

Online & offline privacy

Radboud Universiteit Nijmegen
Bachelorscriptie

25 juni 2011

<i>Naam:</i>	Niek Wolfkamp
<i>Studentnummer:</i>	0709409
<i>Opleiding:</i>	Informatiekunde
<i>Vakcode:</i>	IBI009 (9 ec)
<i>Begeleiders:</i>	Luca Consoli & Theo van der Weide (Radboud Universiteit Nijmegen)
<i>Afstudeernummer:</i>	153

INHOUDSOPGAVE

1.	Voorwoord	4
2.	Het onderzoek.....	5
	Probleemstelling	5
	Verantwoording	6
	Theoretisch Kader	7
3.	Privacy in theorie	8
	Deelvraag 1: Wat wordt tegenwoordig verstaan onder privacy en hoe is dit beschermd?	8
	Privacybescherming	12
	Deelvraag 2: Wat is online privacy en hoe gaat de gebruiker hiermee om?	16
	Deelvraag 3: Wat is offline privacy en hoe gaat de gebruiker hiermee om?	19
	Case: Online en offline betalen.....	21
	Online betalen.....	24
	Offline betalen	26
4.	Privacy in de Praktijk	28
	Situatieschets enquête	28
	Resultaat	30
	Deelvraag 4: In welke mate is de doelgroep zich bewust van zijn privacy?	31
	Deelvraag 5: Hoe gedraagt de doelgroep zich ten opzichte van zijn privacy?	36
5.	Online en offline privacy	40
6.	Conclusie	43
7.	Bibliografie	44
8.	Appendix	46
	Enquête: Online & offline privacy	46
	Verzamelde gegevens	49
	Enquête gegevens: algemeen	49
	Enquête gegevens: stellingen	54

1. VOORWOORD

In deze bachelorscriptie voor de studie Informatiekunde aan de Radboud Universiteit te Nijmegen zal privacy, zowel online als offline, onderzocht worden. Door middel van twee fases, te weten een theoretische fase en vervolgens een praktijk fase, wordt aangetoond hoe de perceptie van personen is ten opzichte van privacy en waarom dit kan verschillen in online en offline situaties.

Voor deze scriptie is een onderzoeksplan opgesteld dat in het volgende hoofdstuk behandeld wordt. In hoofdstuk drie komt het begrip privacy uitvoerig aan bod in haar theoretische context. Aan de hand van een drietal deelvragen zal privacy bestudeerd worden. Hierbij zal informatie vanuit juridisch gebied, ICT en sociologisch perspectief aangevoerd worden. Daaropvolgend komt in hoofdstuk vier de praktijk aan bod. Door middel van enquêtes zal de perceptie van studenten ten opzichte van privacy blootgelegd worden. Ook wordt het verschil tussen online en offline privacy/situaties zo goed als mogelijk uiteengezet en verklaard aan de hand van de theoretische fase.

De onderzoeksvraag wordt op basis van de deelvragen beantwoord in het vijfde hoofdstuk. Hoofdstuk zes bestaat uit een korte conclusie van het gehele onderzoek en suggesties voor aanvullend onderzoek. Na de daaropvolgende bibliografie zijn alle resultaten van onderzoek uit de praktijkfase terug te vinden in de appendix.

De heren Luca Consoli en Theo van der Weide van de Radboud Universiteit Nijmegen hebben bijgedragen in de begeleiding van deze scriptie. Graag wil ik hen bedanken voor suggesties, tips en kritische blik op deze scriptie. Ook scriptiecoördinator Engelbert Hubbers wil ik bedanken voor zijn coördinerende rol en de gegeven feedback.

Ik wens u veel leesplezier,

Niek Wolfkamp

2. HET ONDERZOEK

Voor deze scriptie is het nu volgende onderzoeksplan opgesteld. De probleemstelling, verantwoording en het theoretisch kader zullen aan bod komen alvorens privacy in theorie onderzocht wordt.

