Nijmegen

Beschermen of bewaken: metaforen in communicatie over digitale privacy

De effecten van communicatie-uitingen over digitale privacy met en zonder talige en visuele metaforen op de risicopercepties en gedragsintenties.

English title

Protecting or monitoring: metaphors in digital privacy communication

The effects of communication messages regarding digital privacy with and without linguistic and visual metaphors on risk perceptions and behavioral intentions.

Masterscriptie

Communicatie en Beïnvloeding

Cursus	LET-CIWM401
Thema	Metaforiek in communicatie over digitale privacy
Naam	Steven van de Cruijs
Studentnummer	s4842499
Contactinformatie	s.vandecruijs@student.ru.nl
Begeleidster	Dr. G. Reijnierse
Tweede lezer	Prof. dr. E. Das
Datum	15-06-2018
Woordenaantal	10566

Samenvatting

Dit onderzoek beoogde te achterhalen welke effecten optreden door talige en visuele metaforen in communicatie-uitingen over digitale privacy. De onderzochte variabelen waren affectieve respons, gepercipieerd gevaar, ernst van de gevolgen en gedragsintenties. Daarnaast werden controlevariabelen onderzocht, om te controleren of de resultaten verder te verklaren zijn. Deze variabelen waren waardering, begrijpelijkheid, overtuigingskracht en een extra controlevraag. Voor dit onderzoek werd een binnen- en tussenproefpersoonontwerp gebruikt met vier verschillende condities, zodat de verschillen in de voor- en nameting en de verschillen per conditie te verklaren zijn. Een pretest is uitgevoerd, om te bepalen welke boodschap de hoogste waardering, elaboratie en begrijpelijkheid had en tevens het meest metaforisch was.

Er werd verwacht dat talige en visuele metaforen een positief effect zouden hebben op risicopercepties, maar in dit onderzoek trad er enkel een interactie-effect van visuele metaforen en waardering op. Dat de waardering hoger werd door visuele metaforen bleek ook uit voorgaande studies en toont daarmee consistente resultaten. Enkel het zien van een communicatie-uiting over digitale privacy zorgde al voor een verhoogde affectieve respons en op een item van gepercipieerd gevaar, namelijk cloudopslag. Blootstelling aan een communicatie-uiting over digitale privacy zorgde dus voor meer negatieve gevoelens ten opzichte van het digitale privacy onderwerp. Het uitblijven van verder reikende significante resultaten is mogelijk te verklaren door (1) het gekozen defensieve frame van de boodschap, (2) doordat het een matig complexe metafoor was en (3) dat de talige metafoor veel leek op de letterlijke boodschap. Daarnaast zouden meerdere communicatie-uitingen per conditie onderzocht kunnen worden om de mogelijk gevonden effecten kracht bij te zetten door gebruik van talige en visuele metaforen. Dat maakt het effect van metaforiek in communicatie-uitingen over digitale privacy meer te generaliseren.

Inleiding

Digitale privacy is een onderwerp dat vaak prominent in de media wordt besproken (Kleinjan, 2018; Chamorro-Premuzic, 2014). Digitale privacy omvat de zorgen die mensen hebben omtrent hun eigen digitale informatie, die vaak gerelateerd worden aan de alsmaar groeiende informatieverspreiding op publieke netwerken (Berlow, 2013). Het is een domein waar veel onwetendheid over bestaat. Mensen hebben in voorgaande studies verschillend gereageerd als het gaat om hun eigen digitale veiligheid (Mols & Janssen, 2017; TNS Opinion & Social (2015). De ene persoon vindt het belangrijker en relevanter dan de ander. Daarnaast denken mensen dat ze verantwoordelijk zijn voor de waarborging van hun eigen digitale privacy, terwijl Mols en Janssen (2017) aantonen dat individuen daar in werkelijkheid weinig controle over hebben. Steeds vaker beschikken grote instanties over de persoonsgegevens van mensen.

Het komt steeds vaker voor dat persoonsgegevens door een hackaanval buitgenomen worden door hackersgroepen (Mayer-Schönberger & Kenneth, 2013). Veel mensen zijn niet voorbereid op hackaanvallen, waarbij persoonsgegevens op straat komen te liggen, doorverkocht worden of misbruikt worden. Een ander potentieel risico is dat mensen vaak apps installeren die tal van onnodige dataeisen stellen om gegevens van gebruikers te verzamelen (Acquisti, Brandimarte & Loewenstein, 2015). Zo bleek enkele jaren geleden uit de onthullingen van Edward Snowden hoe onder andere de NSA zo veel mogelijk data van burgers probeerde te verzamelen, via communicatienetwerkwerken en software. Veel mensen staan niet stil bij de mogelijke gevolgen van een dergelijke massa dataverzameling (Chamorro-Premuzic, 2014).

In Nederland is recent gebleken dat de perceptie van digitale privacy aan het veranderen is. Een meerderheid van de Nederlanders stemden tegen de sleepwet (Radar, 2018). Dit is een wet die het voor inlichtingendiensten mogelijk maakt om als het ware met een sleepnet in een buurt grote hoeveelheden data van alle burgers te verkrijgen. Volgens Kleinjan (2018) blijkt dat Nederlanders steeds vaker inzien dat ze zelf hun digitale privacy meer moeten beschermen. Echter, Mols en Janssen (2017) en Acquisti en Loewenstein (2013) tonen aan dat nog steeds veel mensen er weinig mee bezig zijn.

Er wordt op dit moment weinig in de media gecommuniceerd over het belang van beschermde digitale privacy. Echter, op televisie komen wel regelmatig reclames voorbij van SIRE – een onafhankelijke belangenorganisatie toegespitst op ideële reclame – over belangrijke risicovolle onderwerpen, zoals huiselijk geweld of appgedrag tijdens autorijden (SIRE, z.d.). Een belangenorganisatie als SIRE heeft nooit een campagne gewijd aan de

belangen die burgers hebben bij beschermde digitale privacy. Het maatschappelijke onderwerp digitale privacy en de risico's van onbeschermde digitale privacy is mogelijk nog onderbelicht.

Mensen verschillen sterk in hun risicoperceptie wat betreft digitale privacy. De risicoperceptie van mensen wordt ontwikkeld door de gepercipieerde angst van een bepaald onderwerp of gebeurtenis, waarbij een reële kans bestaat dat de persoon of omgeving er schade aan leidt (Slovic, 1987). Die schade vormt een bedreiging voor de mens. De risicoperceptie van digitale privacy speelt een belangrijke rol bij het ontwikkelen van gedachtes maar ook van gedragsintenties (Slovic, 1987). De gedragsintentie is uit onderzoek een belangrijke voorspeller van gedragsverandering gebleken (Fischbein & Ajzen, 2010). Communicatie over onderwerpen die risico's met zich meebrengen wordt geframed om de ontvanger bewust te maken van de mogelijke gevolgen, vaak met als doel om gedrag van mensen te beïnvloeden. Framing is het creëren van een denkkader waarbinnen de boodschap wordt gecommuniceerd en tegelijkertijd andere informatie bewust wordt verhuld (Entman, 1993). Zodoende kan communicatie over digitale privacy dusdanig geframed worden dat de ontvanger digitale privacy als risicovol onderwerp ervaart. Een voorbeeld waarbij risico's omtrent het verliezen van je digitale persoonsgegevens worden geïntroduceerd in een boodschap is: "beveilig je persoonlijke digitale apparaten tegen hackaanvallen". De boodschap impliceert namelijk dat zonder beveiliging je persoonlijke digitale apparaten kwetsbaarder zijn voor hackaanvallen.

Een belangrijk instrument in framing om bepaalde aspecten van een boodschap te benadrukken en te verhullen is metaforiek (Lakoff & Johnson, 1980). Een metafoor is een idee of conceptueel domein dat wordt beschreven en/of begrepen in termen van een ander domein (Lakoff & Johnson, 1980). Uit meta-analyses blijkt dat metaforen in advertenties de waardering van een boodschap verhoogt en de boodschap tevens persuasiever maakt (Van Stee, 2018; Sopory & Dillard, 2002). Tevens blijkt dat metaforen regelmatig positievere associaties bij de ontvanger kunnen bewerkstelligen, dan wanneer een letterlijke boodschap wordt gecommuniceerd (Thibodeau, Hendricks & Boroditsky, 2017). Dit werkt doordat ontvangers uitgedaagd worden om de metafoor te begrijpen en de achterliggende boodschap te achterhalen (Van Enschot-van Dijk, 2006; McQuarrie & Mick, 1996). Daarnaast zijn visuele metaforen in advertenties regelmatig effectiever in het communiceren van een bepaalde boodschap dan letterlijke visualisaties van het doeldomein (Van Mulken, Van Hooft & Nederstigt, 2014; Phillips & McQuarrie, 2004).

Tot op heden is er veel onderzoek gedaan naar de effecten van metaforiek in de communicatiewetenschap, maar voor zover bekend nooit eerder in het digitale privacy domein. Daarnaast is voor zover bekend nooit onderzoek gedaan naar het effect van metaforen in samenhang met risicopercepties inclusief gedragsintenties. Daarom wordt onderzoek gedaan in hoeverre communicatieboodschappen toegespitst op het digitale privacy domein met visuele en/of talige metaforen, leiden tot een hogere risicoperceptie en gedragsintentie dan letterlijke boodschappen.

Theoretisch kader

Digitale privacy nader verklaard

Het internet is steeds meer verweven met ons dagelijkse leven. We laten een digitaal spoor achter met onze geldtransacties, gps-locaties en sociale mediaberichten over wat we doen, met wie en waar (Acquisti et al., 2015). Grote bedrijven onttrekken deze gegevens om alsmaar meer over ons te weten te komen. Steeds vaker is onze persoonlijke informatie voor derde partijen toegankelijk door alle activiteiten die wij online (Mayer-Schönberger et al., 2013). Er wordt gesteld dat het digitale spoor dat wij uitzetten met alle onlineactiviteiten al meer zegt over onszelf dan een persoonlijk gesprek (Acquisti et al., 2015). Ook dit komt door alle gegevens die online over ons bekend zijn. Zo kunnen mensen en organisaties tot zekere hoogte in elkaars (digitale) privéleven kijken (Acquisti et al., 2013).

Mensen zijn over het algemeen weinig bezig met hun eigen digitale privacy (Mols & Janssen, 2017; Acquisti et al., 2015; Potzsch, 2009; Barnes, 2006). Daardoor kunnen ze de mogelijke gevolgen van gebrekkige bescherming van hun digitale privacy wellicht niet goed overzien. Mensen zijn relatief eenvoudig in staat een fictieve waarde aan hun digitale privacy toe te kennen, maar tegelijkertijd willen zij niet hetzelfde bedrag uitgeven aan de bescherming ervan (Acquisti & Loewenstein, 2013). De onderzoekers gingen na in hoeverre men bereid is haar privacy op te offeren in ruil voor een cadeaukaart. De respondenten werd gevraagd hoeveel geld zij zouden accepteren om hun privacygegevens te openbaren en hoeveel zij bereid zouden zijn te betalen om potentieel openbare informatie te beschermen. In het onderzoek werden verschillende soorten cadeaukaarten gebruikt met en zonder privacy vriendelijke consequenties en respectievelijk een lagere en hogere monetaire waarde. Van de respondenten die een privacy vriendelijke cadeaukaart kregen, koos 52% voor de privacy vriendelijke cadeaukaart en niet voor de privacy onvriendelijke variant met een hogere monetaire waarde. Een andere groep proefpersonen mocht kiezen tussen beide cadeaukaarten. In deze conditie bleek 42% van de respondenten liever de privacy vriendelijke cadeaukaart te kiezen. Wanneer proefpersonen de privacy onvriendelijk cadeaukaart kregen en vervolgens gevraagd werden of ze de cadeaukaart wilden inwisselen voor een privacy vriendelijke variant met een lagere monetaire waarde, dan blijkt ineens slechts 27% te kiezen voor de privacy vriendelijke variant. De onderzoekers concluderen daarom dat er heel gevarieerd gereageerd wordt door de proefpersonen als het gaat om privacybescherming zodra er een beloning aan verbonden is.

Zodra de beloning eerst wordt gegeven, zijn mensen het minst bereid hun privacy te beschermen.

Nederlanders kijken anders tegen hun digitale privacy aan dan de werkelijke stand van hun privacy (Mols & Janssen, 2017). Nederlanders denken vaak dat hun privacy een persoonlijke kwestie is, terwijl het in feite een sociale kwestie is, wat betekent dat ze er zelf weinig grip op hebben. Nederlanders schatten daarnaast hun digitale privacy in tussen non-problematisch en hoopvol tot zorgelijk en problematisch. De ene persoon vindt digitale privacy niet zorgelijk, terwijl de andere groep dit juist wel vindt. De onderzoekers concluderen daarmee dat de attitude van Nederlanders ten opzichte van hun privacy veel verschilt.

