Bachelor Scriptie - Thesis Hub Bachelor Economics – FEB63006

Vertrouwenspercepties van online privacy en -security

Erasmus School of Economics - 16-10-2020

Student: Uz, E.S.

Studentnummer: 456614

Eerste beoordelaar: Hasselt, M.J.L. van

Tweede beoordelaar: Barendregt, A.T.

Inhoudsopgave

Executive Summary

Er blijkt een verschil te bestaan tussen het werkelijke- en waargenomen vertrouwen in online privacy. Binnen deze studie wordt gefocust op het analyseren van het subjectieve vertrouwen in online privacy, door de determinanten te achterhalen die dit vertrouwen beïnvloeden. De onderzoeksvraag luidt daarom als volgt: *welke determinanten leiden tot het verhogen van het subjectieve vertrouwen in online privacy?* Het onderzoek bestaat uit een onderbouwing voor de maatschappelijke- en wetenschappelijke relevantie, literatuuronderzoek, kwalitatief- en kwantitatief onderzoek, conclusie, tekortkomingen en aanbevelingen.

Eerdere onderzoeken hebben het vertrouwen in privacy als één aspect behandeld met mogelijke invloeden op het koopgedrag. Wel is er al onderzoek gedaan naar, of het waargenomen vertrouwen en waargenomen risico een positief dan wel negatief effect hebben op het vertrouwen. Echter is er geen duidelijke uiteenzetting van de specifieke factoren die het waargenomen vertrouwen vormen. Ook de mate waarin de factoren het subjectieve vertrouwen in privacy beïnvloeden zijn niet weergegeven. Het uitgangspunt van dit onderzoek is om bedrijven en organisaties meer inzicht te bieden over de vorming van het gevoel van vertrouwen in privacy. Met als reden om hen te ondersteunen bij het formuleren van een optimaal functionerende privacyregelgeving en gebruiksvriendelijke website. Dit is mogelijk door de attributen die significant van invloed zijn op het subjectieve vertrouwen in privacy mee te nemen in de totstandkoming van dit subjectieve vertrouwen.

In het literatuuronderzoek wordt het fenomeen “privacy paradox” uitgebreid behandeld, door verschillende studies en meningen naast elkaar te zetten. De privacy paradox verwijst naar de tegenstrijdigheid tussen de bezorgdheden rondom privacy en het werkelijke gedrag rondom privacy. Oftewel, hoewel beweerd wordt dat men zich grote zorgen maakt over hun privacy, wordt toch relatief weinig actie ondernemen om persoonlijke gegevens te beschermen. Het antwoord op deelvraag 1 of er een verband bestaat tussen de waargenomen bezorgdheden in privacy en het werkelijke gedrag wordt in dit stuk uitgelicht. Het is gebleken dat het wel of niet bestaan van de paradox context-afhankelijk is.

Uit het kwalitatief onderzoek blijkt dat er vraag bestaat naar een 100% veilige applicatie. Technisch gezien is dit waarschijnlijk onhaalbaar, maar in dit onderzoek is ernaar gevraagd indien het realiseerbaar zou zijn. De 100% veilige app heeft in dit onderzoek betrekking op een app met de volgende kenmerken: 100% virusvrij, 100% overheidsdetectie-vrij, 100% cookies-vermindering en 100% advertentievermindering. Verdere resultaten van het kwalitatief onderzoek wijzen erop dat het overgrote deel van de ondervraagden onbekend zijn met het proces van datawerving en -verspreiding en de consequenties van onveilig internetgebruik. Hiermee is antwoord gegeven op deelvraag 2: in hoeverre zijn internetgebruikers op de hoogte van online gevaren en hoe gedragen ze zich ernaar? Verder wordt de volgende stelling die gevormd is in het literatuuronderzoek verworpen: de privacyvoorwaarden hebben een positief effect op het subjectieve vertrouwen.

In het kwantitatief onderzoek is naar voren gekomen dat het subjectieve vertrouwen in privacy al beïnvloed kan worden door slechts een ondervraging naar het subjectieve vertrouwen met behulp van een enquête. Dit is gebleken doordat ongeveer een kwart van de deelnemers een negatief gevoel en de andere kwart een positief gevoel heeft beleefd. Verder worden betaalgegevens, camerabeelden/foto's, inloggegevens en Whatsapp-berichten/ SMS/ mail als belangrijkste type data beschouwd. De entiteiten die het minst vertrouwt worden zijn bedrijven gevolgd door overheden en als laatst hackers.

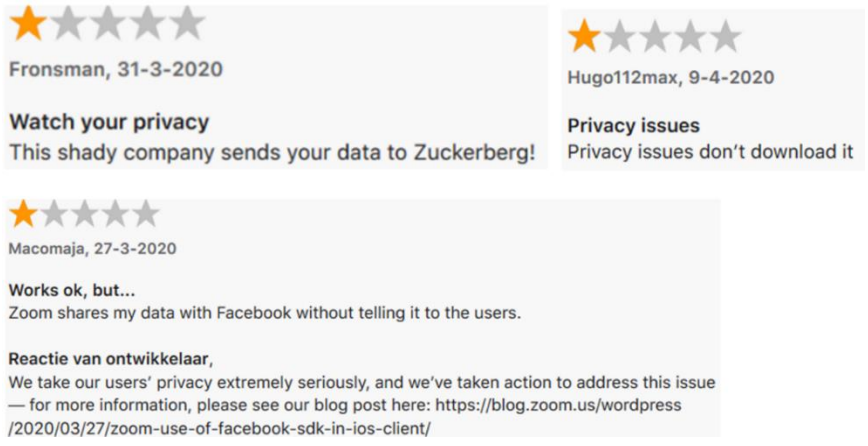
Het online veiligheidsgevoel is opgemeten in een voor- en nameting. Deze beoordeling van het subjectieve vertrouwen heeft in de voormeting zonder context een *rating* van 52.44. Vergeleken met de constante van de conjoint analyse van 42.62 wordt dit hoger gewaardeerd. Hieraan kunnen twee redenen ten grondslag liggen. Of de conjoint analyse geeft exactere inschattingen weer door de bijbehorende specifieke context of er is sprake van een *confirmation bias*. De attributen die het meest gewaardeerd worden in de 100% veilige app zijn een lage prijs en virusvrije internet. Overheidsdetectievrije internet wordt ook erg gewaardeerd, maar alleen indien het 100% beveiligd is. Als laatst, de omzet maximaliserende prijs voor de 100% veilige app beschreven in dit onderzoek is €10. Kortom, deelvraag 3 en 4 waarin gevraagd wordt of er een betalingsbereidheid bestaat voor de app en welke attributen het gevoel van vertrouwen beïnvloeden worden in dit deel beantwoord.

1. Theoretisch Kader

1.1 Probleembeschrijving

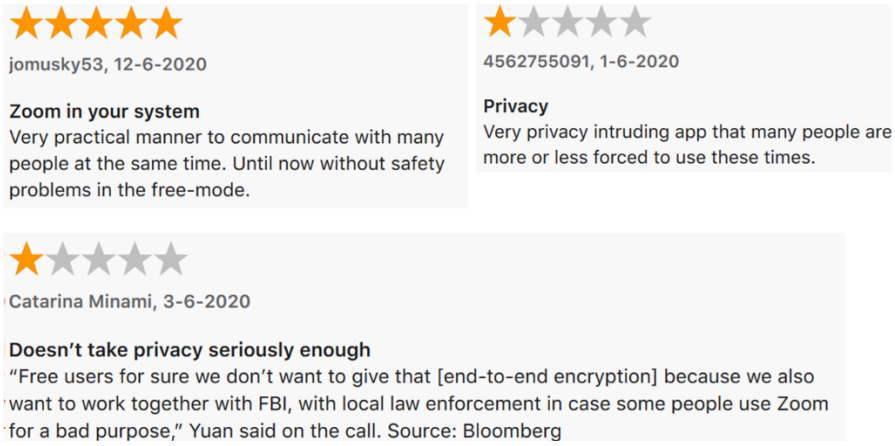
Het internet heeft een groot aantal positieve producten en services waar een gebruiker voordeel bij kan hebben. Het internet kan tijd- en kostenbesparend werken. In de laatste vijf jaar zijn de verkopen via internet aan Nederlandse consumenten bijna verdubbeld (CBS, 2020). De groei van internet geeft steeds meer nieuwe mogelijkheden waar zowel bedrijven als consumenten van kunnen profiteren (Mandic, 2009). Het bewustzijn van de gebreken en de gevaren voor privacy en security van internetgebruik lijkt daarentegen veel lager.

Meer en meer internetgebruikers beginnen de consequenties in te zien van niet goed genoeg beschermde sites en applicaties. Een voorbeeld dat op dit moment speelt is de Zoom app. In de eerste maanden van 2020 is vanuit huis werken onontkoombaar geworden door de uitbraak van het COVID-19 virus. Dit betekent dat instituten, zoals universiteiten en bedrijven, massaal overgaan op het gebruik van videobellen. Zoom is een van de applicaties die het mogelijk maakt om met grote groepen te videobellen. Het blijkt nu dat persoonlijke data van Zoom-gebruikers zijn gelekt, waardoor er enorme ophef ontstond onder de afnemers. Honderden Nederlandse scholen verbieden hierom het videobellen met de Zoom applicatie (RTLNieuws Contributors, 2020). In figuur 1 zijn ter illustratie enkele reviews over de datalek van de Zoom app weergegeven die verkregen zijn uit de App store (2020). Zoom heeft haar privacy statement aangepast vanaf 29 maart 2020, (Louw, 2020). Uit de recensies na de aanpassing van de privacy statement blijkt dat er alsnog met argwaan gekeken wordt naar de app (figuur 2).



Figuur 1: Recencies over de Zoom app omtrent privacyproblemen en de reactie van Zoom (rondom het moment van de privacy statement verandering).

De subjectieve vorm van vertrouwen lijkt tevens beschadigd te zijn wanneer de reacties, rondom- en na de verandering van de privacy statement, vergeleken worden. Wel is er enigszins herstel te bemerken van de schade aan het subjectieve vertrouwingsgevoel en het blijkt dat kritiek vaker wordt geuit over de funtionaliteiten van de app dan over de privacykwesties (App Store, 2020).



Figuur 2: Recensies over de Zoom app na de verandering van de privacy statement.

Net als Zoom zijn er vele andere online bedrijven die gegevens verzamelen zonder dat de gebruiker bewust is van wat er werkelijk gebeurt met hun persoonlijke data. Ook na de ophef over de Zoom app, gebruiken mensen massaal vergelijkbare apps. Dit leidt tot het thema van deze thesis: hoe is het gesteld met de subjectieve beoordeling van vertrouwen in online privacy?

1.2 Onderzoeksvraag

Zoals Acquisti, Brandimarte, & Loewenstein (2015) beschreven: "Als dit het informatietijdperk is, is databescherming de kwestie van onze tijd". Van online webwinkels, zoekmachines, gamewerelden, blogs, vlogs tot datingssites; informatie is overal vrij eenvoudig en snel verkrijgbaar. Het feit dat het internet veel ruimte biedt om snel en efficiënt een uitwisseling te doen, betekent niet dat deze datanetwerk slechts gebruikt zal worden voor legale doeleinden. Zowel individuen, bedrijven en overheden profiteren van de functionaliteiten van het internet. Echter kunnen dezelfde partijen veel schade oplopen, als hun data in verkeerde handen vallen. Hackers, virussen en datalekkages zijn potentiële gevaren voor deze groepen.

Verder blijkt dat onder internetgebruikers er een verschil bestaat tussen het werkelijke- en het waargenomen vertrouwen in privacybeschermingsprotocollen (Pavlou, 2003). Dit onderzoek zal

zich vooral focussen op het meten van het subjectief waargenomen vertrouwen in privacy. Het is noodzakelijk om hiervoor het verschil tussen het werkelijke vertrouwen in privacy en waargenomen vertrouwen in privacy uiteen te zetten. Dit is uitgewerkt in het literatuuronderzoek.

Dit probleem brengt de volgende onderzoeksvraag te boven: *Welke determinanten leiden tot het verhogen van het subjectieve vertrouwen in online privacy?* Verdere inhoud van het onderzoek is als volgt georganiseerd: als eerst wordt een uitgebreide definitie gegeven van online privacy en -veiligheid, waarna de wetenschappelijke relevantie en maatschappelijke relevantie uiteengezet worden. Vervolgens worden na diepgaande onderzoeken naar het privacy paradox in het literatuuronderzoek de methodologie en de resultaten belicht. De resultaten worden opgedeeld in het kwalitatief- en het kwantitatief onderzoek. De laatste sectie biedt een discussie van de resultaten met inbegrip van de tekortkomingen en aanbevelingen voor een vervolgonderzoek.

1.3 Online privacy en -veiligheid

Er zal van tevoren een uitgebreide definitie van privacy en veiligheid verstrekt worden om naderhand verwarring te voorkomen. Mandic (2009) omschrijft duidelijk het verschil tussen privacy en veiligheid. Privacy is de bescherming van persoonlijke informatie. Het online beschermen van persoonsgegevens is dan gerelateerd aan de beleidslijnen van bedrijven betreffende het gebruik van consumentendata dat verworven is van het internet. Een belangrijke factor voor privacy is consumenten toestemming, oftewel dat aan de consument de keus wordt gegeven om te bepalen waarvoor zijn persoonlijke informatie gebruikt wordt. Terwijl privacy duidt op de legale vereisten waar het aan moet voldoen rondom het managen van persoonlijke data, wijst veiligheid op de technische aspecten die dit mogelijk maken, aldus Mandic (2009). Hierbij kan gedacht worden aan het gebruik van methoden, zoals encryptie.