Probleemstelling

Tegenwoordig zijn steeds meer mensen zich bewust van hun privacy. Opvallend is wel het onderlinge verschil, omdat de één zeer argwanend en de ander niet voorzichtig is met het verstrekken van privégegevens (1). Er is ook een duidelijk verschil zichtbaar tussen online en offline handelingen. In het dagelijkse leven (offline) is het verstrekken van gegevens vaak niet vanzelfsprekend en wordt hier goed op gepast. Op het internet (online) worden echter heel wat gegevens (soms onbewust) uitgewisseld en komt privacy minder hoog in het vaandel te staan (2). Betalen met een acceptgiro wordt door sommigen veiliger geacht voor de privacy dan betalingen via internet. Recent plaatste de gemeente Nijmegen van alle woningen en panden in haar gemeente erg veel informatie online, waaronder bouwtekeningen. Ook dit zou de bedreiging van privacy erg in de hand kunnen werken. De online en offline handelingen lopen ook steeds meer door elkaar heen en de grens wordt steeds vager waardoor het verschil niet altijd duidelijk te onderscheiden is.

De grens tussen online en offline privacy is echter erg afhankelijk van de mens zelf, wat acht hij verstandig en wat niet? Is men goed op de hoogte van de gevaren met betrekking tot hun privacy en in hoeverre dienen organisaties en de overheid hen hier bewust van te maken? Hierbij speelt ICT een grote rol, zowel qua voorlichting als gemak bij online handelingen. De menselijke factor in het proces van de bescherming van privacy, wat ook raakvlakken met security heeft, is uiteindelijk vaak de zwakste schakel ten opzichte van de techniek/ICT (3).

Interessant is de vraag hoe het verschil tussen online en offline handelingen te verklaren is. Hiertussen bestaat, gezien de online ontwikkelingen, immers een duidelijk verschil. De onderzoeksvraag luidt dan ook als volgt:

“Welke perceptie hebben studenten bij online privacy en welke bij offline privacy, welke verschillen zijn er en hoe zijn deze te verklaren?”

Verantwoording

Tegenwoordig krijgt iedereen met situaties te maken waarbij privacy een belangrijke en grote, al dan niet overheersende, rol speelt (4). De huidige maatschappij is immers doordrongen van dergelijke situaties. Dagelijks vragen bedrijven, instanties en personen om gegevens die de privacy zouden kunnen bedreigen. Een mogelijk extreem gevolg hiervan is identiteitsdiefstal. Aan de andere kant kan het afstaan van dergelijke gegevens voor gemak zorgen. Voorbeelden hiervan zijn informatiestromen die speciaal toegespitst zijn op de gebruiker. Zo maken meerdere websites gebruik van persoonlijke webcontent om de gebruiker van voor hem relevante informatie te voorzien. Dit is gebaseerd op gegevens van deze gebruiker die privacygevoelig kunnen zijn. In dit geval dient zowel de website als de gebruiker een afweging te maken welke gegevens aangeboden worden en in welke mate.

Een persoon zou vrij moeten kunnen kiezen om zodoende in zijn ogen een gezonde balans te creëren tussen privacy en gemak. Waar ligt de ethische grens in deze online wereld ten opzichte van die in de dagelijkse offline wereld. De perceptie hiertussen kent namelijk een verschil. Het aantonen waarom men anders over privacy denkt in de online wereld ten opzichte van in de offline wereld kan deze perceptie verklaren (1). In een rationele situatie zou men zich namelijk gelijk dienen op te stellen en te gedragen, zowel offline als online.