Er blijken tevens grote tegenstrijdigheden te bestaat tussen de zorgen die mensen hebben omtrent hun eigen digitale privacy en hun daadwerkelijke online gedrag (Potzsch, 2009; Barnes, 2006). Als gevraagd wordt wat mensen vinden van het belang van privacy, dan blijkt het als belangrijk ervaren te worden, maar uit onderzoek met onder andere de cadeaukaart van Acquisti & Loewenstein (2013) blijkt het daadwerkelijke gedrag vaak te verschillen. Dit wordt toegeschreven aan de *privacy paradox*: het spanningsveld tussen het menselijk bewustzijn omtrent zorgen over privacy en daadwerkelijk gedrag (Mols & Janssen, 2017; Acquisti et al., 2015). Men vindt het eng om digitaal en sociaal uitgesloten te worden. Het resultaat is dat hoewel mensen aangeven digitale privacy belangrijk te vinden, zij toch hun gedragingen daar niet op afstemmen.

Van alle Europese burgers maken Nederlanders zich het minste zorgen om het uit handen geven van hun digitale informatie (TNS Opinion & Social, 2015). Zo blijkt ook dat 48% van de Nederlanders geen moeite heeft om persoonlijke informatie te verstrekken om gebruik te kunnen maken van een onlinedienst of applicatie. Uit de resultaten van het onderzoek van TNS Opinion & Social (2015) komt naar voren dat Nederland wel bij de top drie van landen behoort die kennis heeft genomen van de NSA-lekken. Als gevraagd wordt of de NSA haar waardigheid heeft verloren door de lekken, dan blijkt dat 43% van de respondenten het eens is met deze stelling. De perceptie van Nederlanders op online veiligheid is dus enigszins tegenstrijdig. Daarmee liggen de resultaten van TNS Opinion & Social (2015) in lijn met de bevindingen van Mols en Janssen (2017).

Risicoperceptie

De percepties van mensen op online veiligheid en digitale privacy worden ontwikkeld door hoe risico's ingeschat worden. De risicoperceptie van mensen bestaat uit een oordeel, gevoel en opvatting over risicovolle onderwerpen (Pidgeon, Hood, Jones, Turner, & Gibson, 1992). Mensen maken een interpretatie van de waarschijnlijkheid van een mogelijk risicovolle gebeurtenis, waarbij schade toegebracht kan worden aan henzelf, anderen of de omgeving (Huurne & Gutteling, 2008). De risicoperceptie is daardoor een belangrijke indicator in hoe iemand denkt over risicovolle onderwerpen (Slovic, 1987). Er wordt bepaald of het risico waarschijnlijk is en of het leidt tot ernstige gevolgen. Zodra een persoon deze interpretatie maakt, volgt een oordeel of actie op basis van de risicoperceptie. Bij een hoge risicoperceptie volgt vaker een actie van de persoon, terwijl bij een lage risicoperceptie vaker geen actie genomen wordt (Huurne & Gutteling, 2008). De interpretatie op basis van de risicoperceptie is daardoor indirect van invloed op de gedragsintenties van een persoon.

Huurne en Gutteling (2008) introduceren het Framework Risk Information Seeking (FRIS), waarmee achterhaald kan worden hoe verschillende determinanten, waaronder de risicoperceptie van invloed zijn op risicovol gedrag van mensen. De risicoperceptie in de studie van Huurne en Gutteling (2008) bestond uit de *Affective response, perceived danger* en *severity of consequences.* De affectieve responsen die men heeft bij een risicovolle gebeurtenis is van invloed op de risicoperceptie van mensen (Huurne & Gutteling, 2008). Is men geneigd negatief tegen een gebeurtenis aan te kijken, dan volgt een negatievere affectieve respons. Het gepercipieerde gevaar wordt ingeschat aan de hand van de waarschijnlijkheid van een risicovolle gebeurtenis. Denkt men dat een risicovolle gebeurtenis reëel is, dan is het gepercipieerde gevaar hoger. De severity of consequences wordt gezien als de ernst van de gevolgen (Huurne & Gutteling, 2008). Is er een klein risico en tevens een grote kans op juist positieve uitkomsten bij een gebeurtenis, dan zal de risicoperceptie lager zijn, dan wanneer het risico groot is en de positieve uitkomsten kleiner.

Tevens worden onbekende gebeurtenissen of situaties als risicovoller ervaren (De Vries, 2002). Als mensen daarentegen bekend zijn met een gebeurtenis, dan wordt de risicoperceptie juist lager. Kahneman & Tversky (1979) stellen dat de beschikbaarheid van risico's van invloed is op percepties, doordat mensen regelmatig al gedachtes hebben bij een gebeurtenis die gemakkelijk uit het geheugen te halen is. Deze gedachtes worden ook wel beschikbaarheidsheuristieken genoemd (Slovic, 1987). Als mensen eenvoudig in staat zijn om gedachtes op te halen, bijvoorbeeld van een eerdere gebeurtenis, dan is dit van invloed op de inschatting van gevaar. Mensen weten dan wat er komen gaat en daardoor kunnen zij zich

voorbereiden op de mogelijke risico's. Een andere belangrijke component is dat mensen risico's hoger inschatten naarmate meer mensen betrokken zijn bij de gebeurtenis (De Vries, 2002).

Mensen hebben ook vaker moeite met risico's inschatten als het om technologische innovatie gaat (De Vries, 2002). De risico's daarvan worden tevens hoger ingeschat, omdat mensen er vaker onbekend mee zijn. Dit ligt in lijn met hoe mensen aankijken tegen digitale privacy, omdat het goed begrijpen enige mate van technologische kennis vergt en technologie snel verandert. Daarnaast zijn mensen ook risicomijdend bij winsten en risico zoekend bij verlies (Kahneman & Tversky, 1979). In het perspectief van bescherming van digitale privacy zou dit kunnen betekenen dat men risico zoekend(er) is, omdat men zijn/haar privacy enkel kan verliezen ten gevolge van een bepaalde gebeurtenis en niet 'winnen'.

Framing van risico's

Hoe mensen denken over een bepaald onderwerpen of gebeurtenissen heeft onder meer te maken met hoe boodschappen in de media geframed worden (Scheufele & Tewksbury, 2007). Framing heeft ten doel om een probleemdefinitie, interpretatie, evaluatie of aanbeveling een richting op te sturen die in het frame wordt beschreven (Entman, 1993). Door het denkkader worden bepaalde elementen uitgelicht of uitgesloten die in communicatie veel voorkomen (Gitlin, 1980). Er wordt gesteld dat framing een effect heeft op het denkkader van de ontvanger. De ontvanger kan namelijk eenzelfde denkkader ontwikkelen, gelijk aan het denkkader van de boodschapper of aan dat van de boodschap (Cappella & Jamieson, 1997). Het is een mogelijkheid dat in persuasieve boodschappen die appelleren aan risico's van onveilige digitale bescherming, de ontvanger zijn gedachtes mogelijk gaat conformeren aan de boodschap. Het gevolg is dat de gedachtes van de ontvanger bepalend zijn voor hoe de risico's worden ingeschat. Een denkkader met een risicoperceptieboodschap is hierdoor van invloed op hoe mensen aankijken tegen risico's omtrent onveilige digitale privacy. Daarom wordt in dit onderzoek onderzocht in hoeverre risicopercepties van mensen veranderen na het zien van een communicatie-uiting in het digitale privacy domein.

H1a: de affectieve respons is hoger na het zien van een digitale privacy communicatie-uiting, dan voor het zien van een digitale privacy communicatie-uiting.

H1b: het gepercipieerde gevaar is hoger na het zien van een digitale privacy communicatie-uiting, dan voor het zien van een digitale privacy communicatie-uiting.

H1c: de ernst van de gevolgen is hoger na het zien van een digitale privacy communicatie-uiting, dan voor het zien van een digitale privacy communicatie-uiting.

Gedragsintenties

De gedragsintentie is een belangrijke voorspeller van daadwerkelijk gedrag (Fishbein & Ajzen, 2010). In persuasieve communicatie wordt vaak gepoogd om iemands gedrag te veranderen, zodat burgers bijvoorbeeld meer maatregelen nemen voor betere privacybescherming. De affectieve respons, het gepercipieerde gevaar en de ernst van de gevolgen hebben invloed op welk soort gedrag mogelijk tot stand komt (Huurne & Gutteling, 2008).

In het onderzoek van Huurne en Gutteling (2008) wordt voornamelijk gekeken naar *intentions to information seeking behavior* om zoekgedrag over een bepaald risico te voorspellen. De intentions to information seeking behavior bepaalt in hoeverre iemand geneigd is om aanvullende informatie op te zoeken na het zien van een risicovolle boodschap. Deze gedragsintentie is dus niet geconcretiseerd voor gedragsverandering van bijvoorbeeld betere privacybescherming. Daarom worden de variabele gedragsintentie voor dit onderzoek vereenvoudigd en in lijn gebracht met de vragen uit de Theory of planned behavior, zodat concreet en specifiek gedrag onderzocht kan worden (Ajzen, 1991). Met behulp van de Theory of planned behavior kan inzichtelijk gemaakt worden hoe gedrag van mensen op een bepaald onderwerp tot stand komt. Het is daardoor mogelijk om te achterhalen of verschillende communicatie-uitingen – met of zonder metaforen – verschillende resultaten weergeven.

Metaforiek als denkkader

Metaforiek is een instrument om communicatieboodschappen persuasiever te maken (Hoeken, Hornikx & Hustinx, 2012). Bij metaforiek wordt een bepaald denkkader gebruikt om ontvangers een bepaalde richting in te sturen. Het is een vorm van figuratieve beeldspraak met een vergelijking tussen twee concepten die feitelijk weinig met elkaar gemeen hebben, maar wel met elkaar vergeleken kunnen worden (Lakoff & Johnson, 1980). Een voorbeeld is de uitspraak ‘het verslaan van kanker’, terwijl we niet daadwerkelijk een fysiek gevecht aangaan (Thibodeau, Hendricks & Boroditsky, 2017). Het doeldomein is waarover je iets wilt zeggen; in dit geval het genezen van kanker. Het brondomein is een (concreter) domein dat gebruikt wordt om over het doeldomein te praten; in dit geval een fysiek gevecht. Een ander voorbeeld

is ‘de race tegen klimaatverandering’. Het doeldomein is in dit geval plannen en acties om klimaatverandering tegen te gaan. Het brondomein is in dit geval een fysieke race. De letterlijke taal als vervanging van de bovengenoemde voorbeelden zijn bijvoorbeeld “genezen van kanker” en “veranderingen tegen klimaatsverandering”.

Het voordeel van metaforen is dat boodschappen regelmatig hoger gewaardeerd worden, de boodschap vaker zorgt voor uitgebreidere gedachtes en uiteindelijk persuasiever kan zijn (Van Stee, 2018; Sopory & Dillard, 2002). Metaforen werken via twee responstypen, namelijk elaboratie en verwerkingsplezier. Mensen vinden het vaak plezierig als ze een metafoor begrijpen. Door de stijl van de boodschap kunnen mensen ontvankelijker worden voor verschillende positieve associaties ten aanzien van de boodschap (McQuarrie & Mick, 2005; Phillips, 1997). Bijvoorbeeld ‘met product x haal je de lente in huis’, wat associaties als frisheid, blijdschap of bloei kan oproepen. De randvoorwaarde is dat de metafoor relatief eenvoudig opgelost moet kunnen worden, omdat mensen vaak weinig aandacht hebben voor advertenties (Hoeken, Hornikx & Hustinx, 2012). Een metafoor werkt minder goed als mensen de boodschap niet kunnen oplossen. Er blijft dan vaak een negatiever gevoel over ten opzichte van de boodschap en het merk (McQuarrie en Mick, 2005).

Talige metaforen

Lakoff en Johnson (1980) stellen dat we in onze talige expressie vaak gebruikmaken van verschillende metaforen. Meta-analyses tonen aan dat metaforen een hogere attitude ten opzichte van de boodschap realiseren, waardoor metaforen ook overtuigender gevonden kunnen worden dan een boodschap met letterlijk taalgebruik (Van Stee, 2018; Sopory & Dillard, 2002). Daarnaast is aangetoond dat het effect van metaforen vergroot wordt als er een goede fit is, oftewel dat er een logische verbinding is tussen beide domeinen (Sopory & Dillard, 2002). Een goede fit is bijvoorbeeld de frisheid van wasmiddelen en een frisse lucht (McQuarrie & Mick, 2005). Mensen ervaren de buitenlucht als fris, net als gewassen kleren met lekker ruikend wasmiddel. Daarnaast blijkt dat wanneer een metafoor vooraan/direct in een boodschap voorkomt of het een nieuwe metafoor betreft, de boodschap beter gewaardeerd wordt (Sopory & Dillard, 2002).

Uit onderzoek naar de werking van tekstuele metaforen versus letterlijke equivalenten in politieke boodschappen over netneutraliteit – een onderwerp dat verwant is aan digitale privacy – blijkt dat ook in dit domein metaforen beter gewaardeerd worden dan letterlijke

boodschappen (Hartman, 2012). De verwachting is dat in het digitale privacy domein gelijksoortige resultaten gevonden worden.

H2a: een digitale privacy communicatie-uiting met een talige metafoor resulteert in een hogere affectieve respons dan een letterlijk equivalent.