Het begrip privacy verwijst in deze studie naar de informationele privacy, zoals gedefinieerd door Holvast (1993). Informationele privacy heeft betrekking op het beheersen van hoe persoonlijke data worden verzameld, opgeslagen, verwerkt en verspreid. Online informationele privacy is dan de controle van deze gegevens, maar dan op het internet.

1.4 Wetenschappelijke relevantie

Eerdere studies hebben zich vooral gefocust op de bepalende factoren bij het verwerkelijken van online-aankopen, gegevensverstrekking op *social media* en de relatie tussen bezorgdheden over privacy en werkelijk gedrag. In grote lijnen is beschreven dat online-transacties voordelen kennen, op *social media* bepaalde *trade-offs* worden gemaakt en dat er een tegenstrijdigheid bestaat tussen de bezorgdheden rondom privacy en het feitelijke gedrag van mensen. Hieronder vallen als voorbeeld de snelle levertijden, het vormen van een sociale imago en de privacy paradox.

Bovendien zijn tot op het heden veel onderzoeken gedaan naar de directe effecten die de bezorgdheden in privacy hebben op de neiging om een online-transactie te verrichten. Hieruit blijkt dat consumentenvertrouwen in de leverancier cruciaal is voor het verwerkelijken van een online aankoop. Ook blijken waargenomen privacy en waargenomen veiligheid de belangrijkste factoren te zijn voor het vormen van vertrouwen in een online-aankoop (Fortes & Rita, 2016). Er is een overvloed aan bewijs dat vertrouwen in een online omgeving een belangrijke factor is voor het doen van een transactie. Echter, er is weinig onderzoek gedaan naar de specifieke determinanten die van invloed zijn op het subjectieve vertrouwen in privacy.

Met dit onderzoek wordt beoogd privacy op te splitsen in meerdere kenmerken om te onderzoeken waaruit het vertrouwen in privacy bestaat. Eerdere onderzoeken hebben het vertrouwen in privacy als één aspect behandeld met mogelijke invloeden op het koopgedrag. Dit onderzoek zal inzoomen op de aspecten van online privacy en -veiligheid om te achterhalen welke attributen in welke mate het subjectief waargenomen vertrouwen in privacy beïnvloeden.

De resultaten bieden nieuwe inzichten over de waardering van persoonlijke gegevens. Er is wel al onderzoek gedaan naar of het waargenomen vertrouwen en waargenomen risico een positief dan wel negatief effect hebben op het vertrouwen. Echter is er geen duidelijke uiteenzetting van de specifieke factoren die het waargenomen vertrouwen vormen. Ook de mate waarin de factoren het gevoel van vertrouwen in privacy beïnvloeden zijn niet weergegeven.

1.5 Maatschappelijke relevantie

Het uitgangspunt van dit onderzoek is om bedrijven en organisaties meer inzicht te bieden over de vorming van het subjectieve vertrouwen in privacy om hen te ondersteunen bij het formuleren van een optimaal functionerende privacyregelgeving en gebruiksvriendelijke website. Dit is mogelijk door de attributen die significant van invloed zijn op het gevoel van vertrouwen in privacy mee te nemen in de totstandkoming van dit subjectieve vertrouwen.

Het is cruciaal om het subjectieve vertrouwen in privacy te onderzoeken, vanwege het indirecte effect dat dit gevoel van vertrouwen heeft op de neiging om een aankoop te doen. Het basisprincipe hiervoor is dat het waargenomen vertrouwen beïnvloed wordt door de waargenomen hoeveelheid veiligheid en waargenomen hoeveelheid privacy. Het waargenomen vertrouwen is op zijn beurt weer van invloed op de neiging om een aankoop te verrichten (Fortes & Rita, 2016). Dus de resultaten van dit onderzoek kunnen bijdragen aan het vormen van een betere marketingstrategie. Door rekening te houden met de attributen die een significant effect hebben op het subjectieve vertrouwen in privacy en deze op te nemen in de bedrijfsuitoefening kunnen verhoogde omzetten gerealiseerd worden.

De resultaten leveren nieuwe inzichten op voor twee specifieke partijen waarvoor het belangrijk is om het gevoel van vertrouwen in privacy nader te onderzoeken. Dit betreffen bedrijven en beleidsmakers. Deze twee entiteiten verkeren zich mogelijkerwijs in een belangenconflict met betrekking tot het verzamelen van persoonlijke data (Kokolakis, 2017). Enerzijds zullen bedrijven, indien de privacy paradox werkelijk bestaat, rechtvaardigen dat personen in werkelijkheid niet even bezorgd zijn om hun gegevens als ze aangeven. Bedrijven zullen hierdoor motiveren dat het verzamelen van persoonlijke data toegelaten moet worden voor het streven naar eigenbelang. Dankzij de verkregen data kan bijvoorbeeld meer gepersonaliseerd geadverteerd worden en is het mogelijk de data door te verkopen aan derden. Anderzijds zijn beleidsmakers verantwoordelijk voor het voldoen aan de verwachtingen van de vertegenwoordigden en kunnen derhalve ingaan op de bestaande bezorgdheden rondom privacy om deze te temperen. Dit kan het vormen van striktere wet- en regelgeving als gevolg hebben voor het verzamelen en gebruiken van data door bedrijven.

Bovendien kunnen bedrijven en organisaties proberen de "100% veilige app" te ontwikkelen om er winst mee te maken, aangezien in dit onderzoek is gebleken dat daar vraag naar is. Technisch gezien is dit waarschijnlijk onhaalbaar, maar in dit onderzoek is ernaar gevraagd indien het realiseerbaar zou zijn. De 100% veilige app in dit onderzoek heeft betrekking op een applicatie met de volgende kenmerken: 100% virusvrij, 100% overheidsdetectie-vrij, 100% cookies-vermindering en 100% advertentievermindering.

1.6 Subvragen:

De bijbehorende deelvragen die onderzocht zullen worden in het onderzoek zijn:

1) Wat is het verband tussen de waargenomen bezorgdheden in privacy en het werkelijke gedrag?
2) In hoeverre zijn internetgebruikers op de hoogte van online gevaren en hoe gedragen ze zich ernaar?
3) Zijn internetgebruikers bereid om te betalen voor het concept van een 100% veilige premium app (indien te verwerkelijken)? Zo ja, wat is de maximale betalingsbereidheid?
4) Welke attributen beïnvloeden de waarneming van het gevoel van vertrouwen in online privacy en databescherming, en in welke mate?

1.7 Mogelijke beperkingen

Wegens de sociale beperkingen die zijn ingevoerd tijdens de coronacrisis om risico's van besmetting en verspreiding te voorkomen, zullen de interviews gevoerd worden via de telefoon en chats. Het communicatieproces zal daarom lastiger verlopen en onpersoonlijker overkomen op anderen. Dit zal mogelijk de resultaten uit de interviews beïnvloeden. Ook de bevindingen van de enquêtes zouden aangetast kunnen worden, omdat ze zijn gebaseerd op de mogelijk incomplete interviews. Wederom, met als reden voorbehoedend te handelen met betrekking tot het virus, zullen de enquêtes online opgestuurd en ingevuld worden, wat het fysiek verspreiden van enquêtes in openbare plekken onmogelijk maakt. Er bestaat een gedeelte van de bevolking die om welke reden dan ook geen gebruik maakt van het internet (CBS, 2018) en zij worden daarom

van het onderzoek uitgesloten. Het onderzoek is op dat gebied dus niet representatief genoeg. Juist degenen die geen gebruik maken van internet zijn interessante cases om te onderzoeken, omdat het mogelijk is dat ze geen internet gebruiken vanwege het gebrek aan vertrouwen in privacy- en veiligheidsmaatregelen.

Verder kan het zijn dat de conjoint analyse niet alle kenmerken bevat waar internetgebruikers hun keuzes op baseren die invloed uitoefenen op het subjectieve vertrouwen in privacy. Variabelen die niet opgenomen zijn in het model, bijvoorbeeld de opslag van de app, kunnen ook de *rating* van de app beïnvloeden. Deze variabelen kunnen meegenomen worden voor een vervolgonderzoek. Verder is het vrij aannemelijk dat het beantwoorden van 15 vergelijkbare conjoint vragen vermoeidheidseffecten met zich mee kan brengen. Respondenten zullen hierdoor vragen onserieus invullen of zelfs overslaan wat de betrouwbaarheid van de resultaten aantast. Als laatst, het is aannemelijk dat er sprake kan zijn van een *bias* in de gegeven antwoorden van de enquête. Het feit dat er vragen worden gesteld over het aspect van vertrouwen op internet kan het bewustzijn over dit onderwerp aanwakkeren en beïnvloeden. Dit kan ertoe leiden dat de deelnemers meer alert antwoorden vergeleken met een scenario waarin het gedrag vooraf totaal niet beïnvloed wordt. Het kan zijn dat iemand niet bewust is van zijn angst over het internet totdat ernaar gevraagd wordt. Om dit effect te analyseren is zowel aan het begin als aan het einde van de enquête gevraagd naar hoe veilig de deelnemers zich voelen op internet.

2. Literatuuronderzoek

Zoals eerder aangegeven bestaat er een verschil in het waargenomen vertrouwen en werkelijke vertrouwen. Het is van belang om het verschil en de relatie tussen het subjectief waargenomen vertrouwen en het werkelijk vertoonde vertrouwen te begrijpen en te kunnen herkennen onder welke omstandigheden het plaatsvindt. Het is mogelijk dat er een tegenstrijdigheid bestaat in de manier waarop personen hun bezorgdheden uiten over privacy en hun feitelijk gedrag met betrekking tot het veiligstellen van hun privacy (Acquisti & Grossklags 2005). Dit verschijnsel wordt ook wel de 'privacy paradox' genoemd. Er bestaan zowel studies die deze paradox bevestigen als studies die dit verwerpen, waarvan enkele in dit onderzoek behandeld zullen worden.

Eerder zijn de verschillende belangen van beleidsmakers en gegevensverzamelaars, zoals bedrijven, over het recht op gebruik van data uiteengezet. Ter aanvulling hierop blijkt dat 64% van senior marketingleiders niet denken dat de regulaties zullen worden aangescherpt voor het verzamelen van data. Niettemin hebben 50% van de consumenten aangegeven online minder actief te zijn wegens privacy bezorgdheden (Boudet, 2020). Indien de relatie wordt achterhaald kunnen duidelijke regels opgesteld worden aangaande het verzamelen en gebruiken van (consumenten)data.

Studies voor privacy paradox

De grondleggers voor de privacy paradox zijn met name Norberg et al. (2007). Samen met andere collega's heeft Norberg twee experimenten uitgevoerd. In het eerste stadium van het eerste experiment zijn studenten getoetst op de bereidheid om persoonlijke informatie te onthullen. Het tweede stadium heeft enkele weken later plaatsgevonden. In een dialoog met een marktonderzoeker zijn de deelnemers gevraagd soortgelijke informatie vrij te geven, waaruit is gebleken dat de betrokkenen een aanzienlijk groter hoeveelheid aan persoonlijke informatie hebben geopenbaard dan is aangegeven. In een tweede vervolgexperiment met dezelfde toegepaste methodologie zijn twee soorten relaties geanalyseerd. De eerste relatie heeft betrekking op het effect van waargenomen risico's op de bereidheid om persoonlijke informatie te verstrekken en de tweede relatie op het effect van waargenomen vertrouwen op het feitelijk

vertoonde gedrag. Hieruit is bevestigd dat de waargenomen risico's een significant effect uitoefenen op de bereidheid om persoonlijke informatie vrij te geven. Echter is er geen verband gevonden tussen het waargenomen vertrouwen en het werkelijk vertoonde gedrag.

In een studie van Brown (2001) zijn door middel van diepgaande interviews met online-consumenten de zorgen van de gebruikers onderzocht met betrekking tot online-privacy en -veiligheid. Zowel de populariteit van online-shoppen als de zorgen om privacy zijn merkbaar gestegen. Brown herkent de privacy paradox in dit verschijnsel. Terwijl online-consumenten hebben aangegeven bezorgd te zijn over hun online-privacy, zijn ze toch bereid om hun persoonlijke informatie af te staan aan webwinkels. Zolang de consumenten baat hebben bij de transactie en er iets voor terug krijgen zijn transacties voortgezet. Athey et al. (2017) heeft bovendien in een onderzoek vermeldt dat kleine prikkels ervoor kunnen zorgen dat individuen eerder persoonsgegevens vrijgeven dan ze aangeven om te willen delen. Ook is bekendgemaakt dat de individuen hebben gevreesd dat er te veel informatie over hen is verzameld. Toch is dit voor hen geen reden geweest om zich te weerhouden van het realiseren van online-aankopen (Brown, 2001).

Spiekermann et al. hebben in 2001 de uitkomsten van een experiment uiteengezet over de relatie tussen de aangegeven privacy-voorkeuren en het feitelijk gedrag rondom privacy met betrekking tot online koopgedrag. Allereerst zijn de participanten in het experiment gevraagd om een enquête in te vullen over hun bezorgheden over privacy. Vervolgens zijn de ze verzocht een online-webwinkel te bezoeken, waarin een gesprek gestart is met een robot. Tijdens het contact met de robot is gebleken dat op de vrij persoonlijke vragen door het merendeel antwoord is gegeven. Dit suggereert dat terwijl internetgebruikers beweren dat online-privacy van hoge prioriteit voor ze is, ze zich niet naar behoren gedragen.