Vanwege het maatschappelijk belang en de relevantie voor elke persoon, die zowel online als offline handelingen uitvoert, kan dit onderzoek een bijdrage leveren. In dit onderzoek komen meerdere aspecten van de studie Informatiekunde aan bod. Uiteraard is er de ICT kant (online), maar daarnaast ook hoe de gebruiker hier mee omgaat. Een afspiegeling aan de kant van de gebruiker in het echte leven (offline) maakt het tot een geheel van factoren die een totaal weergave bieden binnen meerdere wetenschappen. Een geheel goed werkende organisatie of systeem staat of valt door een architectuur en het gedrag van de gebruiker. Een systeem dient daarnaast toegespitst te zijn op de perceptie van de gebruiker. Zowel de gebruiker kan hierdoor met zijn neus op de feiten gedrukt worden en wellicht zal er bewustwording en aanpassing van gedrag plaatsvinden. Ook de overheid en politie kunnen baat hebben bij een verklaring van perceptie op het gebied van voorlichting aan burgers. Daar informatiekunde de brug is tussen gebruiker en de ICT en het academisch niveau meerdere disciplines bevat is dit een relevant onderzoek.

Theoretisch Kader

In dit onderzoek ligt de focus op het onderzoeken van de perceptie van gebruikers bij zowel online als offline privacy. Daarom is het van belang de begrippen in de onderzoeksvraag te definiëren en duidelijk te stellen. Het is nodig om een korte definitie van perceptie, doelgroep/gebruiker en privacy, zowel online als offline, opgesteld te hebben alvorens aan het onderzoek te beginnen.

- **Perceptie**

De perceptie is het gevoel en beeld/oordeel dat een persoon heeft bij in dit geval privacy (1). Deze perceptie komt deels voort uit informatiekunde maar ook uit de sociologie. Dit begrip kent zowel een positieve als negatieve uitstraling. Het beeld kan namelijk positief zijn maar uiteraard ook negatief en alles wat hier tussen in ligt. Dit hangt af van het vertrouwen in de bescherming van privacy en de noodzaak voor deze bescherming. De perceptie zal bij online privacy waarschijnlijk verschillen van die van offline privacy. Perceptie zal in deze scriptie uitgedrukt worden op een 7-puntsschaal waarbij 1 geheel oneens en 7 geheel eens is.

- **Doelgroep/gebruiker**

Een groep personen die representatief is voor het te onderzoeken doel. Aangezien deze binnen de scope en tijd van deze scriptie dient te vallen is gekozen om een groep personen af te bakenen tot een behapbaar aantal en een specifieke leeftijdsgroep. De personen zullen dan ook geselecteerd worden op leeftijd en op basis van de tijd die online besteed wordt. Met gebruiker wordt een persoon uit deze groep aangeduid. In dit geval zijn dit studenten.

- **Privacy**

Een begrip dat al lange tijd bestaat maar sinds enkele voorvallen in de geschiedenis (aanslag 9/11) en opkomende technologieën steeds meer aandacht krijgt. Het hebben van privacy is een recht van de mens (5) (in veel landen opgenomen in de grondwet) en is erg veranderlijk gedurende de jaren (6). Er zijn meerdere soorten privacy. Zo is er privacy in de vorm van persoonlijke vrijheid (het recht om alleen gelaten te worden) en gegevensprivacy, wat doelt op welke gegevens van een persoon bewaard en gebruikt mogen worden voor bepaalde doeleinden. Dit laatste is waar het in deze scriptie om draait.

- **Online en offline**

Privacy is er zowel in de online als offline wereld. Ondanks dat deze scheiding steeds minder herkenbaar is zal dit als volgt gedefinieerd worden. Online privacy is het geval wanneer men op een website of computer/telefoon handelingen uitvoert waarbij persoonlijke gegevens nodig zijn. Deze wereld is ook aan te duiden als virtueel. De offline wereld daarentegen is de echte wereld. Hier speelt privacy ook een rol in de zin dat ook daar persoonlijke gegevens worden uitgewisseld en gebruikt. Een kort voorbeeld: online wereld is betaling via internetbankieren/iDeal en offline wereld is betaling via acceptgiro.