H2b: een digitale privacy communicatie-uiting met een talige metafoor resulteert in een hogere gepercipieerd gevaar-inschatting dan een letterlijk equivalent.

H2c: een digitale privacy communicatie-uiting met een talige metafoor resulteert in een hogere ernst van de gevolgen-inschatting dan een letterlijk equivalent.

H2d: een digitale privacy communicatie-uiting met een talige metafoor resulteert in een hogere gedragsintentie dan een letterlijk equivalent.

Visuele metaforen

Visuele metaforen zijn feitelijk identiek aan een talige metafoor, maar het verschil is dat de metafoor is gevisualiseerd. Hoe in talige metaforen het brondomein wordt beschreven om met figuratieve beeldspraak het doeldomein te verklaren, is dit proces bij visuele metaforen juist gevisualiseerd. In het eerdergenoemde voorbeeld van frisse lucht en wasmiddel zal een visuele verbinding gelegd worden tussen bijvoorbeeld lenteweer en een wasmiddelproduct.

Uit onderzoek blijkt dat een metafoor die een visuele scene nabootst, beter wordt gewaardeerd dan een visuele scene die een letterlijke boodschap visualiseert (Van Mulken, le Pair & Forceville, 2010; Richardson & Matlock, 2007). Daarnaast blijkt uit onderzoek van Van Mulken et al (2014) dat wanneer een advertentie een matig uitdagende visuele metafoor heeft, de waardering van de advertentie hoger is, dan bij een complexere visuele metafoor. De complexiteit van een metafoor kan verklaard worden door verschillende visuele kenmerken. Advertenties kunnen opgemaakt worden waarbij de verschillende domeinen naast elkaar worden afgebeeld – ook wel juxtapositie metaforen genoemd (Van Mulken et al., 2014). Daarnaast bestaan er ook metaforen die beide domeinen in elkaar laat vloeien: de fusiemetafoor. Een volledige vervanging – het brondomein vervangt het doeldomein – zijn het meest complex (Phillips & McQuarrie, 2004). Een voorbeeld uit de studie van Van Mulken et al. (2014) in een opticien reclame-uiting is een afbeelding van een wortel, omdat het eten van wortels goed voor je ogen is. De associatie die mensen maken, indien ze de boodschap van de

opticien met de wortel begrijpen, is dat de opticien wellicht brillen verkoopt die je zicht bevorderen.

Is de boodschap te complex, dan bestaat de mogelijkheid dat ontvangers de boodschap niet kunnen achterhalen. De fusiemetafoor is daarentegen matig complex en de betekenis van de boodschap is daardoor nog goed te achterhalen (Van Mulken et al., 2014; Phillips & McQuarrie, 2004). Een fusiemetafoor heeft tevens het voordeel dat ontvangers naast de werkelijke betekenis van de boodschap meer positieve associaties ten aanzien van de advertentie en het geadverteerde merk of organisatie ontwikkelen (Van Mulken et al., 2014). Daardoor wordt gesteld dat bij visuele metaforen de fusiemetafoor de hoogste waardering oplevert en het meest overtuigend is. In dit onderzoek wordt daarom uitsluitend gekozen voor fusiemetaforen in de condities waarbij visuele metaforen aanwezig zijn. De onderstaande hypotheses zijn opgesteld om te achterhalen of een visuele metafoor hoger scoort dan een letterlijk equivalent.

H3a: een digitale privacy communicatie-uiting met een visuele metafoor resulteert in een hogere affectieve respons dan een letterlijk equivalent.

H3b: een digitale privacy communicatie-uiting met een visuele metafoor resulteert in een hogere gepercipieerd gevaar-inschatting dan een letterlijk equivalent.

H3c: een digitale privacy communicatie-uiting met een visuele metafoor resulteert in een hogere ernst van de gevolgen-inschatting dan een letterlijk equivalent.

H3d: een digitale privacy communicatie-uiting met een visuele metafoor resulteert in een hogere gedragsintentie dan een letterlijk equivalent.

Combinatiemetaforen

Talige en visuele metaforen kunnen ook gecombineerd worden in advertenties. De meta-analyses van Van Stee (2018) en Sopory en Dillard (2002) tonen aan dat een communicatieboodschap profijt heeft van een talige metafoor als het gaat om een hogere waardering van de boodschap en het merk. Daarnaast stijgt de waardering van communicatieboodschappen sterker bij visuele metaforen dan letterlijke beelden. (Van Mulken et al., 2014; Phillips & McQuarrie, 2004). Indien de metafoor aanzet tot een plezierige verwerking van de boodschap, dan worden mensen vaak ontvankelijker voor meerdere

positieve associaties ten aanzien van de boodschap (McQuarrie & Mick, 2005; Phillips, 1997). De verwachting is dat communicatieboodschappen in het digitale privacy domein met een combinatie van zowel een talige als visuele metafoor zorgen voor een hogere risicoperceptie en gedragsintentie dan letterlijke equivalenten. Hieronder zijn de hypotheses beschreven die interactie-effecten verklaren.

H4a: er is een interactie-effect tussen talige en visuele metaforen en affectieve respons bij communicatie-uitingen over digitale privacy.

H4b: er is een interactie-effect tussen talige en visuele metaforen en gepercipieerd gevaar bij communicatie-uitingen over digitale privacy.

H4c: er is een interactie-effect tussen talige en visuele metaforen en ernst van de gevolgen bij communicatie-uitingen over digitale privacy.

H4d: er is een interactie-effect tussen talige en visuele metaforen op de gedragsintenties bij communicatie-uitingen over digitale privacy.

Hoofdvraag

Wat is het effect van digitale privacy communicatie-uitingen met en zonder talige en visuele metaforen op de risicopercepties en gedragsintenties van mensen?

Methode

Het onderzoek betrof een experiment met Nederlandse burgers. Door middel van een online vragenlijst werd onderzocht welke effecten optraden bij digitale privacy communicatieboodschappen met (visuele/talige/combinatie) metaforen en letterlijke taal op risicopercepties en gedragsintenties. Daarnaast zijn er controlevariabelen geanalyseerd. Dit waren waardering, begrijpelijkheid, overtuigingskracht en een controlevraag. In de methodesectie is tevens de pretest voor het experiment beschreven onder *pretest.*

Proefpersonen

Het experiment werd uitgevoerd bij 211 proefpersonen. Na het eruit filteren van proefpersonen die de vragenlijst niet volledig hebben ingevuld (39), jonger waren dan achttien (2), korter dan vier minuten over de vragenlijst deden (19) of langer dan een uur (7), kwam het aantal proefpersonen op 166. De data van 45 proefpersonen werden uit het uiteindelijke databestand gefilterd. Redelijkerwijs kon de vragenlijst niet in minder dan vier minuten afgerond worden. Proefpersonen die langer dan een uur over de vragenlijst deden konden mogelijkerwijs afgeleid zijn.

De proefpersonen waren tussen de 18 en 70 jaar oud (M = 30.45, SD = 12.63). Van de proefpersonen was 64% vrouw en 36% man. Het hoger beroepsonderwijs kwam het vaakst voor (49%), gevolgd door wetenschappelijk onderwijs (30%), middelbaar beroepsonderwijs (15%) en middelbare school (6%). Uit de χ^2-toets tussen Geslacht en Condities bleek geen significant verschil te bestaan (χ^2 (3) = 4.414, p = .220). Uit een χ^2-toets tussen Opleidingsniveau en Condities bleek geen significant verschil te bestaan (χ^2 (9) = 6.150 p = .725). Uit een eenweg variantieanalyse van Leeftijd op Conditie bleek geen significant verschil te bestaan (F (3, 162) < 1). De leeftijd, het geslacht en het opleidingsniveau waren gelijkmatig verdeeld over de condities.

Design

Dit experimentele onderzoek betrof een mixed design met als onafhankelijke variabelen visuele metaforen en tekstuele metaforen en de afhankelijke variabelen affectieve respons, gepercipieerd gevaar, ernst van de gevolgen en gedragsintenties. Daarnaast werden de controlevariabelen waardering, begrijpelijkheid, overtuigingskracht en een controlevraag onderzocht. De afhankelijke variabelen waren van ordinaal meetniveau. Hierdoor betrof het een 2 (visuele metaforen: aanwezig en letterlijke beelden) × 2 (tekstuele metaforen: aanwezig en letterlijke taal) tussenproefpersoonontwerp. Daarnaast had het experimentele onderzoek een binnenproefpersoonontwerp met de afhankelijke variabelen affectieve respons, gepercipieerd gevaar en ernst van de gevolgen. Deze afhankelijke variabelen werden gemeten door middel van een voormeting en nameting.

Procedure

De proefpersonen werden verkregen via persoonlijk contact en/of via een link naar het onderzoek. Er werd gevraagd of mensen willen deelnemen aan een onderzoek over de digitale wereld waarin wij leven. Om het respondentenaantal te vergroten werd gevraagd om de link naar de online vragenlijst te delen met vrienden, familie en collega's. Daarnaast werd vermeld dat drie van de deelnemende proefpersonen een Bol.com cadeaukaart konden winnen, indien de proefpersoon haar e-mailadres achter zou laten.

De proefpersonen werden gerandomiseerd ingedeeld in een van de vier condities. Elke proefpersoon kreeg daardoor een van de vier condities te zien die elk bestond uit een poster. In de periode 30 april tot en met 2 mei 2018 werd de online vragenlijst beschikbaar gesteld. Het onderzoek nam gemiddeld elf minuten in beslag.

De proefpersonen werd gevraagd de vragen geheel naar eigen mening in te vullen. Na *informed consent* konden proefpersonen verder naar het onderzoek. Proefpersonen jonger dan achttien werden verteld dat ze niet konden deelnemen in verband met de minimale leeftijd van achttien jaar en werden vriendelijk bedankt.

Het online experiment bestond uit drie onderdelen. Ten eerste de voormeting met vragen over risicopercepties en extra vragen over digitale veiligheid om het onderzoek te verhullen. Deze vragen hadden betrekking op straling van mobiele apparaten en kijkgedrag naar digitale schermen. Het tweede deel betrof een dertig seconden durende puzzel zoek-de-verschillen om de proefpersonen af te leiden, zodat ze niet meer wisten wat ze bij de eerste set vragen hadden ingevuld. Dit was nodig aangezien dezelfde vragen herhaald werden in de nameting, om het effect van de poster te achterhalen. Ten derde volgde de poster en de nameting met vragen over risicopercepties en gedragsintenties. Elk onderwerp binnen de vragenlijst werd geïntroduceerd met een korte zin en/of instructie. Vervolgens werden er vragen over de waardering, de begrijpelijkheid, de overtuigingskracht en een extra controlevraag gesteld. Tot slot volgden gesloten vragen over geslacht en opleidingsniveau.

Aan het einde van het onderzoek werden proefpersonen gedebrieft, waarin verteld werd dat het onderzoek ging over metaforen in communicatie-uitingen over digitale privacy. De complete vragenlijst van het experiment is te vinden in de bijlage, Bijlage B.

Materiaal

Voor dit onderzoek werd gebruikgemaakt van vier verschillende posters die ontworpen zijn aan de hand van de criteria die gelden voor fusiemetaforen (Van Mulken et al., 2014). De posters waren elk gelijkwaardig aan elkaar, maar verschilden in metaforiek.

Alle versies van de poster hadden een korte tekst van een regel die groot werd afgebeeld op de bovenste helft van de staande poster. Op de onderste helft van de poster werd de visuele component weergegeven; een smartphone met of zonder screensaver van een waakhond. De achtergrond van de poster bevatte geen visuele elementen en was wit. Dit om ervoor te zorgen dat er geen andere onvoorziene effecten zouden optreden.

De visuele metaforen waren fusiemetaforen en de talige metaforen een metafoor: ‘bewaak uw digitale privacy’, waarbij ‘bewaak’ in dit domein een metafoor is voor ‘beschermen’.

De visuele manipulatie betrof een poster met fusiemetafoor en een letterlijk beeld. De boodschappen werden zo ontworpen dat ontvangers de digitale privacy boodschap konden zien als een goed idee; meer bescherming van je digitale privacy.

Visuele weergave van de posters die gebruikt zijn in het experiment.