Een mogelijke verklaring voor de tegenstrijdigheid tussen de aangegeven bezorgdheden over privacy en de werkelijk onthulde informatie is de *immediate gratification* (onmiddelijke bevrediging) *bias*, aldus (Acquisti, 2004). Deze *bias* verwijst naar de neiging om de huidige baten hoger te waarderen dan de toekomstige risico's. Dus voor individuen wegen de huidige baten van informatieverstrekking zwaarder dan de toekomstige risico's wat betreft privacy. Barth & de Jong

(2017) bevestigen het bestaan van een risico-baten evaluatie onder individuen als het gaat om het vrijgeven van gegevens. Ook is aangegeven dat bepaalde individuen het onrealistisch kunnen vinden om zich te beschermen tegen ieder mogelijke inbreuk op de privacy. Het is daarom aanneembaar dat individuen niet bereid zijn om een methode ter bescherming voor privacy te hanteren, omdat te betwijfelen valt of dit zal helpen (Acquisti, 2004). Hallam & Zanella (2017) zien hier een andere *bias* in, welke betrekking heeft op de afstand van het heden en de toekomst. Zo stellen zij dat individuen de sociale baten van het vrijgeven van informatie waarnemen als het meer concrete heden. De privacy risico's worden echter gezien als in een abstract en psychologisch verre toekomst.

In het onderzoek van Beresford et al. (2012) zijn deelnemers verzocht om een keuze te maken voor het kopen van een DVD tussen twee identieke webwinkels. Het verschil tussen de winkels is het soort informatie dat verstrekt moet worden bij een aankoop van een DVD. De eerste winkel vereist relatief meer gevoelige informatie. De te verstrekken informatie omvat enerzijds het inkomen en geboortedatum en anderzijds de lievelingskleur en geboortejaar, voor respectievelijk winkel één en winkel twee. De resultaten tonen dat bij een gelijk gehanteerde prijs voor een DVD in beide winkels, dezelfde hoeveelheid klanten een aankoop doen in de winkels. Echter, bij een prijsdaling van één euro in winkel één hebben vrijwel alle deelnemers de transactie verwerkelijkt bij de eerste winkel, ondanks de meer gevoelige informatie dat verstrekt moet worden. Verder is door middel van een vragenlijst onderzocht of de participanten bezorgd zijn over hun online-privacy. Maar liefst 95% heeft aangegeven geïnteresseerd te zijn in de bescherming van hun persoonlijke informatie. Dus ook hier is er sprake van een tegenstrijdigheid in de bezorgdheden over privacy en het werkelijke gedrag rondom privacy.

De relatie tussen de bezorgdheden over privacy en informatie onthullend gedrag is ook onderzocht in een *social media* setting door Tufekci (2008). Met behulp van een vragenlijstonderzoek onder studenten is geconstateerd dat er weinig tot geen relatie bestaat tussen online privacybelangen en het feitelijke gedrag rondom privacy. Een bijkomend conclusie van het onderzoek is dat de studenten hun zorgen over privacy niet reguleren door minder

persoonlijke data te openbaren, maar door de zichtbaarheid van hun informatie op *social media* aan te passen.

Met diepte-interviews hebben Lee et al. (2013) ondervonden dat er een tegenstrijdigheid bestaat tussen de bezorgdheden over privacy en het werkelijke gedrag. Door het verband te evalueren van de verwachte baten en verwachte risico's op het gedrag om informatie vrij te geven, is gebleken dat individuen ondanks hun zorgen over privacy actief persoonlijke gegevens delen. De verklaring die hiervoor is gegeven, is dat niet alleen rekening gehouden wordt met de bezorgdheden over privacy, maar ook met de verwachte voordelen van het verstrekken van informatie. Oomen en Leenes (2008) hebben een soortgelijke conclusie getrokken over het verband tussen de waargenomen risico's over privacy en het gebruik van technologieën die de privacy bevorderen. Alhoewel de individuen op de hoogte zijn van de mogelijke gevaren, blijken ze niet naar behoren te gedragen. Immers, een hoge waarneming van de risico's met betrekking tot privacy blijkt geen drijfveer te zijn voor het verschaffen van privacy bevorderende technologieën.

Volgens de studie van Tsai (2011) zijn consumenten geneigd een transactie te verrichten bij webwinkels die hun privacy beter beschermen, indien de privacyvoorwaarden expliciet worden weergegeven. Er zijn twee experimenten uitgevoerd. Het eerste experiment verwijst naar een online enquête over privacybezorgdheden. Het tweede experiment refereert naar een *online shopping* experiment, welke is uitgevoerd met een online zoekmachine die informatie weergeeft over de privacyvoorwaarden. Consumenten die voorzien zijn van gevoelige informatie aangaande privacy hebben rekening gehouden met die informatie door aankopen te doen van onlinewebwinkels die beschikken over relatief beter dan gemiddelde privacyvoorwaarden. In tegenstelling tot vele andere studies is geconcludeerd dat de consument wellicht bereid zou zijn om een premie voor privacy te betalen. Hieruit volgt de volgende stelling: de privacyvoorwaarden hebben een positief effect op het subjectieve vertrouwen.

Een groot aantal deskundigen bevestigen dus het bestaan van een tweedeling in de bedenkingen van mensen over online privacy en hun handelen ernaar. Echter zijn er ook studies die het tegendeel beweren. In het volgende onderdeel zal dit behandeld worden.

Studies tegen privacy paradox

Uit onderzoek van Miltgen & Peyrat-Guillard (2014) is te beweren dat er geen sprake is van een privacy paradox. Na het gedrag van jongeren op *social media* onderzocht te hebben is gebleken dat jongeren de bezorgdheden over privacy wegnemen door eigen methoden toe te passen, zoals het opgeven van valse namen en misleidende informatie. Ook worden privacyinstellingen zo aangepast om te voorkomen dat eenieder toegang heeft tot een profiel. Christofides et al. (2009) bevestigen deze stelling en voegen hier het weigeren van vriendschapsverzoeken en het verwijderen van foto's en labels aan toe. Er bestaan dus meerdere aanpakken om de bezorgdheden omtrent privacy van individuen te ontnemen. De privacy paradox wordt dus gedeeltelijk ontkracht op het moment dat deze aanpak als geldig wordt verklaard. Jongeren die aangeven bezorgd te zijn over hun privacy blijken zich immers wel naar behoren te gedragen door hun eigen maatregelen te hanteren en informatie op *social media* te vervalsen.

Lutz & Strathoff (2014) hebben een telefonisch onderzoek uitgevoerd bestaande uit enquêtevragen die betrekking heeft op de privacyvoorkeuren. Statistisch gezien is bevestigt dat er een zwak maar significant verband bestaat tussen de bezorgdheden over privacy en het werkelijke gedrag. Personen die beweren bezorgd te zijn over hun privacy hebben dus wel rekening gehouden met de vrijgave van persoonlijke informatie. Hargittai & Marwick (2016) constateren ook uit diepgaande interviews dat jongvolwassenen geven om hun privacy en in ieder geval een aantal privacybeschermende gedragingen vertonen op *social media*. Het slechts delen van foto's onder bekenden is daar een voorbeeld van. Echter, vinden de ondervraagden dat het onomkeerbaar is om persoonsgegevens van internet te halen indien het eenmaal is vrijgegeven. Ze voelen zich vrij machteloos hierover. Het gevoel geen controle te hebben over persoonlijke gegevens op internet noemt Hoffmann et al. (2016) ook wel het "privacy cynisme". Zij sluiten zich erbij aan dat dit fenomeen werkelijk bestaat.

Verder is in een vragenlijstonderzoek van Boyles et al. (2012) geconstateerd dat bezorgdheden over privacy de neiging op het protectief handelen aanwakkert. De enquête heeft getoond dat 54% van smartphonegebruikers hebben besloten om een applicatie niet te downloaden op het moment dat ze hebben ontdekt hoeveel persoonlijke informatie vrijgegeven moet worden om het

te kunnen gebruiken. Daarnaast heeft 30% een geïnstalleerde applicatie verwijderd, omdat ze erachter zijn gekomen dat het persoonlijke informatie verzameld die ze niet willen delen. Verder heeft 19% van de ondervraagden de locatie tracerende functie uitgezet. Dus ook hier is er sprake van een correlatie tussen de bezorgdheden over privacy en de vrijgave van persoonlijke informatie.

Conclusie

Al met al, verschillende studies concluderen tegenstrijdig over de privacy paradox. Alhoewel er nog geen zeker antwoord gegeven kan worden op de vraag of het verband tussen de waargenomen bezorgdheden in privacy en het werkelijke gedrag positief of negatief is, kan wel beantwoord worden of er überhaupt een verband bestaat. Uit de studies blijkt dat er inderdaad per context verschillende verbanden bestaan tussen het waargenomen- en werkelijke vertrouwen in privacy. Vaak worden persoonsgegevens snel vrijgegeven in ruil voor een klein voordeel, zoals in het voorbeeld van het prijsverschil van €1,- in de DVD-shop of het vrijgeven van foto's op social media voor versterking van sociale banden. Hiermee is antwoord gegeven op deelvraag 1. Als laatst, de keuzes van individuen kunnen ook beïnvloed worden door *biases* en *heuristics*, zoals de *immediate gratification bias* vermeld door Acquisti (2004). In dit geval wordt hier verwezen naar de neiging om de huidige baten hoger te waarderen dan de toekomstige risico's van informatieverstrekking op internet.

In tabel 1 wordt een overzicht van de hoofdbevindingen van de studies weergegeven en samengevat. Zo kan gezien worden dat mensen in categorieën geplaatst kunnen worden wat betreft hun houding en bedenkingen over online privacy. In feite is er alleen sprake van een privacy paradox voor de categorie 'bezorgd' en 'nemen geen maatregelen'. Echter, zoals vooraf is vermeld valt te bediscussiëren of degenen die gebruik maken van valse informatie ook onder de privacy paradox vallen. Ter verduidelijking, de super-*cyber-sceptic* is iemand die ondanks alle maatregelen die genomen worden alsnog vreest voor datamisbruiken. De *no-awareness* personen hebben geen weet over het internet en de bijbehorende gevaren, waardoor ze zich ook geen zorgen maken.

Tabel 1: Overzicht van de kenmerken van mensen wat betreft de privacy paradox

Privacy paradox	Bezorgd	Onbezorgd
Nemen maatregelen	1. *Super-cyber-sceptic* 2. Gebruik van schuilnamen, zichtbaarheid aanpassen etc.	1. Onbezorgd omdat ze maatregelen nemen (neemt genoeg maatregelen voor veilig internet en vindt het onnodig om bezorgd te zijn 2. Nemen maatregelen maar zijn onbezorgd (beter voorkomen dan genezen).
Nemen geen maatregelen	1. De baten van informatie-verstrekking wegen hoger dan de kosten 2. Denken dat het onomkeerbaar is om sporen te wissen op internet 3. Weten niet hoe het proces van dataverzameling werkt en waarvoor het gebruikt wordt	1. *No-awareness* 2. Zijn bewust van de gevaren en nemen het risico. 3. Vinden het onrealistisch om zich voor ieder mogelijke inbreuk te beschermen.

3. Methodologie

3.1 Onderzoeksopzet

Voor het beantwoorden van de subvragen zullen de verwachtingen en waargenomen gevaren omtrent de online privacy- en veiligheidsprotocollen uitvoerig bestudeerd worden. Onder de doelgroep behoren 12 tot 65-jarigen die, vrijwillig of mede door de technologische ontwikkelingen in de samenleving gebruik maken van het internet, ongeacht of ze zich veilig of onveilig voelen op het internet. De benoemde leeftijdsgroep is geselecteerd, gezien zij het meest actief zijn op het internet (CBS, 2019) en daarom het meest kwetsbaar zijn voor het in contact komen met virussen en datalekken, waardoor het gevoel van vertrouwen in privacy aangetast kan worden. Ook degenen die internet als gevaar beschouwen en er geen gebruik van maken behoren tot de doelgroep. Het is van belang om deze deelgroep te analyseren om te achterhalen wat voor hen de aanleiding is geweest om zich van het internet te distantiëren, aangezien de waarschijnlijkheid bestaat dat het betrekking heeft op het lage subjectief waargenomen vertrouwen in privacy.

3.2 Kwalitatief onderzoek

In dit deel van het onderzoek zijn interviews bestaande uit 11 personen afgenomen, die als voorproef dienen voor het kwantitatief onderzoek. Hun visie over de verwachtingen en gevaren op internet betreft online privacy en -veiligheid is belangrijk voor het opstellen van een representatieve enquête. Individuen zullen afzonderlijk geïnterviewd worden om diepere inzichten te verkrijgen over de verwachtingen van internetgebruikers ten aanzien van online privacy en -bescherming. Het is de bedoeling om het huidige niveau van vertrouwen te meten en mogelijke oplossingen te inventariseren.

3.3 Kwantitatief onderzoek

Van de diepgaande opvattingen van ondervraagden uit de focusgroep zijn geprobeerd relevante en adequate vragen op te stellen. Het hoofddoel van de enquête is om te kunnen toetsen welke onafhankelijke variabelen in welke mate van invloed zijn op het subjectieve vertrouwen in privacy van de deelnemers. Het eerste deel van de enquête bevat persoonsgegevens om te controleren of de steekproef representatief is met de werkelijke populatie. Het tweede deel onderzoekt de meningen over de bestaande (waargenomen) gevaren op internet. Deel drie bestaat uit een conjoint analyse van vijftien vragen met de *rating* als afhankelijke variabele. Iedere vraag is samengesteld uit vijf kenmerken met ieder drie levels gegeven aan de denkbeeldige app. De 15 vragen zijn automatisch zorgvuldig uitgekozen uit het totaal aantal combinaties van vragen met behulp van *fractional factorial design* in het programma R. Hiermee worden verlangens naar kenmerken voor een veilige app bestudeerd. Met Stata is uiteindelijk de regressie uitgevoerd om de effecten van de coëfficiënten op de rating te achterhalen.