3. PRIVACY IN THEORIE

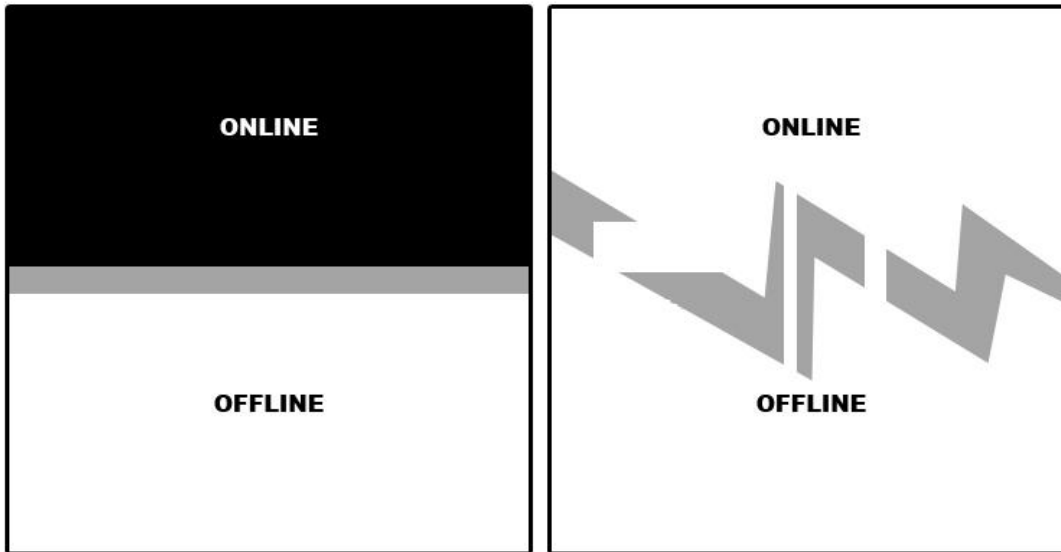
Privacy is niet meer weg te denken uit de huidige maatschappij. Wereldwijd is het een 'hot-issue' aangezien (ICT-)systemen en organisaties er door staan of vallen. Er zijn echter verschillende soorten privacy te kenmerken. Informatieprivacy is datgene waar ook in dit hoofdstuk op in zal worden gegaan. Privacy is vaak een moeilijk begrip in het opzicht van definitie en omgang. Allereerst wordt daarom uiteengezet wat er tegenwoordig verstaan wordt onder privacy en hoe deze privacy beschermd is. Vervolgens wordt dit specifiek gemaakt voor zowel online en offline privacy en hoe gebruikers hier in beide gevallen mee omgaan.

Deelvraag 1: Wat wordt tegenwoordig verstaan onder privacy en hoe is dit beschermd?

Privacy is een verschijnsel dat gekenmerkt wordt door haar veranderlijke opvattingen. Wat precies wel en wat niet onder privacy valt is niet altijd duidelijk zichtbaar, zowel voor bedrijven, overheden maar ook voor individuen. In het verleden werd privacy ook anders opgevat dan tegenwoordig in de eenentwintigste eeuw. Tegenwoordig is het steeds belangrijker dat wat onder privacy verstaan wordt ook daadwerkelijk is vastgelegd in een document of in ieder geval gedefinieerd is. Veelal gebeurt dit in de vorm van een zogenoemde disclaimer of in een privacybeleid. Bij het aangaan van diensten of aanschaffen van producten is er dan vaak een overeenkomst waarin privacy gedetailleerd wordt beschreven voor de betreffende situatie.

Desondanks blijft er altijd ambiguïteit ontstaan. Vooral op internationaal niveau is dit het geval. Volgens Räikkä (2008) (1) blijkt dat per cultuur privacy dusdanig anders opgevat kan worden dat het soms juist wel of juist niet als goed of slecht gezien wordt. Räikkä beschrijft in hetzelfde artikel dat privacy gezien wordt als een kostbaar goed en dat men veelal meer privacy wil hebben dan het geval is. Een persoon zou zich namelijk alleen op eigen wijze kunnen ontwikkelen bij een voldoende niveau aan privacy. Volgens Rachels (1975) (4) blijkt dat het daarnaast lastig is om een precies antwoord te geven op de vraag wat privacy precies is. Rachels geeft aan dat dit komt door het feit dat dit afhangt van meerdere belangen, welke in het geding kunnen komen bij een aanval op hun privacy.