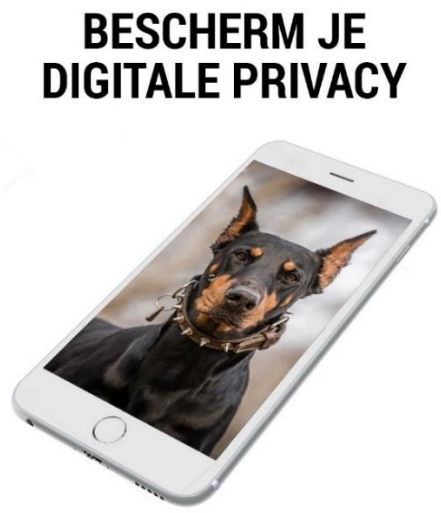
Controleconditie

Letterlijke taal & letterlijk beeld

Talige metafoor

& letterlijk beeld

Letterlijke taal & visuele metafoor



Combinatie-metafoor

Visuele & talige metafoor

Pretest

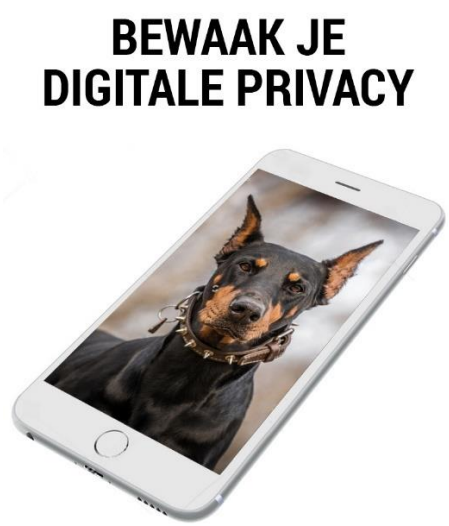
Er werd een pretest uitgevoerd om te achterhalen of de posters voldeden aan enkele basiswaarden. De pretest werd uitgevoerd onder achttien proefpersonen (n=18), waarvan 72% man en 28% vrouw. De proefpersonen hadden in de meeste gevallen hoger beroepsonderwijs (61%) afgerond, gevolgd door wetenschappelijk onderwijs (33%) en middelbare school (6%).

De afhankelijke variabelen waren waardering, begrijpelijkheid en mate van elaboratie. Daarnaast is gevraagd in hoeverre proefpersonen de poster letterlijk of figuurlijk vonden en in hoeverre de poster concreet versus abstract was. Deze variabelen werden onderzocht bij drie verschillende posters.

Visuele weergave van de posters die gebruikt zijn voor de pretest.

Poster 1 – hek

Poster 2 – hond



Poster 3 – slot

De vragen/stellingen waren: “welke waardering geef je de boodschap van de poster” (1 zeer slecht – 7 zeer goed), “de poster zet mij aan het denken” (1 helemaal niet mee eens – 7 helemaal mee eens) en “de boodschap is makkelijk te begrijpen” (1 helemaal niet mee eens – 7 helemaal mee eens). Er werden drie ontwerpen gemaakt van de combinatiemetafoor conditie, waarbij tekstuele en visuele metaforen gecombineerd werden. De poster met de hoogste gemiddeldes op waardering, begrijpelijkheid en elaboratie, werd gebruikt in het uiteindelijke onderzoek. De pretest vragenlijst is te raadplegen in de bijlagen, Bijlage A. In tabel 1 zijn de resultaten van de pretest beschreven.

Tabel 1. Gemiddeldes per poster over digitale privacy uit de pretest (standaarddeviaties tussen haakjes: minimaal 1, maximaal 7; n = 18).

Construct	Poster 1: Hek	Poster 2: Hond	Poster 3: Slot
Waardering	4.17 *(1.51)*	4.50 *(1.20)*	4.44 *(1.38)*
Elaboratie	3.83 *(17.2)*	4.61 *(1.46)*	4.50 *(1.04)*
Begrijpelijkheid	4.50 *(1.82)*	4.67 *(1.85)*	5.17 *(1.34)*
Letterlijk vs. Figuurlijk	4.28 *(1.90)*	4.39 *(1.50)*	3.94 *(1.92)*
Concreet vs. Abstract	3.94 *(1.77)*	*4.11 (1.18)*	3.83 *(1.69)*

Notitie: er is niet voldaan aan het minimumaantal proefpersonen van 30. Er is voldaan aan de Mauchly's test of Sphericity.

Uit de repeated measures variantieanalyse voor Waardering van de boodschap met als binnen-proefpersoonfactor Waardering bleek geen significant hoofdeffect voor Waardering (F (1, 17) < 1). Het bleek dat de waardering van de communicatie-uitingen over digitale privacy niet van elkaar verschilden.

Uit de repeated measures variantieanalyse voor Gedachtes over de boodschap met als binnen-proefpersoonfactor Elaboratie bleek geen significant hoofdeffect voor Elaboratie (F (1, 17) = 2.96, p = .104). Het bleek dat de gedachtes die proefpersonen hadden over de communicatie-uitingen over digitale privacy niet van elkaar verschilden.

Uit de repeated measures variantieanalyse voor Begrijpelijkheid van de boodschap met als binnen-proefpersoonfactor Begrijpelijkheid bleek geen significant hoofdeffect voor Begrijpelijkheid (F (1, 17) = 1.94, p = .181). Het bleek dat de begrijpelijkheid van de communicatie-uitingen over digitale privacy niet van elkaar verschilden.

Uit de repeated measures variantieanalyse voor Mate van letterlijkheid van de boodschap met als binnen-proefpersoonfactor Letterlijk vs. Figuurlijk bleek geen significant hoofdeffect voor Mate van letterlijkheid (F (1, 17) < 1). Het bleek dat de communicatie-uitingen over digitale privacy niet van elkaar verschilden op letterlijk vs. figuurlijk.

Uit de repeated measures variantieanalyse voor Mate van concreetheid van de boodschap met als binnen-proefpersoonfactor Concreet vs. Abstract bleek geen significant hoofdeffect voor Mate van concreetheid (F (1, 17) < 1). Het bleek dat de communicatie-uitingen over digitale privacy niet van elkaar verschilden op concreet vs. abstract.

De poster van de hond had uiteindelijk de hoogste gemiddeldes van waardering en elaboratie. Tevens bleek deze poster het meest metaforisch. De poster van de hond was het meest figuurlijk en het meest abstract. Daarom is voor de poster van de hond gekozen in het experiment.

Instrumentatie

De risicoperceptie bestond uit drie determinanten, afkomstig uit het Framework of Risk Information Seeking (FRIS) model van Huurne & Gutteling (2008). Als toevoeging werd de gedragsintentie onderzocht. Tevens werd de evaluatie van de boodschap met de controlevariabelen waardering, begrijpelijkheid en overtuigingskracht gemeten, inclusief een extra controlevraag. De interne consistentie van de bovengenoemde determinanten werden getest met de Cronbach's α.

Affectieve respons werd gemeten aan de hand van zes items met op een vijfpunts likertschaal uit het onderzoek van Huurne & Gutteling (2008). De vraag die gesteld werd ging over zes verschillende typen gevoelens. De vraag was: "welke gevoelens heb je wanneer je denkt aan de risico's omtrent jouw eigen digitale privacy" (1 helemaal niet – 5 heel erg). De items waren gespannen, angstig, bekwaam, aangenaam, bezorgd en rustig en waren vertaald met Google Translate uit het Engels (tense, content, anxious, comfortable, worried en at ease). Bekwaam en aangenaam worden omgepoold, zoals in het onderzoek van Huurne en Gutteling (2008). De betrouwbaarheid van de variabele 'affectieve respons' uit de voormeting bestaande uit zes items was acceptabel $\alpha = .708$ en uit de nameting acceptabel $\alpha = .772$.

Gepercipieerd gevaar werd gemeten aan de hand van drie items met een vijfpunts likertschaal, zoals werd toegepast in het onderzoek van Huurne & Gutteling (2008), afkomstig uit het onderzoek van Slovic (1987). De vragen zijn herformuleerd en vertaald met Google Translate uit het Engels, zodat ze van toepassing zijn op het onderwerp digitale privacy. Oorspronkelijk gingen de vragen over gevaarlijke stoffen. De vragen die gesteld werden in dit onderzoek gingen erover in hoeverre iemand risico's inschat omtrent zijn eigen digitale privacy. De vragen waren: "hoe riskant is het volgens jou om persoonlijke foto's via sociale media te delen", "hoe riskant is het volgens jou om een zwak wachtwoord te gebruiken voor je e-mailaccount" en "hoe riskant is het volgens jou om je persoonlijke gegevens op te slaan in een digitale online cloud" (1 helemaal niet riskant – 5 heel riskant). De betrouwbaarheid van de variabele 'gepercipieerd gevaar' uit de voormeting bestaande uit drie items was slecht $\alpha =$

.588 en uit de nameting eveneens slecht α = .649. Het verwijderen van één item maakte de schaal niet betrouwbaar genoeg en daarom zijn de drie items afzonderlijk berekend in de resultatensectie.

Ernst van de gevolgen werd gemeten aan de hand van twee items met een vijfpunts likertschaal uit het onderzoek van Huurne & Gutteling (2008). De stellingen zijn vertaald met Google Translate uit het Engels en gecontroleerd door een tweede persoon. De stellingen waren: "als kwaadwillenden mijn digitale privacy misbruiken, dan zal het mijn leven enorm verstoren" en "als kwaadwillenden mijn digitale privacy misbruiken, dan zal dat een groot aantal mensen treffen" (1 helemaal niet – 5 heel erg). De betrouwbaarheid van de variabele 'ernst van de gevolgen' uit de voormeting bestaande uit twee items was goed α = .806 en uit de nameting ook goed α = .861.

Waardering werd gemeten aan de hand van vier items op een zevenpunts semantische differentiaal, zoals toegepast in het onderzoek van Lagerwerf & Meijers (2008). Hierdoor werd de waardering op verschillende aspecten van de poster beoordeeld. De stelling was: "de poster vind ik" slecht – goed, onaantrekkelijk – aantrekkelijk, misleidend – informatief en voorspelbaar – verrassend. De betrouwbaarheid van de variabele 'waardering' uit de nameting bestaande uit vier items was acceptabel α = .758.

Begrijpelijkheid werd gemeten aan de hand van drie items op een zevenpunts likertschaal uit het onderzoek van Vermeulen (2014). De stellingen waren: "de poster is begrijpelijk", "de poster brengt de boodschap duidelijk naar voren" en "de poster maakt duidelijk wat de boodschapper wil vertellen" (helemaal mee oneens – 7 helemaal mee eens). De betrouwbaarheid van de variabele 'begrijpelijkheid' uit de nameting bestaande uit drie items was goed α = .859.

Overtuigingskracht werd gemeten aan de hand van vier items met een zevenpunts semantische differentiaal, gebaseerd op het onderzoek Van Enschot-van Dijk (2006), maar aangepast met betrekking tot dit onderzoek. De stelling was: "ik vind digitale privacy" onbelangrijk – belangrijk, irrelevant – relevant, oninteressant – interessant en zinloos – zinvol. De betrouwbaarheid van de variabele 'overtuigingskracht' uit de nameting bestaande uit vier items was goed α = .893.

Gedragsintenties werden gemeten aan de hand van drie items op een zevenpunts likertschaal. Deze vragen zijn gebaseerd op de Theory of planned behavior van Fishbein en Ajzen (2010) en herformuleerd, zodat ze van toepassing zijn op digitale privacy. De stellingen

waren: “ik zal mijn privacy instellingen op sociale media aanpassen”, “ik zal mijn accounts en digitale gegevens beter beschermen”, “ik zal minder persoonlijke gegevens verspreiden” (1 helemaal niet mee eens – 7 helemaal mee eens). De betrouwbaarheid van de variabele ‘gedragsintenties’ uit de nameting bestaande uit vier items was goed $\alpha = .871$.

De extra controlevraag “het belang van digitale privacy wordt onderschat” werd gemeten aan de hand van een zevenpunts likertschaal, waarbij 1 helemaal niet mee eens en 7 helemaal mee eens.

Statistische toetsing

Door middel van Factorial mixed ANOVA werd onderzocht of effecten optraden tussen de verschillende condities op de afhankelijke variabelen voor zowel de voor- en nameting (Field, 2015). Met de Factorial mixed ANOVA was het mogelijk interactie-effecten tussen variabelen te vinden. Om het verschil in waardering, begrijpelijkheid, overtuigingskracht, gedragsintenties en voor de controlevraag te onderzoeken werden univariate twee-weg ANOVA’s gebruikt. De bovengenoemde toetsen en analyses werden met behulp van statistiekprogramma IBM SPSS Statistics 23 uitgevoerd.

Resultaten

In de resultatensectie zijn alle analyses per variabele weergegeven. Bij elke variabele is de statistische toets weergegeven, inclusief significantieniveaus. In tabel 2 is de tussenproefpersoon variabele gedragsintenties weergegeven, inclusief de controlevariabelen en de extra controlevraag. In tabel 3 zijn de gemiddeldes en standaarddeviaties uit de voor- en nameting weergegeven van affectieve respons, gepercipieerd gevaar en ernst van de gevolgen.

Controlevariabelen

Waardering

De assumptie voor gelijke varianties was voor deze test geschonden, waardoor de *F*-waarde gecorrigeerd werd. Uit de tweeweg variantieanalyse van Talige metaforen en Visuele metaforen op Waardering bleek een significant hoofdeffect van Visuele metaforen (F (1, 162) 16.43, $p < .001$), maar niet van Talige metaforen (F (1, 162) < 1). Het bleek dat de communicatie-uiting over digitale privacy met visuele metaforen ($M = 3.97$, $SD = 1.24$) hogere waarderingen genoten dan de equivalenten met letterlijke beelden ($M = 3.29$, $SD = 0.87$). Er trad geen interactie op tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1).