3.4 Data benadering

Voor het onderzoek is een enquête opgesteld van 28 vragen, waarvan 15 beoordelingsvragen voor de conjoint analyse. De resterende vragen zijn vooral gericht op persoonsgegevens, zoals leeftijd, geslacht en meningen van de deelnemers over online privacy en -veiligheid. Het doel van het analyseren van de persoonsgegevens is om te controleren voor het bestaan van *selection bias*. Dit is nodig om de representativiteit van het onderzoek te verifiëren. De enquête is online geconstrueerd en gedistribueerd. Na het verwijderen van de grotendeels onvolledige enquêtes zijn hieruit 202 deelnemers verworven. De reden dat de enquête slechts via online platforms gedeeld is, heeft met de maatregelen van het Covid-19 virus te maken. Om zoveel mogelijk deelnemers te werven zijn deelnemers verzocht om de link binnen hun omgeving te delen. De link is onder andere gedeeld via groepspagina's met tientallen onbekenden in Facebook, Whatsapp, Instagram, LinkedIn en Canvas.

Voor de focusgroep zijn bewust mensen van verschillende leeftijden, geslachten en achtergronden (telefonisch) geïnterviewd om de populatie zo nauwkeurig mogelijk te kunnen representeren. De

enquête zal niet langdradig moeten worden om vermoeidheidsgevolgen (stimuli) te voorkomen. Dus om de uitslagen onaangetast te houden en betrouwbaarheid en validiteit van het onderzoek te waarborgen, zijn de vragen ingeperkt tot 28 vragen. Door het willekeurig verspreiden van de enquête onder meerdere deelgroepen is geprobeerd *selection bias* te minimaliseren.

4. Resultaten

4.1 Kwalitatief onderzoek

De tweede deelvraag heeft betrekking op het bewustzijn van internetgebruikers over de risico's op online platforms en hun handelingen ernaar. Dit zal uiteengezet worden in het kwalitatief onderzoek. De hoofdconclusie die is getrokken binnen een focusgroep gericht op elf personen is dat er vraag bestaat naar een 100% veilige applicatie. Niet iedere kandidaat is ervan overtuigd dat het uitvinden van een dergelijke applicatie realiseerbaar of haalbaar is, maar ook zij vinden dat er behoefte is naar een 100% veilige app. Het overgrote deel dat gelooft dat het mogelijk is om een dergelijke app uit te vinden, kan onderverdeeld worden in twee groepen: zij die bereid zijn er geld voor neer te zetten en zij die niet bereid zijn te betalen. Degenen die er niet voor willen betalen zijn voornamelijk personen die beweren niets te verbergen te hebben en personen die zich niet verzetten tegen het verzamelen en verspreiden van hun data door derde partijen. Ze vinden het daarom onnodig om extra voorzichtig te zijn met de sites die ze bezoeken, *posts* die ze plaatsen en *likes* die ze geven. Toch vinden ze dat er behoefte is aan een dergelijke app om extreme gevallen van misbruik, zoals virussen en lekkage van betaalgegevens te voorkomen. Tevens zijn er personen die de applicatie zouden willen gebruiken, maar alleen indien het kosteloos is. Degenen die wel bereid zijn te betalen voor de app zijn bereid maximaal €150 per jaar te betalen.

Dan zijn er enkelingen die wel bereid zijn te betalen, maar niet geloven dat het haalbaar is om een 100% veilige app tot stand te brengen. Het lijkt ze eenmaal te moeilijk of zelfs onmogelijk om een systeem te creëren dat onkraakbaar is, oftewel een systeem dat technisch onrealiseerbaar is. Als laatst zijn er degenen die niet geloven dat het mogelijk is een 100% veilige app te maken en er absoluut niet voor willen betalen. Dit zijn vooral degenen die wantrouwig en pessimistisch kijken naar iedere soort instantie en gezag. Degenen die het programma of de app uitbrengen zouden ze wantrouwen voor het behoeden van hun data. Een typische opmerking is: waarom zou ik hen wel moeten vertrouwen? Deze gegevens zijn samengevat in tabel 2. Dus ongeacht of de 100% veilige app uitgevonden wordt of niet, er zal nooit geslaagd worden in het winnen van het subjectieve vertrouwen door iedere individu, gezien er altijd enkelen sceptisch zullen staan tegenover dit concept.

Tabel 2: Matrix over de 100% veilige app waarin de opvattingen worden samengevat van mensen die er wel/niet in geloven en wel/niet voor bereid zijn te betalen.

100% veilige app	Gelooft in realiseerbaarheid	Gelooft niet in realiseerbaarheid
Wil betalen	Gelooft dat het kan en zou ervoor willen betalen. Max. 150 euro per jaar.	Wilt wel betalen, maar vindt het onrealistisch om iets wat niet kraakbaar is te creëren. Max. 150 euro per jaar.
Wil niet betalen	1.Wilt de app wel aanschaffen en gelooft dat het kan, maar wilt er niet voor betalen 2.Gelooft dat het kan, maar wilt niet aanschaffen/ betalen, omdat beweert wordt niks te verbergen te hebben	Gelooft niet dat het kan en wilt er absoluut niet voor betalen, omdat ze de instanties die die app zouden creëren ook zullen wantrouwen. (Waarom hen wel moeten vertrouwen?)

Een ander resultaat is dat de meerderheid geen tot weinig weet blijkt te hebben over hoe bedrijven omgaan met hun data en waarvoor data gebruikt wordt. Er is gevraagd in hoeverre ze bekend zijn met de termen HTTP(S), SSL, Encryptie, Cookies, VPN en Firewall om het bewustzijn over beveiligd internet te analyseren. Slechts drie van de elf personen hebben een globaal idee over de inhoud. De ondervraagden weten niet wat er met hun gegevens gebeurt of welke virussen er bestaan, maar geven wel om het feit dat hun computer virusvrij en lekkagevrij is. Sommigen hebben VPN aangeschaft, anderen hebben add-blockers en antivirussen gedownload, maar hebben er verder niet veel verstand van. Slechts drie ondervraagden hebben zich werkelijk verdiept en kennen de gevaren. Dit wijst erop dat het overgrote deel van de ondervraagden onbekend zijn met het proces van datawerving en -verspreiding en de consequenties van onveilig internetgebruik. Het antwoord op de tweede deelvraag is hiermee gegeven. Alhoewel de ondervraagden weinig afweten van veilig internet is er geen reden om het onderzoek irrelevant te achten, aangezien deze studie betrekking heeft op de kenmerken die subjectieve vertrouwen scheppen. Tijdens het vragen naar de kenmerken waar een 100% veilige app aan zou moeten voldoen, zijn de componenten aangegeven die volgens hen vertrouwen creëren en deze zijn dus niet gebaseerd op de kenmerken die werkelijk vertrouwen vormen. Het is van belang hoe de ondervraagden veilig internet definiëren, waardoor het niet van toegevoegde waarde is om de echte gevaren te

herkennen. Toch zijn ze ondervraagd naar hun bewustzijn over de echte gevaren om specifieke kenmerken voor de conjoint analyse in het kwantitatief onderzoek te kunnen gebruiken.

De ondervraagden hebben de mogelijkheid gekregen om aan te geven welke specifieke kenmerken ze verwachten van een 100% veilige app. Niet iedere ondervraagde heeft dezelfde verwachtingen, maar bepaalde kenmerken zijn relatief gezien vaker naar voren gekomen. Deze kenmerken zijn onder andere het niet te traceren zijn door bedrijven (en overheden), geen virussen, lekkage van foto's en/of berichten en gehackte betaalgegevens. Minder vaak naar voren gekomen zijn geen verplichte cookiesacceptatie en geen aanbevolen advertenties op basis van voorkeuren voor producten en diensten.

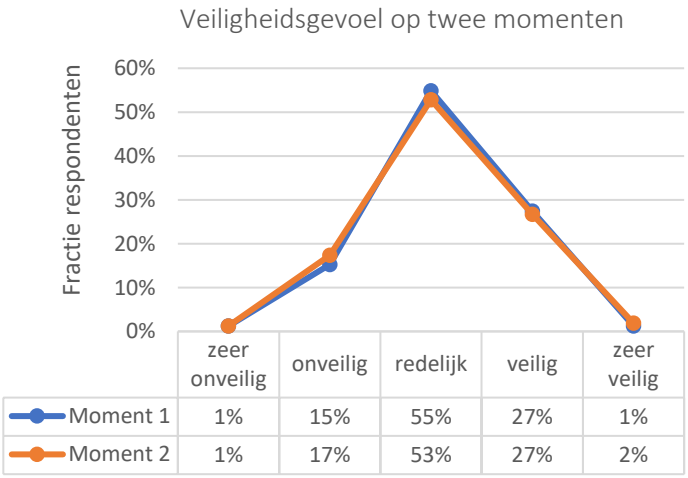
De ondervraagden zijn gevraagd of ze weleens privacyvoorwaarden doorlezen en of ze zich prettig voelen als deze voorwaarden duidelijk worden weergegeven. Geen van de respondenten lezen dit intensief door of voelen zich er goed bij. De stelling dat de privacyvoorwaarden een positief effect hebben op het subjectieve vertrouwen wordt dus verworpen. Verder hebben velen aangegeven cookies 'irritant' te vinden. Er is vermeld dat het fijner zou zijn als er helemaal niet gevraagd zou worden naar hun toestemming en toch persoonsgegevens verzameld zou worden dan het verplicht moeten accepteren van cookies om door te kunnen gaan op de website. Dit betekent niet dat ze niet geven om hun privacy maar dat het bewust weg moeten geven van data harder aankomt dan het onbewust weggeven. De reden hiervoor is dat het bijna onmogelijk is om sociaal betrokken te functioneren zonder ergens cookies geaccepteerd te hebben. Het subjectieve vertrouwen wordt hierdoor negatief beïnvloed. De baten van cookiesacceptatie wegen dus zwaarder dan de kosten. Enkelen hebben gesteld sites met verplichte cookiesacceptatie direct te verlaten. Anderen accepteren de cookies en gaan door maar blijven het ergerend vinden. Instelbare cookies worden geprefereerd boven verplichte cookies. Bij instelbare cookies heeft iemand aangegeven ze altijd te minimaliseren. Anderen doen dit niet te alle tijden, maar het geeft ze wel het idee een website te bezoeken dat hun privacy meer respecteert.

Aangezien de deelnemers niet volledig bewust zijn van de specifieke gevaren zijn er algemene attributen opgesteld om de conjoint analyse in het vervolg begrijpelijk te maken voor alle betrokkenen.

4.2 Kwantitatief onderzoek

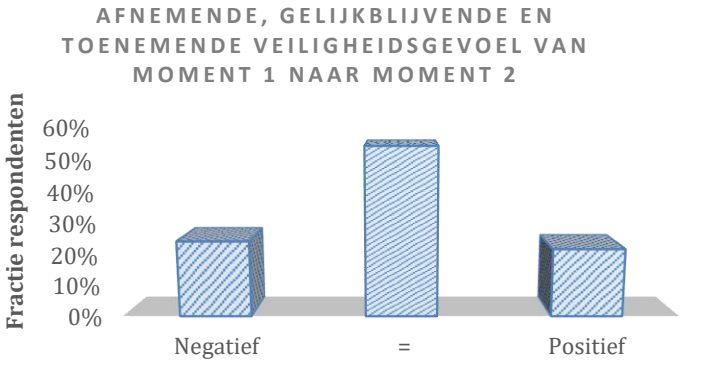
Voor- en nameting: mate van veiligheidsgevoel

Om te kunnen controleren of de enquête de mening van de deelnemer heeft beïnvloed, is de vraag of de deelnemer zich veilig voelt op internet tweemaal gesteld in de enquête (zie tabel 5 Appendix). De mogelijkheid bestaat dat deelnemers zich vooraf veilig voelden, maar na het beantwoorden van de vragen over privacy en veiligheid bewuster zijn geworden van de situaties die zich voor kunnen doen rondom privacyinbreuk. Met als gevolg dat ze zich meer of minder veilig kunnen voelen op het internet. Het is uit het onderzoek gebleken dat 46% van de deelnemers hun veiligheidsgevoel anders hebben beoordeeld na het invullen van de enquête. Indien er alleen wordt gekeken naar figuur 3**Fout! Verwijzingsbron niet gevonden.**, zou er geconcludeerd kunnen worden dat de survey geen effect heeft gehad op de kijk naar waargenomen vertrouwen en risico's op internet van de deelnemers. Echter, als we kijken naar figuur 4, zien we dat dit patroon is te verklaren door een ongeveer gelijke hoeveelheid stroom aan respondenten die zich meer en minder veilig voelen op de twee momenten. De enquête heeft dus voor ongeveer een kwart van de deelnemers een negatief effect gehad, waarmee wordt bedoeld dat ze een relatief minder veilig gevoel hebben ervaren op moment 2 dan op moment 1. Voor de andere kwart is er een positief effect, wat indiceert op een relatief veiliger gevoel op moment 2 dan op moment 1, en voor de helft is er geen effect opgetreden.



	zeer onveilig	onveilig	redelijk	veilig	zeer veilig
Moment 1	1%	15%	55%	27%	1%
Moment 2	1%	17%	53%	27%	2%

Figuur 3: Veiligheidsgevoel op twee momenten.



Negatief	=	Positief
24%	54%	22%

Figuur 4: Het verschil in het veiligheidsgevoel van moment 1 naar moment 2.