Privacy kan daarnaast zowel plaatsvinden in de online als in de offline wereld. Deze werelden zijn ook steeds meer met elkaar verweven. Tegenwoordig is er geen duidelijke grens meer te trekken tussen beide werelden. Beiden zullen zodanig in elkaar overgaan dat het soms zelfs als eenzelfde wereld gezien kan worden. Dit is schematisch weergegeven in figuur 3.1.1.



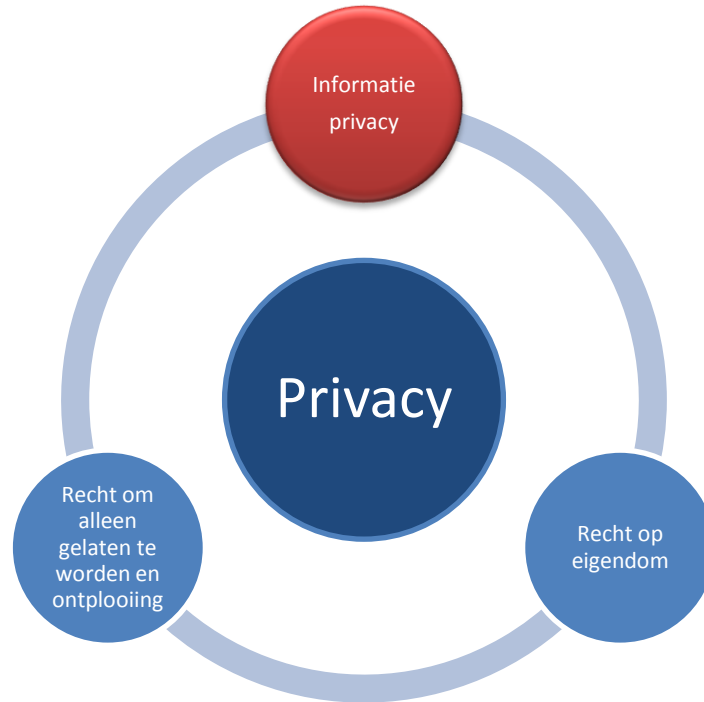
Figuur 3.1.1 “Links: online en offline wereld gescheiden - Rechts: online en offline wereld gaan in elkaar over en de grens wordt vager”

Met de opkomst van computers, mobiele telefoons en (mobiel) internet (zie figuur 3.1.2) wordt dit alleen maar versterkt en is de bescherming van informatie complexer geworden. Ondanks dat de grens tussen online en offline privacy minder duidelijk wordt is er nog wel een verschil tussen deze twee. Ben-Ze'ev (2003) stelt dat privacy en emotionele betrokkenheid en privacy openheid in de echte (offline) wereld verschillen van die in cyberspace (online) (7). Hier is veronderstelde anonimiteit veelal oorzaak van mindere waarde aan privacy. Beweerd wordt dat privacy dan gemakkelijker te creëren is dan in de offline wereld. Ook zal men leren van handelingen in een wereld en deze ook in de andere wereld toepassen. Ondanks de steeds groter wordende samenhang is er dus nog daadwerkelijk een verschil qua omgang.

Jaar	Internet	Mobiel internet
2005	83 %	13 %
2010	94 %	39 %
Toename	11 % (x 1.13)	26 % (x 3)

Figuur 3.1.2 “CBS: Personen in Nederland met internet – Personen in Nederland met internet op mobiele telefoon (in vijf jaar tijd met factor 3 toegenomen). Bijgewerkt op 26 oktober 2010 (8)”

Het voorgaande geeft aan dat privacy een groot en veelomvattend begrip is. In deze scriptie gaat het specifiek om *informatieprivacy*. Daarnaast zijn er meerdere soorten privacy te onderscheiden. Zo is er ook privacy in de betekenis om alleen gelaten te worden en jezelf te kunnen ontplooien, maar ook het recht tot eigendom van bepaalde aspecten. Bijvoorbeeld eigenaar van het eigen lichaam en bepalen wat daarmee gebeurt zonder dit kenbaar te hoeven maken. Onderling zijn er tussen deze soorten wel raakvlakken. In figuur 3.1.3 is dit schematisch weergegeven. Informatieprivacy staat nu centraal en is datgene waar verder op in gegaan zal worden.