Begrijpelijkheid

Uit de tweeweg variantieanalyse van Talige metaforen en Visuele metaforen op Begrijpelijkheid bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) < 1) en er trad geen interactie op tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). Het bleek dat er tussen de condities met en zonder talige en visuele metaforen geen verschillen zijn in de mate van begrijpelijkheid van de communicatie-uiting over digitale privacy.

Overtuigingskracht

Uit de tweeweg variantieanalyse van Talige metaforen en Visuele metaforen op Overtuigingskracht bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) < 1) en er trad geen interactie op tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). Het bleek dat er tussen de condities met en zonder talige en visuele metaforen geen verschillen zijn in overtuigingskracht van de communicatie-uiting over digitale privacy.

Extra controlevariabele

Uit de tweeweg variantieanalyse van Talige metaforen en Visuele metaforen op Belang van digitale privacy bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) < 1) en er trad geen interactie op tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). Het bleek dat er tussen de condities met en zonder talige en visuele metaforen geen verschillen zijn op de perceptie van mensen over het belang van digitale privacy door de communicatie-uiting over digitale privacy.

Gedragsintenties

Uit de tweeweg variantieanalyse van Talige metaforen en Visuele metaforen op Gedragsintenties bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) < 1) en er trad geen interactie op tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). Het bleek dat er tussen de condities met en zonder talige en visuele metaforen geen verschillen zijn op de gedragsintenties van mensen door de communicatie-uiting over digitale privacy.

Tabel 2. Gemiddeldes per conditie met talige/visuele metaforen en letterlijke taal/beelden (standaarddeviaties tussen haakjes: minimaal 1, maximaal 7).

Construct	Controleconditie Letterlijke taal & letterlijk beeld n = 40	Talige metafoor & letterlijk beeld n = 40	Letterlijke taal & visuele metafoor n = 45	Combinatie-metafoor Visuele & talige metafoor n = 41
Gedragsintenties	4.47 *(1.37)*	4.38 *(1.42)*	4.56 *(1.45)*	4.42 *(1.43)*
Waardering**	3.21 *(0.95)**	3.37 *(0.78)**	3.93 *(1.24)**	4.00 *(1.24)**
Begrijpelijkheid	4.40 *(1.63)*	4.73 *(1.36)*	4.61 *(1.51)*	4.66 *(1.57)*
Overtuigingskracht	5.78 *(1.11)*	5.51 *(1.20)*	5.83 *(1.06)*	5.76 *(1.13)*
Controlevariabele – onderschatten privacy	5.65 *(1.05)*	5.60 *(1.26)*	5.38 *(1.35)*	5.59 *(1.24)*

* Assumptie voor gelijke varianties geschonden
** Tussenproefpersoon hoofdeffect significantie $p < .05$

Tabel 3. Gemiddeldes per conditie met talige/visuele metaforen en letterlijke taal/beelden (standaarddeviaties tussen haakjes: minimaal 1, maximaal 5).

	Controleconditie Letterlijke taal & beeld n = 40		Talige metafoor & letterlijk beeld n = 40		Letterlijke taal & visuele metafoor n = 45		Combinatie-metafoor Visuele & talige metafoor n = 41	
Construct	**Voormeting**	**Nameting**	**Voormeting**	**Nameting**	**Voormeting**	**Nameting**	**Voormeting**	**Nameting**
Affectieve respons*	3.27 *(0.54)*	3.28 *(0.53)*	3.14 *(0.57)*	3.24 *(0.53)*	3.28 *(0.65)*	3.49 *(0.71)*	3.19 *(0.63)*	3.35 *(0.62)*
Gepercipieerd gevaar - Social media risico's	3.40 *(0.81)*	3.48 *(0.72)*	3.40 *(0.87)*	3.38 *(0.84)*	3.31 *(0.87)*	3.36 *(0.80)*	3.27 *(0.87)*	3.32 *(0.93)*
Gepercipieerd gevaar - E-mailbeveiliging	3.88 *(0.91)*	3.85 *(0.86)*	3.78 *(0.92)*	3.78 *(0.77)*	3.93 *(0.90)*	3.89 *(0.83)*	3.68 *(1.01)*	3.80 *(1.01)*
Gepercipieerd gevaar – Cloudopslag*	3.15 *(0.77)*	3.40 *(0.71)*	3.10 *(0.93)*	3.30 *(0.85)*	3.22 *(1.02)*	3.38 *(0.96)*	2.90 *(1.02)*	3.15 *(0.96)*
Ernst van de gevolgen	3.40 *(0.85)*	3.36 *(0.91)*	3.36 *(0.76)*	3.33 *(0.81)*	3.28 *(0.99)*	3.41 *(1.02)*	3.34 *(1.07)*	3.41 *(0.92)*

* Binnenproefpersoon hoofdeffect significantie $p < .05$

Affectieve respons

Uit de tweeweg mixed design variantieanalyse voor Affectieve respons met als binnen-proefpersoonfactor Affectieve respons en tussen-proefpersoonfactoren Talige metaforen en Visuele metaforen bleek een significant hoofdeffect voor Affectieve respons (F (1, 162) = 12.37, p = .001). Het bleek dat de affectieve respons van mensen hoger was (M = 3.35, SD = 0.61) na het zien van een communicatie-uiting over digitale privacy dan ervoor (M = 3.22, SD = 0.60). Er bleek geen interactie-effect tussen Affectieve respons en Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) = 3.30, p = .071). Tevens bleek er geen interactie-effect tussen Affectieve respons, Talige metaforen en Visuele metaforen (F (1, 162) = 1.04, p = .309).

Uit de tweeweg mixed design variantieanalyse van de nameting Talige metaforen en Visuele metaforen op Affectieve respons bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) = 1.34, p = .249) en Visuele metaforen (F (1, 162) = 1.68, p = .281). Tevens bleek geen significant interactie-effect op te treden tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). In de nameting waren er geen verschillen in affectieve respons tussen de verschillende condities met en zonder talige en visuele metaforen.

Gepercipieerd gevaar

De drie items van gepercipieerd gevaar bleken niet intern consistent, waardoor de drie items afzonderlijk van elkaar werden geanalyseerd. De items waren Social media risico's, E-mailbeveiliging en Cloudopslag.

Item 1: Social media risico's

Uit de tweeweg mixed design variantieanalyse voor Gepercipieerd gevaar met als binnen-proefpersoonfactor Social media risico's en tussen-proefpersoonfactoren Talige metaforen en Visuele metaforen bleken geen significant hoofdeffecten voor Social media risico's (F (1, 162) < 1), Talige metaforen (F (1, 162) > 1) en Visuele metaforen (F (1, 162) < 1). Er bleek tevens geen interactie-effect op te treden tussen Social media risico's, Talige en Visuele metaforen (F (1, 162) < 1). Het bleek dat de perceptie van social media risico's omtrent persoonlijke foto's gelijk bleef voor en na het zien van een communicatie-uiting over digitale privacy.

Uit de tweeweg mixed design variantieanalyse van de nameting Talige metaforen en Visuele metaforen op Social media risico's bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) <1). Tevens bleek geen significant interactie-effect op te treden tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). Er waren geen verschillen in de percepties van social media risico's omtrent persoonlijk foto's tussen de verschillende condities met en zonder talige en visuele metaforen.

Item 2: E-mailbeveiliging

Uit de tweeweg mixed design variantieanalyse voor Gepercipieerd gevaar met als binnen-proefpersoonfactor E-mailbeveiliging en tussen-proefpersoonfactoren Talige metaforen en Visuele metaforen bleken geen significant hoofdeffecten voor E-mailbeveiliging (F (1, 162) < 1). Er bleek geen interactie-effect tussen E-mailbeveiliging en Talige metaforen (F (1, 162) = 1.04, p = .310) en Visuele metaforen (F (1, 162) < 1). Er bleek tevens geen interactie-effect op te treden tussen E-mailbeveiliging, Talige en Visuele metaforen (F (1, 162) < 1). Het bleek dat het gebruik van een zwak e-mailaccountwachtwoord voor en na het zien van een communicatie-uiting over digitale privacy als even risicovol werd ervaren.

Uit de tweeweg mixed design variantieanalyse van de nameting Talige metaforen en Visuele metaforen op E-mailbeveiliging bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) <1). Tevens bleek geen significant interactie-effect op te treden tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). Het bleek dat er tussen de verschillende condities met en zonder talige en visuele metaforen geen verschillen waren op het gebruik van een zwak e-mailaccountwachtwoord.

Item 3: Cloudopslag

Uit de tweeweg mixed design variantieanalyse voor Gepercipieerd gevaar met als binnen-proefpersoonfactor Cloudopslag en tussen-proefpersoonfactoren Talige metaforen en Visuele metaforen bleek een significant hoofdeffecten voor Cloudopslag (F (1, 162) = 19.72, p < .001). Het bleek dat het opslaan van persoonlijke gegevens in een online cloud na het zien van een communicatie-uiting over digitale privacy (M = 3.31, SD = 0.88) als meer risicovol werd ervaren dan ervoor (M = 3.10, SD = 0.94). Er bleek geen interactie-effect tussen Cloudopslag en Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) < 1). Tevens bleek er geen interactie-effect op te treden tussen Cloudopslag, Talige en Visuele metaforen (F (1, 162) < 1).

Uit de tweeweg mixed design variantieanalyse van de nameting Talige metaforen en Visuele metaforen op Cloudopslag bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) = 1.72, p = .191) en Visuele metaforen (F (1, 162) <1). Tevens bleek geen significant interactie-effect op te treden tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). In de nameting waren er geen verschillen tussen de verschillende condities met en zonder talige en visuele metaforen bij het opslaan van persoonlijke gegevens in een online cloud.

Ernst van de gevolgen

Uit de tweeweg mixed design variantieanalyse voor Ernst van de gevolgen met als binnen-proefpersoonfactor Ernst van de gevolgen en tussen-proefpersoonfactoren Talige metaforen en Visuele metaforen bleken geen significante hoofdeffecten voor Ernst van de gevolgen (F (1, 162) < 1). Er trad geen interactie-effect op tussen Ernst van de gevolgen en Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) = 2.56, p = .111). Daarnaast bleek er geen interactie-effect tussen Ernst van de gevolgen, Talige metaforen en Visuele metaforen (F (1, 162) < 1). Het bleek dat de ernst van de gevolgen niet veranderde tussen voor en na het zien van een communicatie-uiting over digitale privacy.

Uit de tweeweg mixed design variantieanalyse van de nameting Talige metaforen en Visuele metaforen op Ernst van de gevolgen bleken geen significante hoofdeffecten van Talige metaforen (F (1, 162) < 1) en Visuele metaforen (F (1, 162) < 1). Tevens bleek geen significant interactie-effect op te treden tussen Talige metaforen en Visuele metaforen (F (1, 162) < 1). Er waren geen verschillen in de inschatting van de ernst van de gevolgen tussen de verschillende condities met en zonder talige en visuele metaforen.

Conclusie

Dit onderzoek beoogde te achterhalen of talige en visuele metaforen in communicatie-uitingen over digitale privacy effect hebben op de risicoperceptie en gedragsintenties van mensen. De hoofdvraag was: *wat is het effect van digitale privacy communicatie-uitingen met en zonder talige en visuele metaforen op de risicopercepties en gedragsintenties van mensen?*

Dit onderzoek vond geen overtuigend bewijs dat zowel talige als visuele metaforen effect hebben op hoe risico's bij communicatie-uitingen over digitale privacy worden ingeschat. Daarnaast bleek het gebruik van metaforen in digitale privacy communicatie-uitingen niet tot verschil in gedragsintenties bij de proefpersonen te leiden. In het experiment had de visuele metafoor wel invloed op de waardering van de boodschap. Mensen die een fusiemetafoor zagen waardeerden de communicatie-uiting over digitale privacy significant hoger dan bij een letterlijke communicatie-uiting.

Proefpersonen hebben na het zien van een communicatie-uiting over digitale privacy een hogere affectieve respons dan ervoor. Dit onderzoek vond bewijs dat een communicatie-uiting die appelleert aan risico's in het digitale privacy domein meer negatieve gevoelens kan opwekken. Er is daarom steun gevonden voor hypothese 1a. Hypothese 1b en 1c hadden ten doel te achterhalen of ook de inschatting van gepercipieerd gevaar en de ernst van de gevolgen verschillen van de voormeting. Voor h1b werd deels steun gevonden, aangezien het gebruik van cloudopslag met privégegevens na het zien van een van de communicatie-uitingen door proefpersonen als risicovoller werd gezien dan ervoor. Voor h1c werd daarentegen geen bewijs gevonden.

Hypothese 2a tot en met 2d hadden ten doel te achterhalen of talige metaforen effect hadden op de afhankelijke variabelen affectieve respons, gepercipieerd gevaar, ernst van de gevolgen en gedragsintenties. In dit experiment bleek dat talige metaforen geen verschillen toonden. Daarom zijn hypothese 2a tot en met 2d verworpen.