Type persoonlijke data

Uit de appendix (figuur 10 en 11) is af te leiden welk type informatie gedacht wordt het meest gevoelig te zijn voor datalekken en wat voor type informatie de respondenten het belangrijkst achten. De deelnemers hebben bij het beantwoorden van de bijbehorende vragen de vrijheid gekregen om meerdere opties te selecteren. Zo toont figuur 10 aan dat deelnemers denken dat locatie/IP-adres, inloggegevens en betaalgegevens het vaakst gehackt worden met respectievelijk 21.6%, 17.8% en 15.3%. Figuur 11 daarentegen, geeft aan welk type informatie het belangrijkst gevonden wordt door de deelnemers. De drie die het meest naar voren gekomen zijn omvatten betaalgegevens, camerabeelden/foto's en inloggegevens met respectievelijk 23.4%, 21.0% en 20.1%. Whatsapp-berichten/ SMS/ Mail is ook een belangrijk type data dat door 17.5% van de deelnemers is geselecteerd.

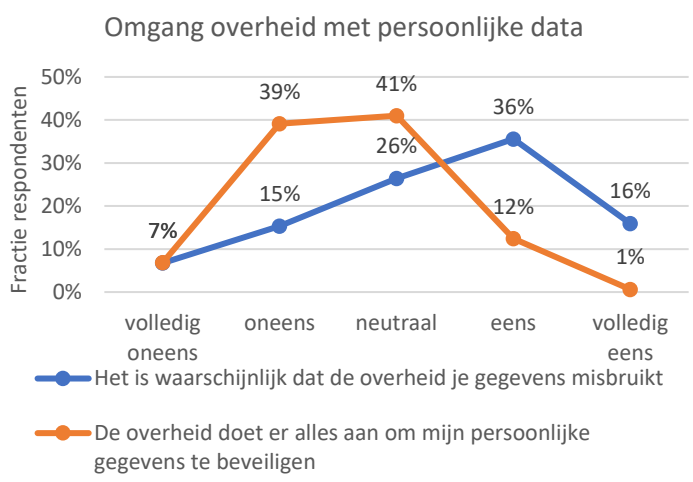
Figuur 12 toont ook aan dat veiligheid belangrijk wordt gevonden, doordat 47% (36% +11%) aangeeft (zeer) veel schade op te lopen als hun data gestolen wordt. Dit indiceert dat het subjectieve vertrouwen aangetast zal worden, indien persoonlijke data gestolen of misbruikt wordt. Verder schat 27% (23%+4%) de waarschijnlijkheid groot dat er een aanmerking zal plaatsvinden met een computervirus.

Omgang met data door verschillende entiteiten

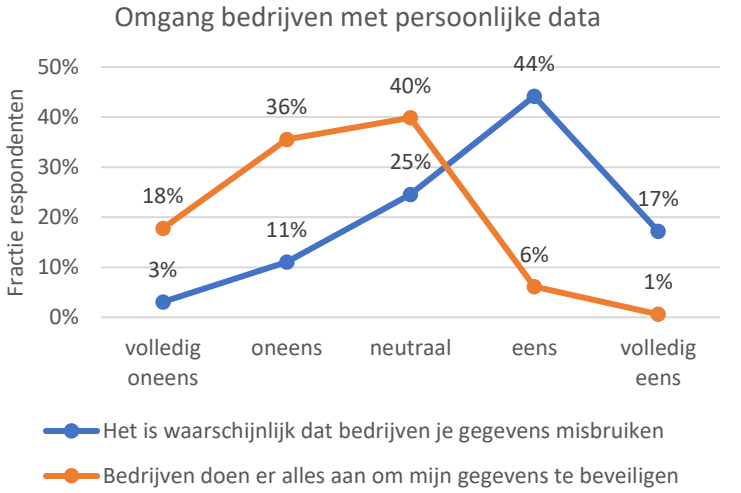
Met de vragen negen en elf uit de enquête zijn de volgende gegevens opgesteld. Alhoewel 52% (36%+16%) van de respondenten denkt dat het waarschijnlijk is dat de overheid hun gegevens misbruikt, is 46% (7%+39%) van mening dat de overheid er niet alles aan doet om hun gegevens te beschermen. Het verschil is mogelijk te verklaren door het feit dat bepaalde individuen de overheid over het algemeen in geen enkel geval beschouwen als een betrouwbare entiteit. Het bleek ook uit de resultaten van de focusgroep dat sommigen vinden dat de overheid er niet alles aan kan/wil doen om hun gegevens te beveiligen. Verder blijkt uit figuur 5 dat 22% (7%+15%) erop vertrouwt dat hun gegevens in goede handen zijn bij de overheid. Echter, blijkt dat maar 13% (12%+1%) van de deelnemers vinden dat de overheid genoeg moeite doet wat betreft het

beveiligen van hun persoonlijke gegevens. Het zou kunnen dat deze groep hun data aan de overheid toevertrouwt, maar dat er ook dan ruimte gezien wordt voor verbetering.

In het geval van de bedrijven blijkt 14% van de deelnemers te vertrouwen dat er geen misbruik gemaakt wordt van hun gegevens. Echter, slechts 7% vindt dat er voldoende maatregelen worden genomen (figuur 6). Wederom is het verschil van 7% te verklaren door het feit dat een deel respondenten tevreden zijn met de behandeling van hun gegevens door bedrijven, maar wel ruimte voor verbetering zien. Het blijkt dat de bedrijven meer gewantrouwd worden dan de overheid, maar liefst 61% (44%+17%) verdenkt bedrijven van datamisbruik. 54% (18%+36%) verwerpt het idee dat bedrijven al het mogelijke gedaan hebben om hun data te beveiligen. Ook hier is het verschil van 7% te verklaren, doordat een gedeelte van de deelnemers in geen geval de bedrijven vertrouwt en dus ook geen ruimte ziet voor verbetering.

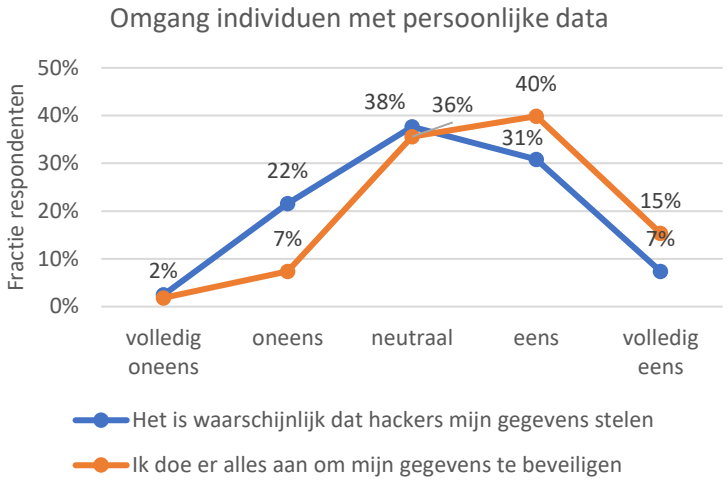


Figuur 5: Meningen over hoe de overheid omgaat met persoonlijke data.



Figuur 6: Meningen over hoe bedrijven omgaan met persoonlijke data.

Wat betreft individuen is 55% van mening dat ze hun taak volbrengen in de veiligstelling van hun persoonlijke data en 38% veronderstelt dat het waarschijnlijk is dat hackers hun gegevens zullen stelen (figuur 7). Dit wijst erop dat een deel van de deelnemers vreest om gehackt te worden en het gevoel heeft al het mogelijke gedaan te hebben. Indien individuen worden overtuigd van een nieuwe manier om hun data veilig te stellen, zal hoogstwaarschijnlijk het overgrote deel de nieuwe manier hanteren. Indien de 100% veilige premium app te verwerkelijken is, is er een mogelijk groot marktsegment beschikbaar voor bediening.



Figuur 3: Meningen over hoe de individuen/ hacker omgaan met persoonlijke data.

Maximale betalingsbereidheid

Voor het uitvoeren van de conjoint analyse is de vraag gesteld hoeveel euro per maand deelnemers maximaal bereid zijn te betalen voor een app (indien realiseerbaar) die 100% persoonlijke gegevensbescherming, virusvbescherming en advertentieblokkage garandeert. Deze vraag is bewust voor de conjoint analyse gesteld om de antwoorden van de respondenten niet te beïnvloeden. Indien de vraag na de conjoint analyse gesteld zou worden, zouden deelnemers een indruk kunnen krijgen over het prijsbereik en dit implementeren in hun keuze over de maximale betalingsbereidheid.

Figuur 13 (appendix) openbaart dat het hoogste bedrag dat deelnemers bereid zijn te betalen voor de app €100 per maand bedraagt. Het laagste bedrag is €0 per maand. Het gemiddelde bedrag dat deelnemers bereid zijn te betalen voor de 100% veilige applicatie is €12,29 per maand. Dit maandelijkse bedrag is vergelijkbaar met een gemiddelde VPN-abonnement dat meestal tussen €10 en €13 ligt. Ongeveer één op de vijf personen in Nederland maakt gebruik van VPN (Janssen, 2019). Een interessante vraag dat naar boven komt is waarom er zo weinig VPN's worden aangeschaft als blijkt dat er vraag is naar veiligere programma's. Dit is een aandachtspunt dat behandeld zal worden in de kwantificatie van de vraag naar de premium app.

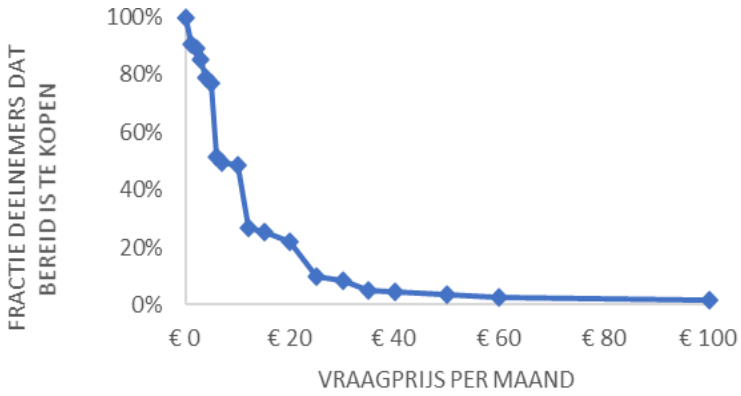
Dus deelvraag 3, waarin is gevraagd of mensen bereid zijn om te betalen voor het concept van een premium app is hiermee beantwoord. Het overgrote gedeelte van de deelnemers (90.5%) is inderdaad bereid om te betalen voor een 100% veilige app. Het percentage van 90.5% is af te leiden uit tabel 3 door het aftrekken van het percentage deelnemers dat €0 over heeft voor de app van 100%. Verder is uit de eerste twee kolommen van tabel 3 af te leiden welke bedragen opgegeven zijn als maximale betalingsbereidheid voor de premium app en wat de bijbehorende percentages van het geheel zijn. De drie meest benoemde bedragen zijn €5, €10 en €20 per maand, die respectievelijk 25,9%, 22,2% en 12,0% uitmaken van het geheel. De twee tussenliggende waarden die vallen onder het 95% betrouwbaarheidsinterval zijn €9.38 en €14.36.

4.2.1. Kwantificatie van de vraag naar de premium app

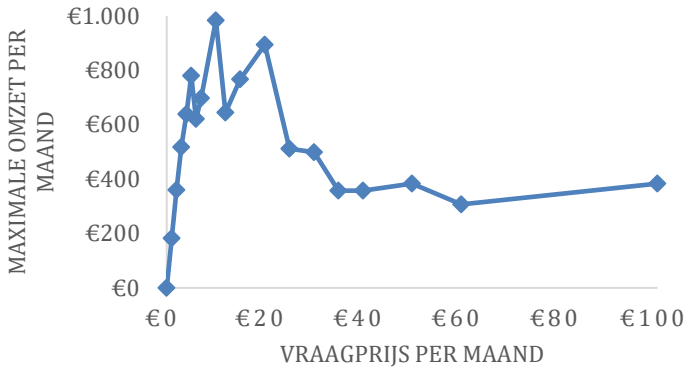
Voor het beantwoorden van deelvraag 3 zijn modellen ontworpen die de vraag naar en omzet van het concept van een abonnement op een premium app introduceren. De modellen zijn gedeeltelijk gebaseerd op de uitslagen van de enquête (zie eerste twee kolommen van tabel 3). De derde kolom omvat de fractie deelnemers die minstens de bijbehorende prijs bereid is af te staan. Figuur 8 toont de vraagcurve naar een premium app binnen de steekproef. De verticale as toont de fractie deelnemers, die bereid zijn om de premium app te bemachtigen tegen de vraagprijs. De vraagprijs is gegeven in euro per maand op de horizontale as.

De maximale omzet per maand is af te leiden uit de laatste kolom van tabel 3. De omzet is gegeneraliseerd naar het totaal aantal deelnemers van het onderzoek. Middels deze gegevens zijn de omzetcijfers te achterhalen bij de gegeven vraagprijzen. Door de maximale prijs te vermenigvuldigen met de 202 deelnemers en de fractie deelnemers dat bereid is de premium app aan te schaffen, worden de maximale omzetten per vraagprijs verworven. In dit geval is de omzet maximaliserende prijs €10 en de maximale omzet €984,43 (gemarkeerd in oranje). Figuur 9 drukt deze gegevens uit in een curve. Mogelijke kosten zijn niet meegenomen in de berekening.