Om te achterhalen of visuele metaforen effect hebben op de risicoperceptie en gedragsintenties zijn h3a tot en met h3d onderzocht. Er is geen bewijs gevonden dat de affectieve respons, gepercipieerd gevaar, ernst van de gevolgen en gedragsintenties van elkaar verschillen. Daarom zijn h3a tot en met h3d verworpen.

Om te bepalen of er interactie-effecten zouden optreden tussen talige metaforen en visuele metaforen en de afhankelijke variabelen zijn h4a tot en met h4d opgesteld. Er bleek

geen steun gevonden te worden van interactie tussen talige metaforen en visuele metaforen en de afhankelijke variabelen affectieve respons, gepercipieerd gevaar, ernst van de gevolgen en gedragsintenties. Daarom zijn h4a tot en met h4d verworpen.

De controlevariabelen en de extra controlevraag hadden ten doel om een mogelijke verklaring te geven voor het al dan niet uitblijven van significantie op de onafhankelijke variabelen. De waardering van de communicatie-uiting met visuele metaforische ondersteuning was significant hoger dan de waardering met letterlijke beelden. Dit effect trad niet op bij de begrijpelijkheid, de overtuigingskracht en de extra controlevraag. Tevens trad er ook geen effect op door talige metaforen.

Digitale privacy communicatie-uitingen met of zonder talige en/of visuele metaforen leiden niet tot een verschil in risicopercepties. Daarnaast is geen bewijs gevonden dat talige en/of visuele metaforiek verschil maakt in gedragsintenties van de proefpersonen.

Discussie

Twee meta-analyses toonden aan dat talige metaforen kunnen leiden tot een hogere waardering van de boodschap (Van Stee, 2018; Sopory & Dillard, 2002). Echter, in dit onderzoek bleef een effect van talige metaforen op risicopercepties uit, ondanks de verwachtingen. Volgens onderzoek zouden talige metaforen via twee responstypen, namelijk elaboratie en verwerkingsplezier leiden tot meerdere impliciete associaties ten aanzien van een boodschap (Thibodeau, Hendricks & Boroditsky, 2017; McQuarrie & Mick, 1999). Op basis van deze theorie werd verwacht dat mensen verder reikende negatieve gedachtes zouden hebben over de metaforische boodschappen, die ervoor zouden zorgen dat ze de risico's als negatiever zouden inzien en daardoor een hogere risicoperceptie hebben.

Een mogelijke verklaring voor het uitblijven van een effect bij talige metaforen is dat de talige metafoor 'bewaak je digitale privacy' niet veel verschilde van de letterlijke boodschap 'bescherm je digitale privacy'. Echter, bewaken van je digitale privacy is een figuratieve metaforische linguïstische vervanging van beschermen van je privacy. Mensen bewaken hun digitale gegevens namelijk niet met een fysiek slot, hek of waakhond. Voor dit onderzoek is duidelijk de keuze gemaakt om de metafoor – het brondomein – dicht bij de werkelijke boodschap – het doeldomein – te houden, zodat bekeken kan worden of er verschillen optreden. In voorgaande studies zijn vaak opvallendere metaforen gebruikt die tegelijkertijd ook meer uitdaagde om te begrijpen (McQuarrie & Phillips, 2005; Phillips, 1997). Dit kwam voor in

zowel talige als visuele metaforen. In het onderzoek van McQuarrie en Phillips (2005) werd namelijk de kracht van een gootsteenontstopper vergeleken met de explosiekracht van een granaat. Phillips (1997) heeft daarnaast aangetoond dat mensen relatief eenvoudig in staat zijn een bron- en doeldomein, die ogenschijnlijk niets met elkaar te maken hebben, met elkaar te combineren om de boodschap te begrijpen. Het is voor vervolgstudies daarom interessant te achterhalen of het gebruik van een talige en visuele, waar het verschil tussen doel- en brondomein groter is, wel resulteert in verder reikende effecten tussen de condities.

De affectieve respons, gepercipieerd gevaar, ernst van de gevolgen en gedragsintenties waren niet hoger bij de condities met visuele metaforen. Dit onderzoek bevestigt wel dat visuele metaforen leiden tot een hogere waardering van de boodschap dan letterlijke afbeeldingen, zoals ook aangetoond in verschillende eerdere onderzoeken (Van Mulken et al., 2014; Hartman, 2012; Phillips & McQuarrie, 2004; McQuarrie & Mick, 1999). In een verwante studie over politiek en netneutraliteit met gebruik van metaforen bleek dat metaforen een positieve werken hebben op de waardering en boodschap kwaliteit (Hartman, 2012). Dankzij deze hogere waardering van de boodschap zouden meerdere verschillende positieve associaties opgewekt worden, maar daar toonde dit onderzoek geen bewijs voor. Tevens was er geen verschil bij begrijpelijkheid, overtuigingskracht en de extra controlevraag.

Het uitblijven van een effect op de risicoperceptie door visuele metaforen is mogelijk te verklaren doordat de fusiemetafoor een screensaver was en geen additioneel attribuut van de getoonde smartphone. Een screensaver is namelijk een standaardscherm op elke smartphone, wat er mogelijk voor zorgde dat mensen het als een normale screensaver konden gaan zien. Dit terwijl de getoonde screensaver met waakhond wel degelijk het doel had mensen alert of waakzamer te maken. Een voorbeeld waarbij het om een extra attribuut gaat in combinatie met de smartphone is een visuele weergave van een slot dat gewikkeld is om een smartphone.

In de studie van Van Mulken et al (2014) bleek een fusiemetafoor die middelmatig complex is de hoogste waardering te hebben, boven visuele metaforen die minder complex zijn of juist te complex. De fusiemetafoor in deze studie bleek redelijk eenvoudig te begrijpen, wat zou betekenen dat de visuele metafoor niet te complex was maar juist eerder eenvoudig. Een verklaring op basis van het onderzoek van Van Mulken et al (2014) is dat een fusiemetafoor meer zou moeten uitdagen dan de fusiemetafoor gebruikt in dit onderzoek, zodat de boodschap meer overtuigingskracht heeft en de boodschap de gedragsintenties verhoogt van mensen ten aanzien van digitale privacybescherming.

De gedragsintentie in de nameting verschilde niet tussen de condities. Het experiment bevatte geen vragen over de gedragsintentie in de voormeting. Wellicht zou de gedragsintentie voor versus na het zien van een communicatie-uiting over digitale privacy mogelijk verschillen. In vervolgonderzoek is het daarom wellicht interessant om de gedragsintentie in de voor- en nameting te onderzoeken, zodat het verschil in gedragsintenties door het zien van een communicatie-uiting over digitale privacy risico's zichtbaar wordt.

In de studie van Huurne en Gutteling (2008) werden in het FRIS-model de vragen afgestemd op risicovollere gebeurtenissen, namelijk het vervoeren van chemische vloeistoffen, beschreven volgens de studie van Slovic (1987). Volgens Slovic (1987) heeft de inschatting van risico's voornamelijk te maken met beschikbaarheidsheuristieken, waarmee een risico eerder als risicovol of minder risicovol kan worden gekenmerkt. Daarnaast spelen eerdere gebeurtenissen omtrent de risicovolle gebeurtenis een rol (Kahneman & Tversky, 1979). In dit onderzoek zou dat kunnen betekenen dat mensen weinig ervaring hebben met ernstige gebeurtenissen omtrent digitale privacy en dat de risico's daardoor niet als groot werden gezien.

Het uitblijven van verschillen in (ten dele) gepercipieerde angst en de ernst van de gevolgen zou ook te verklaren zijn aan het feit dat mensen een smartphone als 'veilig' ervaren. Bijvoorbeeld doordat mensen wachtwoorden of de vingerafdrukscanner gebruiken om toegang te krijgen tot de smartphone, maar men kan ook zelf bepalen welke apps ze installeren en welke niet. Veiligheid heb je daardoor als gebruiker voor een groot deel zelf in de hand. De werkelijke perceptie van digitale veiligheid zou daardoor mogelijk kunnen verschillen ten opzichte van dit onderzoek. In dit onderzoek werd de perceptie van digitale veiligheid tussen enigszins riskant en nogal riskant geschat. Het gebruik van mobiele apparaten die mogelijk onveiliger zijn dan smartphones, zoals laptops met een verouderd besturingssysteem of niet up-to-date software zouden wellicht andere resultaten kunnen tonen.

Uit vooronderzoek bleek dat mensen weinig bezig zijn met hun eigen digitale privacy (Mols & Janssen, 2017; Acquisti et al., 2015; Potzsch, 2009; Barnes, 2009). Daarnaast bleek dat Nederlanders verschillend aankijken tegen hun eigen digitale privacy (Mols & Janssen, 2017). Tevens bleek ook dat Nederlanders in vergelijking met andere EU-landen minder angstig zijn over hun digitale privacy. Wellicht is het zo dat doordat mensen er weinig mee bezig zijn, er meer nodig is om ze te overtuigen. Een vervolgonderzoek zou in meerdere verschillende landen kunnen plaatsvinden om te achterhalen of de gevonden resultaten per land

verschillen. Dat zou kunnen verklaren waarom in dit onderzoek bij Nederlandse mensen geen effect werd gevonden.

Daarnaast kan ook een ander frame gebruikt worden in de communicatie-uitingen, waarmee de ontvanger een bepaalde richting op gestuurd wordt (Entman, 1993). Met framing is het mogelijk om de dreiging van digitale privacy weer te geven als gevaar van buitenaf of als verdedigingsmechanisme. De ontvanger kan namelijk eenzelfde denkkader ontwikkelen en zodoende het als eng of minder angstig zien (Cappella & Jamieson, 1997; Gitlin, 1980). Het denkkader dat gebruikt is in dit onderzoek is meer gericht op verdedigen, zowel in de letterlijke boodschappen als de metaforische varianten. De verdediging komt tot uiting in het talige aspect 'beschermen' en 'bewaken', maar ook in de waakhond die afgebeeld is in twee condities. Daarnaast is de boodschap omschreven dat je je digitale privacy kunt beschermen, wat verwant is aan een winstframe, terwijl ook een verliesframe toegepast had kunnen worden. Bij een winstframe worden de positieve aspecten van het uitvoeren van gedrag benadrukt, terwijl in een verliesframe juist de negatieve gevolgen van het niet uitvoeren van gedrag worden benadrukt (Kahneman & Tversky, 1979). Een voorbeeld van een verliesframe is: "zonder digitale privacybescherming ben je kwetsbaar". Mensen gaan namelijk vaker risico's uit de weg bij winst, terwijl het tegenovergestelde gebeurt bij verlies (Kahneman & Tversky, 1979). Een vervolgstudie zou verschillende frametypes in combinatie met metaforen kunnen gebruiken om te achterhalen of het risicozoekende gedrag van mensen ook voorkomt in metaforen en in communicatie-uitingen over digitale privacy.

In dit onderzoek werd gebruikgemaakt van vier condities, elk verschillend door het gebruik van talige en visuele metaforen versus letterlijke boodschappen en afbeeldingen. Iedere proefpersoon zag slechts een van de vier condities, waardoor ze niet doorkregen waarop gemanipuleerd werd. Hierdoor waren de resultaten van elke conditie goed met elkaar vergelijkbaar en kon het effect van visuele en tekstuele metaforen geanalyseerd worden.

Het onderzoek bevatte echter geen manipulatiecheck. Daarentegen werd met de pretest geanalyseerd welke van de drie posters het meest figuurlijk en abstract was versus letterlijk en concreet. De poster die het meest figuurlijk en abstract was, werd gebruikt in het experiment. De manipulatiecheck is echter een hulpmiddel om te controleren of mensen wel of geen metafoor zagen in de condities. Deze gegevens zouden interessant geweest zijn om te analyseren, aangezien de talige metafoor op geen enkele variabele aantoonbaar verschilde van

de letterlijke boodschap. Dit terwijl de condities met een visuele metafoor een hogere waardering van de boodschap kregen.

Een alternatieve verklaring voor de onderzoeksresultaten is dat de digitale online vragenlijst over digitale privacy mensen mogelijk forceert om hun gedrag te koppelen met hun overtuigingen, waar een schriftelijke vragenlijst ze meer afstand van hun digitale gedrag kan bieden. De privacy paradox verklaart namelijk dat er tegenstrijdigheden bestaan tussen overtuigingen van mensen omtrent hun digitale privacy en welk gedrag ze daadwerkelijk vertonen (Mols & Janssen, 2017; Acquisti et al., 2015). Mensen vinden digitale privacy over het algemeen een belangrijk onderwerp, maar toch blijven mensen gebruikmaken van privacy onvriendelijke online tools. Het experiment uitvoeren door middel van een papieren vragenlijst heeft mogelijk als voordeel dat de onderzoeker de omgevingsfactoren van het experiment meer in hand heeft en dat kan de kwaliteit van het onderzoek ten goede komen.