Om perspectief te geven over de privacy paradox wordt teruggeblikt naar het aantal aanschaffers van een VPN abonnement. Eerder is aangegeven dat maar ongeveer 20% van de Nederlanders gebruik maakt van een VPN. Verder liggen de gemiddelde prijs voor een VPN en de winstmaximaliserende prijs voor de premium app grotendeels op één lijn. Dit is een interessant kernpunt, aangezien zowel een VPN als de premium app zouden moeten bijdragen aan veiliger internet, althans aan een hogere subjectieve vertrouwen in online veiligheid. Feitelijk heeft 90.5% van de deelnemers duidelijk gemaakt om te willen betalen voor de premium app. Echter, als de cijfers rondom het gebruik van een VPN vergeleken worden, kan in werkelijkheid een veel lager percentage verwacht worden. Ook dit verschijnsel is een aanwijzing voor de privacy paradox: een grote groep is bezorgd om hun veiligheid en er zijn eenvoudig te installeren en goedkope VPN's, maar slecht 20% maakt hier gebruik van.



Figuur 4: De vraagcurve naar een premium app binnen de steekproef.



Figuur 5: Maximale omzet per vraagprijs binnen de steekproef voor de premium app.

Tabel 3: De prijsclassificatie en bijbehorende omzet voor de maximale betalingsbereidheid van de participanten voor een premium app.

Maximale prijs	Percentage deelnemers	Fractie deelnemers bereid te kopen	Maximale omzet per maand
€ 0	9,5%	100%	€ 0,00
€ 1	1,3%	90,5%	€ 182,82
€ 2	3,8%	89,2%	€ 360,53
€ 3	6,3%	85,4%	€ 517,78
€ 4	1,9%	79,1%	€ 639,24
€ 5	25,9%	77,2%	€ 779,87
€ 6	1,9%	51,3%	€ 621,34
€ 7	0,6%	49,4%	€ 698,05
€ 10	22,2%	48,7%	€ 984,43
€ 12	1,3%	26,6%	€ 644,35
€ 15	3,2%	25,3%	€ 767,09
€ 20	12,0%	22,2%	€ 894,94
€ 25	1,9%	10,1%	€ 511,39
€ 30	3,2%	8,2%	€ 498,61
€ 35	0,6%	5,1%	€ 357,97
€ 40	0,6%	4,4%	€ 357,97
€ 50	1,3%	3,8%	€ 383,54
€ 60	0,6%	2,5%	€ 306,84
€ 100	1,9%	1,9%	€ 383,54
	100%	**0,0%**	

4.2.2. Conjoint Analyse

In dit gedeelte van het onderzoek worden de vragen 13 tot en met 27 uit de enquête (zie appendix) geanalyseerd en uitgewerkt. Om te achterhalen welke attributen het hoogst gewaardeerd worden is er een conjoint analyse uitgevoerd middels *fractional factorial design*. In totaal zijn er 15 vragen geconstrueerd, waarvan iedere vraag vijf kenmerken toekent aan een app. Het betreft de volgende vijf kenmerken: virusvrij, cookies-vermindering, overheidsdetectievrij, advertentie-vermindering en prijs. Aan ieder bovengenoemd attribuut werden drie attributenlevels toegekend, dit waren €0, €5 en €10 voor prijs (per maand) en 0%, 50% en 100% voor alle andere attributen. In totaal hebben 202 participanten deelgenomen aan het onderzoek, dat resulteert in een samenstelling van 3030 vragen (202*15). Echter zijn enkele vragen, bewust of onbewust, leeggelaten. Met in totaal 134 onbeantwoorde vragen is de analyse dus uitgevoerd met 2896 vragen.

Tabel 4 is een uiteenzetting van de uitkomsten van de conjoint analyse van onder andere de parameters, de bètanummers en de bijbehorende coëfficiënten. Naast deze gegevens zijn de *range* en *importance* van de coëfficiënten berekend en verwerkt. Om de conjoint analyse toe te kunnen passen is uitgegaan van een *base case*, oftewel een app dat 0% virusvrij en 0% overheidsdetectie-vrij 0% is en 0% cookies-vermindering en 0% advertentie-vermindering heeft voor een prijs van €0 per maand. De formule die is gebruikt om de rating te bepalen is als volgt:

$$\begin{aligned} Rating = {} & \beta 0 + \beta 1 * Virusvrij50 + \beta 2 * Virusvrij100 + \beta 3 * CookiesV50 + \beta 4 * CookiesV100 \\ & + \beta 5 * OverheidsdetectieV50 + \beta 6 * OverheidsdetectieV100 + \beta 7 \\ & * AdvertentieV50 + \beta 8 * AdvertentieV100 + \beta 9 * Prijs5 + \beta 10 * Prijs10 + \varepsilon \end{aligned}$$

De constante, ofwel $\beta 0$, van 42.62 uit tabel 4 is op te vatten als de gemiddelde waarde die gehecht wordt aan een app in de *base case*. De waarde van 42.62 is dus ook te interpreteren als de gemiddelde waarde die gegeven wordt aan het niet beschikken over een app. Alle coëfficiënten van de parameters vertonen een voorspelbaar negatief of positief effect. Zo werd verwacht dat alle parameters een positief effect zouden hebben op de rating, behoudens de parameter prijs. Logischerwijs wordt verwacht dat naarmate de prijs van de app stijgt, de waarde die wordt gegeven aan de app zal verminderen, wat de negatieve coëfficiënten bij de prijslevels verklaart.

Voor alle andere parameters is het toepasselijk dat de verkregen waarde zal stijgen indien de parameterlevels verhogen, omdat het ten gunste is van de koper. Hier zal zich dus een positief effect voordoen.

Voor- en nameting: conjoint analyse

Om diepere inzichten te verkrijgen over het subjectieve vertrouwen worden de ratings voor- en na de conjoint analyse vergeleken. Als de mate van veiligheid aan het begin van de enquête geanalyseerd wordt, kunnen de gegevens omgezet worden in een gemiddeld cijfer tussen de 0 en 100. Figuur 14 in de appendix zet de deelnemers uiteen in vijf groepen. Bij aanname dat "zeer onveilig=10", "onveilig=30", "redelijk=50", "veilig=70" en "zeer veilig=90" is, kan een gemiddelde score berekend worden voor het veiligheidsgevoel op het web. Dit kan door deze getallen te vermenigvuldigen met het aantal deelnemers die gekozen hebben voor een specifieke categorie en hier het gemiddelde van te nemen. Het resultaat is een gemiddelde score van 52.44.

Tabel 4: Resultaten van de conjoint analyse, range en importance.

Parameter	Bèta	Coëfficiënt	Range	Importance
Virusvrij: 50%	1	4.28*	21.83	28.7%
Virusvrij: 100%	2	21.83*		
Cookies-vermindering: 50%	3	9.19*	9.19	12.1%
Cookies-vermindering: 100%	4	7.89*		
Overheidsdetectievrij: 50%	5	2.85	12.90	17.0%
Overheidsdetectievrij: 100%	6	12.90*		
Advertentievermindering: 50%	7	1.09	7.06	9.30%
Advertentievermindering: 100%	8	7.06*		
Prijs: €5/maand	9	-17.08*	24.96	32.9%
Prijs: €10/maand	10	-24.96*		
Constante	0	42.62		
R-squared		0.3229		
(*) = significant				

Zonder enige situatieschetsing blijken deelnemers hun online veiligheidsgevoel dus te waarderen op 52.44. Vergeleken met de uitslag van de conjoint analyse, oftewel de constante van 42.62 is deze *rating* hoog gewaardeerd. De uitslagen indiceren dat deelnemers een hogere waardering geven wanneer ze geen context krijgen bij het vragen naar hun waardering voor hun veiligheidsgevoel op internet. En bij specifieke situatieschetsingen waarin privacy en veiligheid gekenmerkt worden met bepaalde attributen (de conjoint analyse), blijkt de waardering veel lager te zitten. Twee zaken kunnen hieruit geconcludeerd worden. Enerzijds dat de conjoint analyse leidt tot exactere inschattingen van de bestaande perceptie van het veilig surfen op internet, aangezien participanten verschillende gevallen met specifieke factoren naast elkaar zetten en waarderen. Anderzijds, dat er sprake is van de *confirmation bias* waarin informatie wordt gebruikt om vooroordelen te bevestigen en bij te dragen aan de huidige overtuigingen. Het is mogelijk dat bijvoorbeeld personen met een laag subjectief waargenomen vertrouwen beïnvloed zijn door de benoemde determinanten in specifieke context. In beide gevallen bewijst dit het bestaan van een subjectief waargenomen vertrouwen.

Bovendien is het plausibel dat bepaalde factoren onopgemerkt zijn en dus niet zijn meegenomen in de analyse. Deze factoren moeten ook in rekening worden gehouden gezien dit het resultaat kan beïnvloeden. De R-squared van 0.3229 geeft ook aan dat 32.29% van de variantie rondom het gemiddelde in de rating verklaard wordt door de ingevoerde attributen. Dit betekent dat er nog andere variabelen zijn die de rating beïnvloeden.

Om deelvraag 4 te beantwoorden wordt gekeken naar de attributen die invloed uitoefenen op de rating en naar de sterkte van de invloeden. Uit tabel 4 is af te leiden dat het prijsattribuut het grootste effect heeft op de rating. Het betreft een significant negatief effect van -24.96 en -17.08 voor een prijs van respectievelijk €10 per maand en €5 per maand. De significantie van de beschreven factoren gaat op bij een significantieniveau van 5%. De *importance* van het prijsattribuut is 32.9% dat bevestigt dat dit het meest doorslaggevende factor is voor de rating. Advertentie-vermindering is de factor die het minst geapprecieerd wordt, met een *importance* van 9.30%. Dit attribuut is niet significant bij een niveau van 50% advertentie-vermindering. Ook het attribuut ''overheidsdetectievrij" is niet significant bij een level van 50%. Deze levels zijn dus

nauwelijks van belang. Alle andere attributenlevels hebben wel een significant effect op *rating*. De meest belangrijke variabele na prijs is "virusvrij" met een *importance* van 28.7%. Ondanks dat de variabele "overheidsdetectievrij" alleen significant is voor een level van 100%, staat het als derde meest belangrijke variabele op de lijst met een *importance* van 17.0%. De deelnemers hebben hoogstwaarschijnlijk het gevoel dat het alleen effectief is indien overheden totaal geen beschikking hebben over persoonlijke informatie.

Al met al kan geconcludeerd worden dat een lage prijs en het virusvrij kunnen surfen op het web het meest gewaardeerd worden onder de deelnemers, alhoewel het niet verassend is dat de prijs een van de grootste rollen speelt in de keuzevorming. Surfen op het web zonder overheidsdetectie wordt ook erg gewaardeerd. Dit is alleen het geval indien het 100% beschermd is van overheden. Verder zijn behoudens de variabelen overheidsdetectievrij-50% en advertentievermindering-50%, alle variabelen(levels) significant bij een significantieniveau van 5%.

Slot

Uit het kwantitatief onderzoek blijkt dat het subjectieve vertrouwen in privacy al beïnvloed kan worden door slechts een ondervraging naar het subjectieve vertrouwen met behulp van een enquête. Dit is gebleken doordat ongeveer een kwart van de deelnemers een negatief gevoel en de andere kwart een positief gevoel heeft beleefd. Verder worden betaalgegevens, camerabeelden/foto's, inloggegevens en Whatsapp-berichten/ SMS/ Mail als belangrijkste type data beschouwd. De entiteiten die het minst vertrouwd worden zijn bedrijven, gevolgd door overheden en, natuurlijk, hackers.

Het online veiligheidsgevoel wordt hoger gewaardeerd zonder context met 52.44 vergeleken met de constante van de conjoint analyse van 42.62. Hieraan kunnen twee redenen ten grondslag liggen: of de conjoint analyse geeft exactere inschattingen weer door de bijbehorende specifieke context of er is sprake van een *confirmation bias*. De attributen die het meest gewaardeerd worden van de 100% veilige app zijn een lage prijs en virusvrije internet. Overheidsdetectievrije internet wordt ook erg gewaardeerd, maar alleen indien het 100% beveiligd is. Bovendien is de omzet maximaliserende prijs voor de 100% veilige app beschreven in dit onderzoek €10.

5. Conclusie & discussie

5.1 Conclusie

In het literatuuronderzoek is de privacy paradox uiteengezet, waarin de tegenstrijdigheid wordt becommentarieerd door verschillende onderzoekers. Privacy paradox wordt gedefinieerd als het volgende: hoewel beweerd wordt dat men zich grote zorgen maakt over hun privacy, wordt toch relatief weinig actie ondernemen om persoonlijke gegevens te beschermen.

Alhoewel er voor- als tegenargumenten zijn gegeven in het literatuuronderzoek voor het bestaan van de privacy paradox, bevestigen de gegevens uit het kwalitatief onderzoek het bestaan van de tegenstrijdigheid. Bij het ondervragen naar het gedrag rondom cookiesacceptatie is naar voren gekomen dat sommige deelnemers vrijwillig maar met tegenzin de cookies accepteren. De reden hiervoor is dat het onmogelijk wordt geacht om zowel nergens cookies te accepteren als om maatschappelijk betrokken te functioneren. Zoals bevestigd door de literatuur en het kwalitatief onderzoek, is de verklaring hiervoor dat de huidige baten opwegen tegen de toekomstige risico's. Een verschil tussen de literatuur en dit onderzoek is dat de verwachting van het bestaan van een positief effect van de privacyvoorwaarden op het subjectieve vertrouwen niet blijkt te bestaan. Hierdoor wordt de stelling verworpen. Ook dit is een bewijs voor het privacy paradox, aangezien wordt aangegeven dat privacy belangrijk wordt gevonden terwijl de privacyvoorwaarden niet doorgenomen worden.