Er is een andere alternatieve verklaring voor de onderzoeksresultaten waarbij de boodschappen op de meeste variabelen niet hoger scoorde na het zien van de boodschap. Proefpersonen konden zich mogelijk herinneren wat ze in de voormeting hadden ingevuld op de vragenlijst. Door middel van een dertig seconden durende zoek-de-verschillen-puzzeltje werd gepoogd de proefpersonen af te leiden, zodat de proefpersonen niet meer konden herinneren wat ze bij de vragen van de voormeting hebben ingevuld. De afleiding was wellicht voor een deel van de proefpersonen niet voldoende. Bij vervolgonderzoek zou daarom rekening gehouden kunnen worden met meer afleiding van de proefpersonen tussen de voor- en nameting.

Het is tevens raadzaam om het onderzoek in haar huidige staat opnieuw uit te voeren waarbij elke proefpersoon in een conditie meer dan een poster te zien krijgt, zodat ook geanalyseerd kan worden of er verschillen optreden tussen de posters. Het voordeel hiervan is dat onderzocht kan worden of het uitblijven van significante hoofd- en interactie-effecten veroorzaakt worden door één poster. Daarmee is het mogelijk om de onderzoeksresultaten meer generaliseerbaar te maken aan metaforiek, zodat de zogeheten *language-as-fixed-effect-fallacy* niet voorkomt (Clark, 1973). Deze fout beschrijft hoe ten onrechte een effect toegeschreven wordt aan een alomvattend talig construct, terwijl slechts één tekst of één poster is gebruikt in een onderzoek (Meuffels & Van den Bergh, 2005). Een experimenteel onderzoek waarbij één boodschap is gebruikt met een metafoor is nog onvoldoende bewijs dat metaforiek het effect verklaart.

In dit onderzoek werd verhuld doordat er twee nieuwe risicovolle onderwerpen werden geïntroduceerd die gingen over de digitale en mobiele wereld waarin wij leven, namelijk straling van mobiele apparaten en overmatige blootstelling aan felle digitale schermen. De onderwerpen konden nieuwe angst ontwikkelen en van beide onderwerpen is niet iedereen volledig op de hoogte. Daarom zou in vervolgonderzoek beter gekozen kunnen worden voor meer bekende risicovolle onderwerpen. Daarnaast hebben beide onderwerpen het risico dat het leidt tot ongunstige gezondheidseffecten op mensen, terwijl dit minder van aard is bij risico's omtrent digitale privacy. Het is mogelijk dat proefpersonen angstig werden door de onderwerpen die beiden over gezondheidsrisico's gingen. Ethisch gezien zouden wellicht onderwerpen die niet met gezondheidsrisico's te maken hebben beter passen in dit onderzoek.

Dit onderzoek draagt nieuwe inzichten aan over hoe metaforiek werkt in communicatie over digitale privacy. Daarnaast is dit de eerste studie die het effect van talige en visuele metaforen onderzocht op risicopercepties omtrent digitale privacy; een onderwerp dat steeds relevanter is voor de samenleving. Ook zijn studies naar talige en visuele metaforiek vaak niet gecombineerd, maar in deze studie is wel een mixed design toegepast door de voor- en nameting, wat de onderzoekbevindingen extra waardevol maakt voor de communicatiewetenschap. Echter, dit experimentele onderzoek heeft zich beperkt tot één communicatie-uiting, waardoor de resultaten niet generaliseerbaar zijn. Toch kan dit onderzoek gezien worden als een belangrijke stap in de richting van meer kennis over de werking van metaforen, specifiek in het digitale privacy domein.

Literatuurlijst

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*(2), 249–274. doi:10.1086/671754

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Age of information. *Science, 347*(6221), 509–515. doi:10.2139/ssrn.2580411

Ajzen, I. 1991. The theory of planned behaviour. *Organizational behaviour and human decision processes, 50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

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

Berlow, E., & Gourley, Sean. (2013). *Mapping ideas worth spreading* [TED]. Geraadpleegd op 10 maart 2018, van https://www.ted.com/talks/eric_berlow_and_sean_gourley_mapping_ideas_worth_spreading

Cappella, J. N., & Jamieson, K. H. (1997). *Spiral of cynicism. The press and the public good.* New York: Oxford University Press.

Chamorro-Premuzic, T. (2016). "Personality, privacy and our digital selves." *The Guardian.* Geraadpleegd op 10 november 2018, van https://www.theguardian.com/media-network/media-network-blog/2014/nov/10/online-privacy-digital-trust-psychology

Clark, H. H. (1973). The language-as-fixed-effect fallacy: A critique of language statistics in psychological research. *Journal of Verbal Learning & Verbal Behavior, 12,* 335-359. doi:10.1016/S0022-5371(73)80014-3

De Vries, N. K. (2002). Risico's en risicoperceptie. *Ned Tijdschr Tandheelkd 109,* 202-206.

Entman, Robert M. (1993). "Framing: toward clarification of a fractured paradigm."

Journal of Communications, 43(4), 51–58.

Field, A. P. (2015). *Discovering statistics using IBM SPSS Statistics* (4e editie). London: Sage.

Fisbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach.* New York: Psychology Press.

Gitlin, T. (1980). *The whole world is watching: Mass media in the making and unmaking of the new left.* Berkeley, CA: University of California Press.

Hartman, T. K. (2012). Toll booths on the information superhighway? Policy metaphors in the case of net neutrality. *Political Communication, 29*(3), 278–298. doi:10.1080/10584609.2012.694983

Hoeken, H., Hornikx, J., & Hustinx, L. (2012). *Overtuigende teksten: Onderzoek en ontwerp* (2e druk). Bussum: Coutinho.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society, 47*(2), 263-291. doi:10.2307/1914185

Kleinjan, G. J. (2018, 8 januari). Deze studenten strijden voor onze digitale privacy. *Trouw*. 8 Januari. Geraadpleegd op 1 maart 2018, van https://www.trouw.nl/democratie/deze-studenten-strijden-voor-onze-digitale-privacy~a6887407/

Lakoff, G., & Johnson, M. (1980). *Metaphors we live by*. Chicago, Ill.: University of Chicago Press.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: a revolution that will transform how we live, work, and think.* New York: Houghton Mifflin Harcourt.

McQuarrie, E. F., & Mick, D. G. (1996). Figures of rhetoric in advertising language. *Journal of Consumer Research, 22*(4), 424-438. doi:10.1086/209459

McQuarrie, E. F., & Mick, D. G. (1999). Visual rhetoric in advertising: Text-interpretive, experimental, and reader-response analyses. *Journal of Consumer Research, 26*(1), 37-54. doi:10.1086/209549

Meuffels, B., & Van den Bergh, H. (2005). De ene tekst is de andere niet. *Tijdschrift voor Taalbeheersing, 27*(2), 106-125. doi:10.5117/TVT2014.1.HORN

Mols, A., & Janssen, S. (2017). Not interesting enough to be followed by the NSA: an analysis of Dutch privacy attitudes. *Digital Journalism, 5*(3), 277–298. doi:10.1080/21670811.2016.1234938

Phillips, B. J. (1997). 'Thinking into it: consumer interpretation of complex advertising images', *Journal of Advertising, 26*(2), 77–87. doi:10.1080/00913367.1997.10673524

Phillips, B. J., & McQuarrie, E. F. (2004). Beyond visual metaphor: A new typology of visual rhetoric in advertising. *Marketing Theory, 4*(1–2), 113–136. doi:10.1177/1470593104044089

Pidgeon, N., Hood, C., Jones, D., Turner, B., & Gibson, R. (1992). *'Risk perception', in the royal society, risk: analysis, perception and management.* London: The Royal Society: 89-134.

Potzsch, S. (2009.) Privacy awareness: A means to solve the privacy paradox? The future of identity in the information society. *IFIP Advances in Information and Communication Technology, 298*, 226–236. doi:10.1080/21670811.2016.1234938

Radar. (2018, 23 maart). Uitslag definitief: Meeste stemmen tegen sleepwet. Geraadpleegd

op 1 juni 2018, van https://radar.avrotros.nl/nieuws/detail/uitslag-definitief-meeste-stemmen-tegen-sleepwet/

Richardson, D., & Matlock, T. (2007). The integration of figurative language and static depictions: An eye movement study of fictive motion. *Cognition, 102*(1), 129–138. doi:10.1016/j.cognition.2005.12.004

Scheufele, D. A., & Tewksbury, D. (2007). Framing, agenda setting, and priming: The evolution of three media effects models. *Journal of Communication, 57*, 9–20. doi:10.1111/j.1460-2466.2006.00326.x

Sopory, P., & Dillard, J. P. (2002). The persuasive effects of metaphor a meta-analysis. *Human Communication Research, 28*(3), 382–419. doi:10.1093/hcr/28.3.382

Slovic, P. 1987. Perception of risk. *Science,* 236(4799), 280–85. doi:10.1126/science.3563507

SIRE. (z.d.). Over SIRE. Geraadpleegd op 2 maart 2018, van https://sire.nl/over-sire/

Thibodeau, P. H., Hendricks, R. K., & Boroditsky, L. (2017). How linguistic metaphor scaffolds reasoning. *Trends in Cognitive Sciences, 21*(11), 852–863. doi:10.1016/j.tics.2017.07.001

Ter Huurne, E., & Gutteling, J. (2008). Information needs and risk perception as predictors of risk information seeking. *Journal of Risk Research, 11*(7), 847–862. doi:10.1080/13669870701875750

TNS Opinion & Social. (2015). *Special Eurobarometer 431 data protection.* (report). http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Van Enschot-van Dijk, R. V. (2006). *Retoriek in reclame: Waardering voor schema's en tropen in tekst en beeld.* (Doctoral dissertation, Radboud University, The Netherlands). http://repository.ubn.ru.nl/bitstream/handle/2066/27425/27425.pdf

Van Mulken, M., le Pair, R., & Forceville, C. (2010). The impact of perceived complexity, deviation and comprehension on the appreciation of visual metaphor in advertising across three European countries. *Journal of Pragmatics, 42*(12), 3418–3430. doi:10.1016/j.pragma.2010.04.030

Van Mulken, M., Van Hooft, A., & Nederstigt, U. (2014). Finding the tipping point: Visual metaphor and conceptual complexity in advertising. *Journal of Advertising, 43*(4), 333–343. doi:10.1080/00913367.2014.920283

Van Stee, S. K. (2018). Meta-analysis of the persuasive effects of metaphorical vs literal messages. *Communication Studies*, *0*(0), 1–22. doi:10.1080/10510974.2018.1457553

Bijlagen

Bijlage A: Online vragenlijst pretest

Beste deelnemer,

Bedankt voor je deelname aan dit vooronderzoek. Het onderzoek is opgesteld door Steven van de Cruijs, masterstudent Communicatie & Beïnvloeding aan de Universiteit in Nijmegen. In deze korte vragenlijst worden vragen gesteld waarbij jouw mening van belang is over drie verschillende posters. De duur van deze vragenlijst is enkele minuten. Jouw gegevens zullen anoniem blijven.

Heb je vragen of wil je meer weten over dit onderzoek? Neem dan contact op met: s.vandecruijs@student.ru.nl.

Steven van de Cruijs

Bekijk onderstaande poster aandachtig. Beantwoord daarna de vragen over de poster.

<Respondenten zien nu in gerandomiseerde volgorde alle drie de onderstaande posters. Na elke poster volgen steeds dezelfde vragen.>

Welke waardering geef je de boodschap van de poster?

- Zeer slecht (1)
- Slecht (2)
- Enigszins slecht (3)
- Noch goed, noch slecht (4)
- Enigszins goed (5)
- Goed (6)
- Zeer goed (7)

De poster zet mij aan het denken...

- Helemaal niet mee eens (1)
- Niet mee eens (2)
- Enigszins mee oneens (3)
- Noch eens noch oneens (4)
- Enigszins mee eens (5)
- Mee eens (6)
- Helemaal mee eens (7)

De boodschap is makkelijk te begrijpen…

- ○ Helemaal niet mee eens (1)
- ○ Niet mee eens (2)
- ○ Enigszins mee oneens (3)
- ○ Noch eens noch oneens (4)
- ○ Enigszins mee eens (5)
- ○ Mee eens (6)
- ○ Helemaal mee eens (7)

Wat maakt de boodschap volgens jou duidelijk?

_____

Ik vind de poster...

	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (7)	
Letterlijk	○	○	○	○	○	○	○	Figuurlijk
Concreet	○	○	○	○	○	○	○	Abstract

Geslacht Wat is je geslacht?

- ○ Man (1)
- ○ Vrouw (2)

Leeftijd Wat is je leeftijd

_____

Wat is je hoogst genoten opleidings niveau?

- ○ Basisonderwijs (1)
- ○ Middelbare school (lbo, vmbo, havo, vwo) (2)
- ○ Middelbaar beroepsonderwijs (mbo) (3)
- ○ Hoger beroepsonderwijs (hbo) (4)
- ○ Hoger Hoger Wetenschappelijk onderwijs (wo) (5)

Bijlage B: Online vragenlijst experiment

Hartelijk dank voor je deelname aan dit onderzoek. Het onderzoek wordt uitgevoerd door Steven van de Cruijs, masterstudent Communicatie- en Informatiewetenschappen aan de Radboud Universiteit Nijmegen. Ik wil je vragen stellen omtrent jouw mening over de mobiele en digitale wereld waarin wij leven en de risico's die daaraan verbonden zijn. Het invullen van de vragenlijst neemt circa 10 minuten in beslag. Indien je de vragenlijst volledig invult en je e-mailadres achterlaat, maak je kans op één van de drie Bol.com cadeaukaarten t.v.w. €10 euro.

De gegevens uit dit onderzoek blijven vertrouwelijk. Jouw antwoorden blijven te allen tijde dus anoniem. Je deelname is uiteraard vrijwillig en je kunt weigeren deel te nemen. Daarnaast ben je in de gelegenheid, indien je deelneemt, op elk moment te stoppen met dit onderzoek. In dat geval worden je data vernietigd. Enkel bij volledige invulling van de vragenlijst worden je data gebruikt voor dit onderzoek.

Het onderzoek kent geen juiste of onjuiste antwoorden. Enkel jouw mening telt.

Heb je vragen of opmerkingen over de vragenlijst? Neem dan contact op met Steven van de Cruijs (s.vandecruijs@student.ru.nl).

Bevestig hieronder je deelname aan dit onderzoek.

○ Ja, ik wil meedoen aan dit onderzoek

Wat is je leeftijd?

_____

Op de volgende pagina volgen de vragen over de mobiele en digitale wereld waarin wij leven.

Heb je in de afgelopen weken iets gehoord, gelezen of gezien over **digitale privacy**?

- ○ Zeker niet
- ○ Niet
- ○ Misschien
- ○ Wel
- ○ Zeker wel

Heb je in de afgelopen weken iets gehoord, gelezen of gezien over **straling van mobiele apparaten**?

- ○ Zeker niet
- ○ Niet
- ○ Misschien
- ○ Wel
- ○ Zeker wel

Heb je in de afgelopen weken iets gehoord, gelezen of gezien over **kijkgedrag naar digitale schermen**?

- ○ Zeker niet
- ○ Niet
- ○ Misschien
- ○ Wel
- ○ Zeker wel

Welke gevoelens heb je wanneer je denkt aan de mogelijkheid op **het verliezen van je digitale privacy door slechte beveiliging**? Dan voel ik mij...

	Helemaal niet	Nauwelijks	Enigszins	Nogal	Heel erg
Gespannen...	○	○	○	○	○
Angstig...	○	○	○	○	○
Bekwaam...	○	○	○	○	○
Aangenaam...	○	○	○	○	○
Bezorgd...	○	○	○	○	○
Rustig...	○	○	○	○	○

Welke gevoelens heb je wanneer je denkt aan de mogelijkheid op **een verslechterde algehele gezondheid door straling van mobiele apparaten**? Dan voel ik mij...

	Helemaal niet	Nauwelijks	Enigszins	Nogal	Heel erg
Gespannen...	○	○	○	○	○
Angstig...	○	○	○	○	○
Bekwaam...	○	○	○	○	○
Aangenaam...	○	○	○	○	○
Bezorgd...	○	○	○	○	○
Rustig...	○	○	○	○	○

Welke gevoelens heb je wanneer je denkt aan de mogelijkheid op **blijvende slechtziendheid door overmatig kijkgedrag naar digitale schermen**? Dan voel ik mij...

	Helemaal niet	Nauwelijks	Enigszins	Nogal	Heel erg
Gespannen...	○	○	○	○	○
Angstig...	○	○	○	○	○
Bekwaam...	○	○	○	○	○
Aangenaam...	○	○	○	○	○
Bezorgd...	○	○	○	○	○
Rustig...	○	○	○	○	○

De onderstaande vragen gaan over **digitale privacy**.

Hoe riskant is het volgens jou om persoonlijke foto’s via sociale media te delen?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou om een zwak wachtwoord te gebruiken voor je e-mailaccount?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou om je persoonlijke gegevens op te slaan in een digitale online cloud? (Denk bijvoorbeeld aan Dropbox, Google Drive of iCloud)

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

De onderstaande vragen gaan over **straling van mobiele apparaten.**

Hoe riskant is het volgens jou om je smartphone altijd in de nacht naast je hoofd op te laden?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou om dagelijks in een huis te leven waarbij de meeste apparaten draadloos met elkaar verbonden zijn?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou om dagelijks meer dan een half uur met je telefoon tegen je hoofd te bellen?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

De onderstaande vragen gaan over **kijken naar digitale schermen**.

Hoe riskant is het volgens jou om dagelijks voorgaande het slapen in bed nog een half uur naar je smartphonescherm te kijken?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou om dagelijks meer dan 5 uur per dag naar je smartphonescherm te kijken?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou als je jouw smartphonescherm altijd op de meest felle stand hebt?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Als kwaadwillenden mijn digitale persoonsgegevens misbruiken, dan zal het mijn leven enorm verstoren…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Enigszins
- ○ Nogal
- ○ Heel erg

Als kwaadwillenden mijn digitale persoonsgegevens misbruiken, dan zal dat ernstige gevolgen hebben in mijn netwerk…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Enigszins
- ○ Nogal
- ○ Heel erg

Als ik een gezondheidsaandoening krijg door straling van mobiele apparaten, dan zal het mijn leven enorm verstoren…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Enigzins
- ○ Nogal
- ○ Heel erg

Als ik een gezondheidsaandoening krijg door straling van mobiele apparaten, dan zal dat ernstige gevolgen hebben in mijn netwerk…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Misschien
- ○ Nogal
- ○ Heel erg

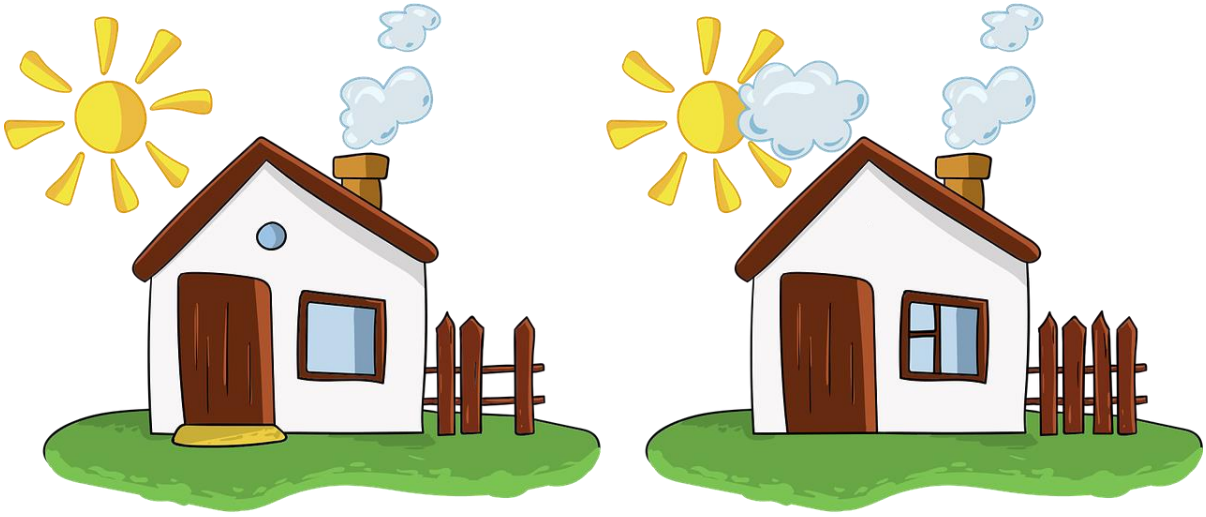
Als ik slechtziend word door overmatig kijken naar digitale schermen, dan zal het mijn leven enorm verstoren…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Misschien
- ○ Nogal
- ○ Heel erg

Als ik slechtziend word door overmatig kijken naar digitale schermen, dan zal dat ernstige gevolgen hebben in mijn netwerk…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Misschien
- ○ Nogal
- ○ Heel erg

Nu volgt een korte puzzel. Neem ongeveer 30 seconden de tijd om alle verschillen te vinden tussen de onderstaande afbeeldingen.



Hoeveel verschillen heb je gezien?

- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6

Je krijgt straks een poster te zien. Bekijk deze aandachtig. Daarna volgen enkele vragen. Na het klikken op 'volgende' kun je niet terugkeren.

<Respondenten zien nu één van onderstaande posters. Daarna volgen voor iedereen dezelfde vragen.>

Welke gevoelens heb je wanneer je denkt aan de mogelijkheid op **het verliezen van je digitale privacy door slechte beveiliging**? Dan voel ik mij...

	Helemaal niet	Nauwelijks	Enigszins	Nogal	Heel erg
Gespannen...	○	○	○	○	○
Angstig...	○	○	○	○	○
Bekwaam...	○	○	○	○	○
Aangenaam...	○	○	○	○	○
Bezorgd...	○	○	○	○	○
Rustig...	○	○	○	○	○

Hoe riskant is het volgens jou om persoonlijke foto’s via sociale media te delen?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou om een zwak wachtwoord te gebruiken voor je e-mailaccount?

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Hoe riskant is het volgens jou om je persoonlijke gegevens op te slaan in een digitale online cloud? (Denk bijvoorbeeld aan Dropbox, Google Drive of iCloud)

- ○ Helemaal niet riskant
- ○ Niet riskant
- ○ Misschien riskant
- ○ Nogal riskant
- ○ Heel riskant

Als kwaadwillenden mijn digitale persoonsgegevens misbruiken, dan zal het mijn leven enorm verstoren…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Enigszins
- ○ Nogal
- ○ Heel erg

Als kwaadwillenden mijn digitale persoonsgegevens misbruiken, dan zal dat ernstige gevolgen hebben in mijn netwerk…

- ○ Helemaal niet
- ○ Nauwelijks
- ○ Enigszins
- ○ Nogal
- ○ Heel erg

Nu volgen enkele vragen over de poster.

De poster vind ik…

	1	2	3	4	5	6	7	
Slecht	○	○	○	○	○	○	○	Goed
Onaantrekkelijk	○	○	○	○	○	○	○	Aantrekkelijk
Misleidend	○	○	○	○	○	○	○	Informatief
Voorspelbaar	○	○	○	○	○	○	○	Verrassend

De boodschap is makkelijk te begrijpen…

- ○ Helemaal mee oneens
- ○ Mee oneens
- ○ Enigszins mee oneens
- ○ Noch eens noch oneens
- ○ Enigszins mee eens
- ○ Mee eens
- ○ Helemaal mee eens

De poster brengt de boodschap duidelijk naar voren…

- ○ Helemaal mee oneens
- ○ Mee oneens
- ○ Enigszins mee oneens
- ○ Noch eens noch oneens
- ○ Enigszins mee eens
- ○ Mee eens
- ○ Helemaal mee eens

De poster maakt mij duidelijk wat de boodschapper wil vertellen…

- ○ Helemaal mee oneens
- ○ Mee oneens
- ○ Enigszins mee oneens
- ○ Noch eens noch oneens
- ○ Enigszins mee eens
- ○ Mee eens
- ○ Helemaal mee eens

Ik vind digitale privacy…

	1	2	3	4	5	6	7	
Onbelangrijk	○	○	○	○	○	○	○	Belangrijk
Irrelevant	○	○	○	○	○	○	○	Relevant
Oninteressant	○	○	○	○	○	○	○	Interessant
Zinloos	○	○	○	○	○	○	○	Zinvol

Het belang van digitale privacy wordt onderschat.

- ○ Helemaal niet mee eens
- ○ Niet mee eens
- ○ Enigszins mee oneens
- ○ Noch eens noch oneens
- ○ Enigszins mee eens
- ○ Mee eens
- ○ Helemaal mee eens

Ik zal mijn privacy instellingen op sociale media aanpassen…

- ○ Helemaal niet mee eens
- ○ Niet mee eens
- ○ Enigszins mee oneens
- ○ Noch eens noch oneens
- ○ Enigszins mee eens
- ○ Mee eens
- ○ Helemaal mee eens

Ik zal mijn accounts en digitale gegevens beter beschermen...

- ○ Helemaal niet mee eens
- ○ Niet mee eens
- ○ Enigszins mee oneens
- ○ Noch eens noch oneens
- ○ Enigszins mee eens
- ○ Mee eens
- ○ Helemaal mee eens

Ik zal minder persoonlijke gegevens digitaal verspreiden…

- ○ Helemaal niet mee eens
- ○ Niet mee eens
- ○ Enigszins mee oneens

- ○ Noch eens noch oneens
- ○ Enigszins mee eens
- ○ Mee eens
- ○ Helemaal mee eens

<Einde van de het pad per conditie>

Bijna klaar... Nog enkele demografische gegevens.

Wat is je geslacht?

- ○ Man
- ○ Vrouw
- ○ Anders

Wat is je hoogst genoten opleidingsniveau?

- ○ Basisonderwijs
- ○ Middelbare school (lbo, vmbo, havo, vwo)
- ○ Middelbaar beroepsonderwijs (mbo)
- ○ Hoger beroepsonderwijs (hbo)
- ○ Wetenschappelijk onderwijs (wo)

Indien je één van de drie Bol.com cadeaukaarten wilt winnen, vul je e-mailadres in.

_____