Bovendien blijken de deelnemers van het kwalitatief onderzoek vrij onbekend te zijn met de gevaren en risico's op het internet. Slechts enkelen hebben een weet van de risico's van onveilig internet en hebben maatregelen genomen, zoals het aanschaffen van VPN en het downloaden van add-blockers en antivirussen. Toch vindt het merendeel het belangrijk om veilig te kunnen surfen op het net. Dit komt niet overeen met de uitslagen van het kwantitatief onderzoek, waarin slechts 9% beweert onvoldoende maatregelen te nemen tegen privacyinbreuk.

Het antwoord op de onderzoeksvraag welke determinanten tot het verhogen van het subjectieve vertrouwen in privacy leiden, is zowel uit het kwalitatieve als uit het kwantitatieve onderzoek af te leiden. Zoals eerder gezegd zorgen verplichte cookies voor een afname van het subjectieve vertrouwen, terwijl instelbare cookies een positiever effect op dit vertrouwen hebben. Instelbare

cookies worden geprefereerd, omdat het een idee geeft een website te bezoeken dat hun privacy meer respecteert. Wat ook is gebleken is dat het subjectieve vertrouwen zowel geschaad als versterkt kan worden door opgedane informatie uit een enquête. Verder zorgt het garanderen voor veiligstelling van betaalgegevens, camerabeelden/foto's, inloggegevens en Whatsapp-berichten/ SMS/ Mail tot versterking van het subjectieve vertrouwen, gezien deze type data het belangrijkst wordt gevonden. Wat betreft de 100% veilige app, zorgen een lage prijs, het virusvrij zijn en overheidsdetectievrij zijn voor de hoogste toename in het subjectieve vertrouwen. Cookiesvermindering en advertentievermindering hebben ook een positief effect op het subjectieve vertrouwen, doch in mindere mate. Wel moet bemerkt worden dat het overheidsdetectievrij en advertentie-vrij zijn alleen een positief significant effect hebben indien hier 100% van gegarandeerd kan worden. Ten slotte is er gebleken dat er behoefte is naar een 100% veilige app dat indiceert dat het subjectieve vertrouwen positief beïnvloedt zal worden door een dergelijke app.

5.2 Tekortkomingen & Aanbevelingen

Zoals verwacht zijn tijdens het invullen van de enquête vermoeidheidseffecten opgetreden. Enkele respondenten hebben doorgegeven voornamelijk de vragen gerelateerd aan de conjoint analyse als langdradig te beschouwen. Het negatieve effect van de lange vergelijkbare vragen op de betrouwbaarheid van het onderzoek kan verkleind worden door het inzetten van *incentives*. Er is enigszins al een prikkel ingezet, door bij de eerste vraag van de enquête aan te kondigen dat de uiteindelijke resultaten van het onderzoek gedeeld zullen worden met de deelnemers die hun e-mailadressen achterlaten. Degenen die hun e-mailadressen hebben ingevuld hebben ook vaker alle vragen beantwoord, wat bewijst dat de prikkel enigszins gewerkt heeft. In totaal heeft 35% van de ondervraagden een e-mailadres vermeld. Voor vervolgonderzoek kunnen er sterkere prikkels ingezet worden, zodat mensen de vragen volledig afronden en serieus invullen. Deze prikkels kunnen het geven van een geldbedrag zijn voor hen die de enquête volledig afronden.

Verder is het kwantitatief onderzoek vooral ingevuld door 21 tot 27-jarigen (59% van de deelnemers) en door vrouwen (74% van de deelnemers). Dit wijst op een laag niveau van

representativiteit van het onderzoek. Voor een vervolgonderzoek wordt geadviseerd om een gelijker aantal aan mannen en vrouwen en verschillende leeftijdscategorieën te ondervragen. De reden hiervoor is dat er een verschil kan bestaan in het risicoprofiel tussen mannen en vrouwen of tussen verschillende leeftijdscategorieën. Gezien de situatie rondom de coronacrisis, is het vooral lastig geweest om aan respondenten te komen. Het is gevaarlijk en bijna onmogelijk om mensen buiten te benaderen voor het invullen van de enquête. Daarom is de enquête online verspreid en ingevuld. Voor vervolgonderzoek wordt aangeraden om mensen ook buiten te benaderen om een meer representatieve en willekeurige steekproef te testen. Zo zullen ook zij die niet gebruik maken van internet ondervraagd kunnen worden, waardoor de reden waarom ze geen gebruik maken van internet achterhaalt kan worden. Voor een vervolgonderzoek wordt dus aangeraden om te onderzoeken in een tijd zonder calamiteiten of om het onderzoek te adapteren.

Nu het duidelijk is wat voor informatie als het meest cruciaal wordt beschouwd, is het relevant om mensen het meest te verzekeren van die factoren. Bedrijven kunnen bijvoorbeeld meer focussen op het garanderen van beveiligde gegevens voor hun klanten die hun websites bezoeken. Bovendien kunnen bedrijven hun online-bezoekers bewijzen dat ze niet de type data hacken/lekken dat het meest cruciaal gevonden wordt. Op deze manier zal het vertrouwen van de bezoekers gewonnen worden, dat zal leiden tot meer verkeer op de site. Voor een goed functionerende bedrijfsplan is het dus fundamenteel om online-bezoekers een goed gevoel op te leveren en te garanderen tegen virussen en datalekkages.

Reflectie

Het grootste meeneempunt van het onderzoek is voor mij het persoonlijk ondervragen van de geïnterviewden en het onderzoeken van de privacy paradox geweest. Het was heel interessant om diepe gesprekken aan te gaan over het veiligheidsgevoel op internet. Het model over de matrix is vrij lastig geweest om op te stellen, omdat het allemaal losse puzzelstukjes zijn geweest waar ik een geheel van heb moeten maken. Nadat dat gelukt was, is het model overzichtelijk geworden. De privacy paradox is op zichzelf al een zeer interessant onderwerp geweest om te onderzoeken. Het naast elkaar zetten en doorlezen van verschillende studies en verschillende meningen heeft veel bijgedragen aan mijn kennis over het menselijk gedrag rondom privacy.

6. Bibliografie

- Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce - EC '04*, 1. https://doi.org/10.1145/988772.988777
- Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33. https://doi.org/10.1109/msp.2005.22
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465
- Athey, S., Catalini, C., & Tucker, C. E. (2017). The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. *SSRN Electronic Journal*, 1. https://doi.org/10.2139/ssrn.2916489
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013
- Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters*, *117*(1), 25–27. https://doi.org/10.1016/j.econlet.2012.04.077
- Boudet, J. (2020, 13 maart). *Consumer-data privacy and personalization at scale: How leading retailers and consumer brands can strategize for both*. Geraadpleegd van https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/consumer-data-privacy-and-personalization-at-scale
- Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. *Pew Research Center*, 1. Geraadpleegd van https://www.pewresearch.org/internet/Reports/2012/Mobile-Privacy.aspx
- Brown, B. (2001). Studying the internet experience. *HP Laboratories Technical Report*, 49. Geraadpleegd van http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf
- Centraal Bureau voor de Statistiek. (2018, 3 februari). *Nederland koploper in Europa met internettoegang*. Geraadpleegd van https://www.cbs.nl/nl-nl/nieuws/2018/05/nederland-koploper-in-europa-met-internettoegang

- Centraal Bureau voor de Statistiek. (2019, 4 januari). *Zes procent nooit op internet*. Geraadpleegd van https://www.cbs.nl/nl-nl/nieuws/2019/01/zes-procent-nooit-op-internet
- Centraal Bureau voor de Statistiek. (2020, 24 april). *Nederlanders besteedden 1,9 miljard euro bij Europese webwinkels in 2019*. Geraadpleegd van https://www.cbs.nl/nl-nl/nieuws/2020/17/nederlanders-besteedden-1-9-miljard-euro-bij-europese-webwinkels-in-2019
- Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, *12*(3), 341–345. https://doi.org/10.1089/cpb.2008.0226
- Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, *22*(3), 167–176. https://doi.org/10.1016/j.iedeen.2016.04.002
- Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033
- Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication 10*, 3737–3757. Geraadpleegd van http://ijoc.org.
- Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), 1. https://doi.org/10.5817/cp2016-4-7
- Holvast, J. (1993). Vulnerability and privacy: are we on the way to a risk-free society? *In: Proceedings of the IFIP-WG9.2 conference*, Namur, Belgium.
- Janssen, D. (2019, 7 oktober). *VPN trends: waarom steeds meer Nederlanders een VPN gebruiken*. Geraadpleegd van https://www.vpngids.nl/nieuws/vpn-gebruik-nederlanders-2019/

- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002
- Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, *71*(9), 862–877. https://doi.org/10.1016/j.ijhcs.2013.01.005
- Louw, N. (2020, 4 mei). *Zoom & privacy: zo kun je veilig videobellen [how to]*. Geraadpleegd van https://www.frankwatching.com/archive/2020/04/03/zoom-privacy-veilig-videobellen/
- Lutz, C., & Strathoff, P. (2014). Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. *Working Paper*, 1. https://doi.org/10.2139/ssrn.2425132
- Mandic, M. (2009). Privacy and security in e-commerce. *CROMAR i Ekonomski fakultet Zagreb*, 1. Geraadpleegd van https://www.ceeol.com/search/article-detail?id=80002
- Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125. https://doi.org/10.1057/ejis.2013.17
- Norberg, A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x
- Oomen, I., & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. *The International Federation for Information Processing, vol 261*, 121–138. https://doi.org/10.1007/978-0-387-77996-6_10
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 1. https://doi.org/10.1080/10864415.2003.11044275
- RTLNieuws Contributors. (2020, 21 april). *Honderden scholen verbieden videobellen met Zoom*. Geraadpleegd van https://www.rtlnieuws.nl/tech/artikel/5097806/honderden-nederlandse-scholen-verbieden-videobeldienst-zoom

- Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. *EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce*, 38–47. https://doi.org/10.1145/501158.501163
- Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260
- Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 20–36. https://doi.org/10.1177/0270467607311484

7. Appendix

7.1 Enquête vragen

Tabel 5: Enquête vragen van het kwantitatief onderzoek.

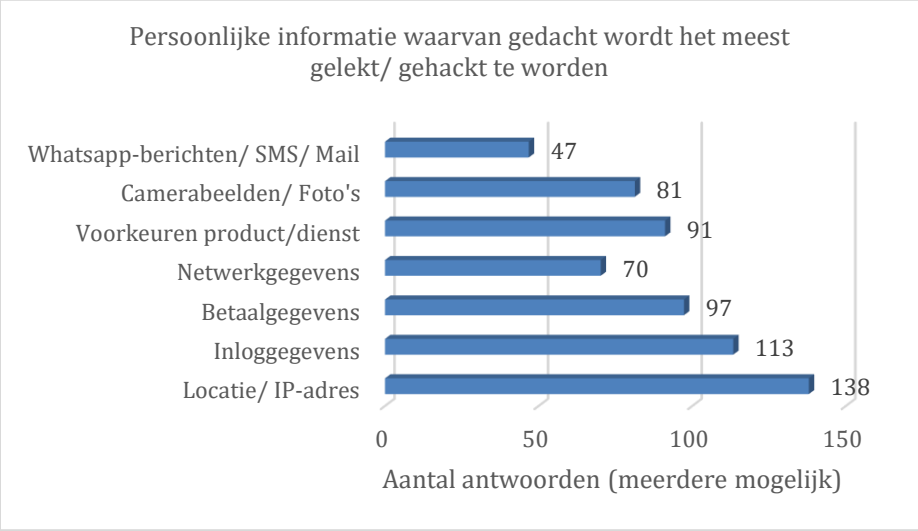
#	Vraag	Soort Vraag	Omschrijving/Mogelijke antwoorden
	Persoonsgegevens		**Persoonsgegevens**
1	Bedankt voor je deelname aan dit onderzoek. Voeg je e-mailadres toe als je de resultaten van het onderzoek wilt ontvangen, nadat het onderzoek is verricht. De gegevens zijn volledig anoniem.	Open vraag	Naam123@hotmail.com
2	Selecteer je geslacht?	Multiple Choice	Man/ Vrouw
3	Selecteer je leeftijd	Open (Integer) Vraag	<20/21-27/28-35/36-44/>45
4	Hoeveel uur zit je gemiddeld per dag op het web?	Open vraag	0-24 uur/dag
	Privacy & Security Data		**Privacy & Security Data**
5	Hoe veilig voel je je op het internet?	Multiple Choice	Zeer onveilig/ onveilig/ redelijk/ veilig/ zeer veilig
6	Hoe waarschijnlijk is het dat je in aanmerking komt met een computervirus?	Multiple Choice	Zeer onwaarschijnlijk/ onwaarschijnlijk/ redelijk/ waarschijnlijk/ zeer waarschijnlijk
7	Welke persoonlijke informatie wordt denk je het vaakst gelekt/gehackt? (Meerdere keuzes mogelijk)	Multiple Choice (Multiple Answer)	Locatie/IP-adres, Inloggegevens, Betaalgegevens, Netwerkgegevens, Voorkeuren product/ dienst, Camerabeelden/ Foto's, Whatsapp-berichten/ SMS/ Mail, Anders, namelijk…

8	Welke persoonlijke informatie is voor jou het meest van belang?	Multiple Choice (Multiple Answer)	Locatie/IP-adres, Inloggegevens, Betaalgegevens, Netwerkgegevens, Voorkeuren product/ dienst, Camerabeelden/ Foto's, Whatsapp-berichten/ SMS/ Mail, Anders, namelijk…
9	Hoe waarschijnlijk is het dat… 1. … hackers je persoonlijke gegevens stelen? 2. … bedrijven je persoonlijke gegevens misbruiken? 3. … de overheid je gegevens misbruikt?	Matrix Tabel	Zeer onwaarschijnlijk/ onwaarschijnlijk/ neutraal/ waarschijnlijk/ zeer waarschijnlijk
10	Hoeveel schade zou je oplopen als je gegevens gestolen worden door hackers/ bedrijven/ overheden?	Multiple Choice	Zeer weinig/ weinig/ matig/ veel/ zeer veel
11	(Lees eerst het onderste) … er alles aan om mijn persoonlijke gegevens te beveiligen. 1. De overheid doet… 2. Bedrijven doen… 3. Ik doe…	Matrix Tabel	Volledig oneens/ oneens/ neutraal/ eens/ volledig eens
12	Indien realiseerbaar, hoeveel €/maand ben je maximaal bereid te betalen voor een app dat je 100% garandeert van persoonlijke gegevensbescherming, virusbescherming en advertentieblokkage?	Open Vraag	Bedragen tussen de 0 en 100 euro
	Conjoint analyse		**Conjoint analyse**
	Algemene vraag voor het volgende deel: Op een schaal van 0 tot 100, hoe tevreden ben je met de kenmerken van de app?		
13	**Virusvrij**: 100% **Cookies-vermindering**: 50% **Overheidsdetectie-vrij**: 100% **Advertentie-vermindering**: 0% **Prijs**: €5 per maand	Likertschaal	Integer schaal van 0-100

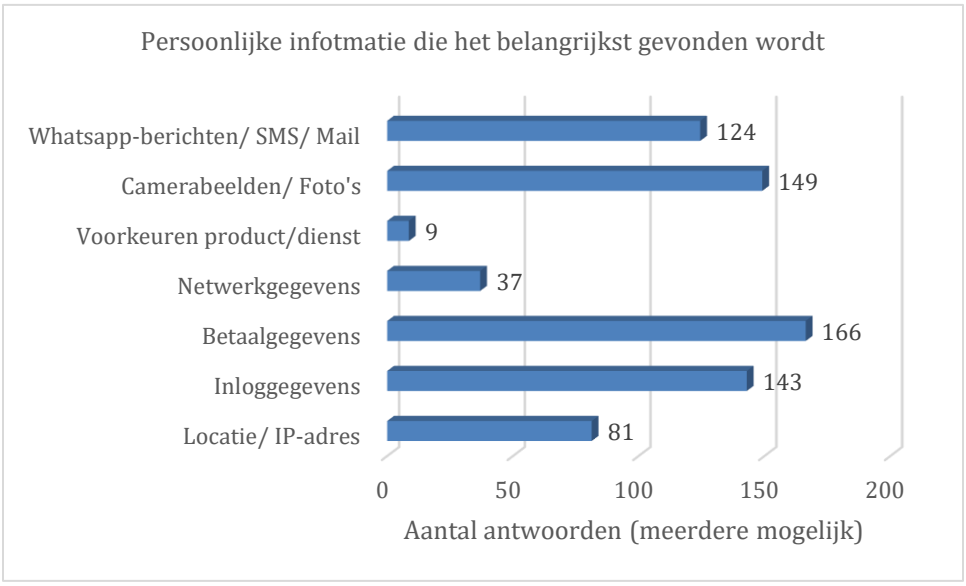
14	**Virusvrij**: 50% **Cookies-vermindering**: 50% **Overheidsdetectie-vrij**: 100% **Advertentie-vermindering**: 100% **Prijs**: €10 per maand	Likertschaal	Integer schaal van 0-100
15	**Virusvrij**: 50% **Cookies-vermindering**:0% **Overheidsdetectie-vrij**: 50% **Advertentie-vermindering**:0% **Prijs**: €0 per maand	Likertschaal	Integer schaal van 0-100
16	**Virusvrij**: 100% **Cookies-vermindering**: 100% **Overheidsdetectie-vrij**: 0% **Advertentie-vermindering**: 50% **Prijs**: €0 per maand	Likertschaal	Integer schaal van 0-100
17	**Virusvrij**: 50% **Cookies-vermindering**: 50% **Overheidsdetectie-vrij**: 0% **Advertentie-vermindering**: 50% **Prijs**: €5 per maand	Likertschaal	Integer schaal van 0-100
18	**Virusvrij**: 0% **Cookies-vermindering**: 100% **Overheidsdetectie-vrij**: 0% **Advertentie-vermindering**: 50% **Prijs**: €10 per maand	Likertschaal	Integer schaal van 0-100
19	**Virusvrij**: 50% **Cookies-vermindering**: 0% **Overheidsdetectie-vrij**: 100% **Advertentie-vermindering**: 50% **Prijs**: €0 per maand	Likertschaal	Integer schaal van 0-100
20	**Virusvrij**: 100% **Cookies-vermindering**: 100% **Overheidsdetectie-vrij**: 100% **Advertentie-vermindering**: 100% **Prijs**: €0 per maand	Likertschaal	Integer schaal van 0-100
21	**Virusvrij**: 0% **Cookies-vermindering**: 0% **Overheidsdetectie-vrij**: 50% **Advertentie-vermindering**: 50% **Prijs**: €5 per maand	Likertschaal	Integer schaal van 0-100
22	**Virusvrij**: 0% **Cookies-vermindering**: 100% **Overheidsdetectie-vrij**: 0% **Advertentie-vermindering**: 100% **Prijs**: €5 per maand	Likertschaal	Integer schaal van 0-100

23	**Virusvrij**: 100% **Cookies-vermindering**: 100% **Overheidsdetectie-vrij**: 0% **Advertentie-vermindering**: 100% **Prijs**: €10 per maand	Likertschaal	Integer schaal van 0-100
24	**Virusvrij**: 0% **Cookies-vermindering**: 0% **Overheidsdetectie-vrij**: 0% **Advertentie-vermindering**: 100% **Prijs**: €0 per maand	Likertschaal	Integer schaal van 0-100
25	**Virusvrij**: 0% **Cookies-vermindering**: 50% **Overheidsdetectie-vrij**: 50% **Advertentie-vermindering**: 100% **Prijs**: €5 per maand	Likertschaal	Integer schaal van 0-100
26	**Virusvrij**: 100% **Cookies-vermindering**: 0% **Overheidsdetectie-vrij**: 0% **Advertentie-vermindering**: 50% **Prijs**: €10 per maand	Likertschaal	Integer schaal van 0-100
27	**Virusvrij**: 100% **Cookies-vermindering**: 0% **Overheidsdetectie-vrij**: 100% **Advertentie-vermindering**: 50% **Prijs**: €10 per maand	Likertschaal	Integer schaal van 0-100
	Afsluitingsvraag		**Afsluitingsvraag**
28	Hoe veilig voel je je op het internet na het invullen van deze enquête?	Multiple Choice	Zeer onveilig/ onveilig/ redelijk/ veilig/ zeer veilig

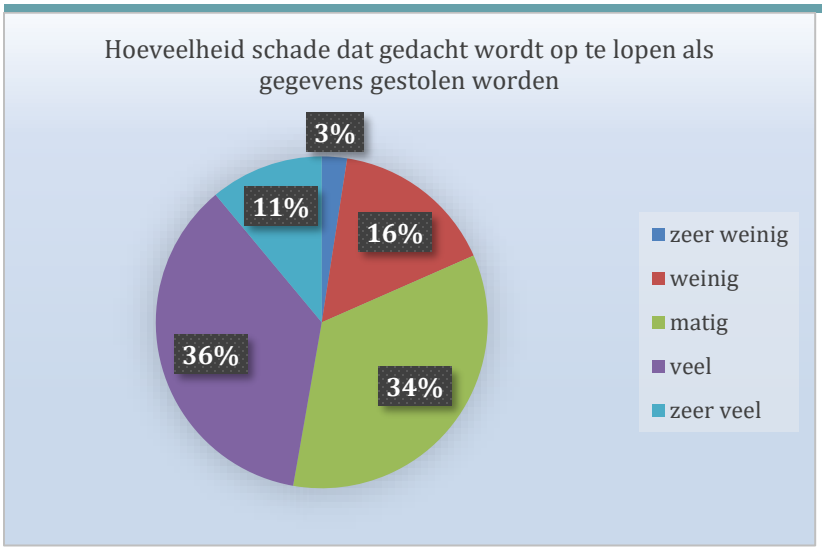
7.2 Figuren



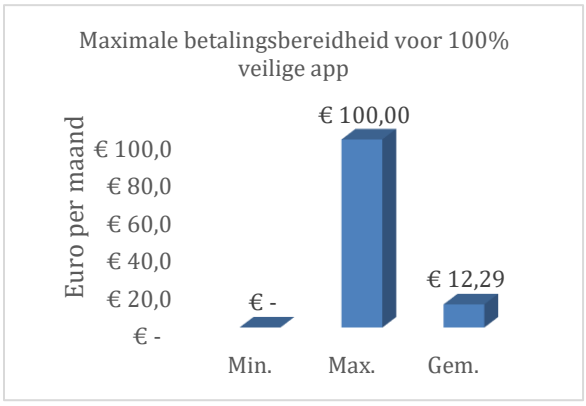
Figuur 6: Het type persoonlijke informatie waarvan gedacht wordt het meest gelekt/gehackt te worden (meerdere antwoorden mogelijk).



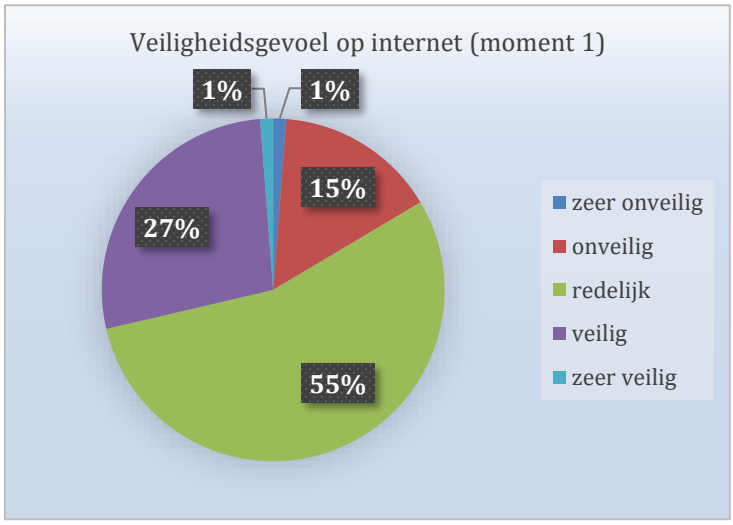
Figuur 7: Het type persoonlijke informatie die het belangrijkst gevonden wordt door de respondenten (meerdere antwoorden mogelijk).



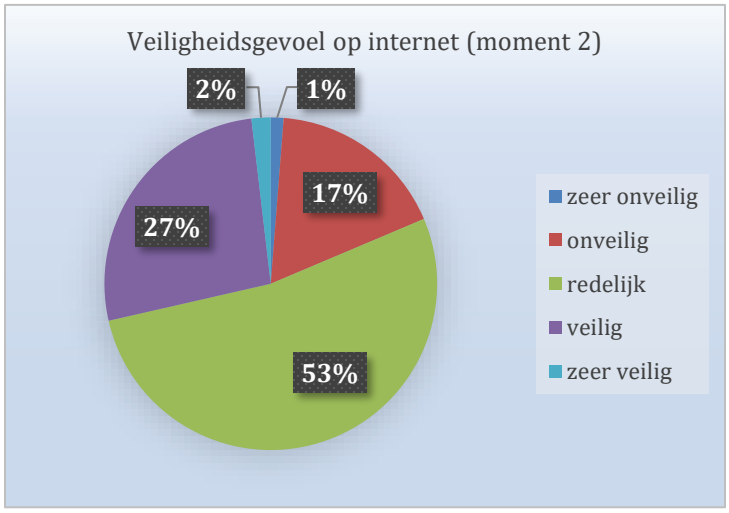
Figuur 8: Hoeveelheid schade dat gedacht wordt op te lopen door de respondenten als gegevens gestolen worden.



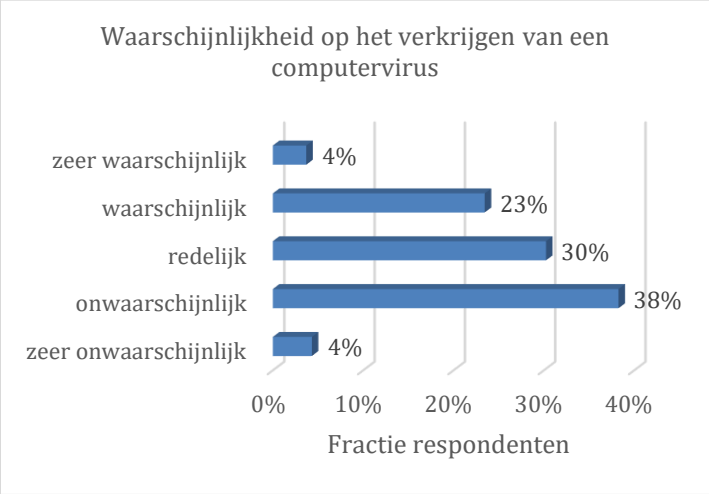
Figuur 13: Gegevens over de maximale betalingsbereidheid voor de 100% veilige app in €/maand.



Figuur 9: Veiligheidsgevoel op internet aan het begin van de enquête.



Figuur 15: Veiligheidsgevoel op internet aan het eind van de enquête.



Figuur 16: Waarschijnlijkheid op het verkrijgen van een computervirus.