Figuur 3.1.3 “Privacy soorten”

Informatieprivacy omvat een groot gebied van het dagelijkse leven. Bij elke aankoop, gebruik van een online of offline dienst of communicatie speelt informatie een belangrijke rol. Veel gegevens hebben als eigenschap dat deze beschermd moeten worden voor correct gebruik en integriteit binnen een systeem of organisatie. Denk bijvoorbeeld aan bankgegevens, verzekeringgegevens, computerbestanden, e-mailberichten/sms en reisgegevens met het openbaar vervoer. Er is wel een verschil qua gegevens die persoonlijk of privé zijn. Persoonsgegevens zijn persoonlijk maar kunnen en moeten kenbaar gemaakt worden voor gebruik van diensten, bijvoorbeeld naam en voorletters. Privé gegevens zijn gegevens die niet kenbaar gemaakt hoeven te worden, bijvoorbeeld een wachtwoord. Wanneer over gegevens gesproken wordt dan gaat het om persoonsgegevens.

Informatie hoeft daarentegen niet per se uit data in de vorm van letters en getallen te bestaan. Ook de beelden die gemaakt worden door bewakingscamera's (in openbare gebieden) verzamelen informatie maar dan in de vorm van beeld. Hetzelfde geldt voor spraakinformatie tijdens een telefoongesprek of in de buurt van microfoons. Hierbij is informatieprivacy tegenwoordig niet meer weg te denken. Regelmatig vinden er dan ook rechtszaken plaats waarbij opvattingen over privacy verschillen. Een recent voorbeeld is dat een telecomprovider het mobiele internetverkeer van klanten zou scannen. De gebruiker zag dit soms als regelrecht af luisteren en inbreuk op zijn privacy. Het bedrijf beweert daarentegen dat het gescand wordt om de kwaliteit van diensten te kunnen garanderen (ook verplicht gesteld door de wet) en dat de inhoud niet bekeken wordt. Een dergelijk voorval kan ook in de offline wereld voorkomen. Bijvoorbeeld wanneer een camera een openbaar gebied moet bewaken maar tegelijkertijd een voordeur van een woonhuis continu in beeld brengt. Door de bewoners kan dit gezien worden als inbreuk op hun privacy.

De gang van zaken rondom privacy is door de overeenkomsten en verschillen tussen online en offline privacy soms lastig te definiëren, ook voor de wet. De wetgeving voorziet namelijk niet altijd in deze online wereld en is meer opgesteld voor de offline wereld. Voordat wetgeving opgesteld kan worden en correct kan worden toegepast moet het onderwerp, in dit geval informatieprivacy, concreet gedefinieerd worden. Woordenboek de Van Dale definieert het woord 'privacy' als volgt:

***pri·va·cy** [prajvesie] de; v(m) de mogelijkheid om in eigen omgeving helemaal zichzelf te zijn*

Deze definitie van privacy is correct maar erg summier en houdt daarnaast niet direct verband met informatieprivacy. Direct verband is er wel met de twee andere soorten uit figuur 3.1.3. Privacy is al sinds lange tijd een recht van de mens. Warren en Brandeis (1890) geven aan dat een individu het recht heeft om totaal beschermd te zijn in persoon en eigendom. Door politieke, sociale en economische veranderingen moest dit recht echter herzien worden (6). Eerst was er enkel bescherming van het fysieke, maar ook bescherming van het spirituele, ofwel informatie, werd steeds belangrijker. Informatieprivacy is dus relatief nieuw. Woordenboek de Van Dale geeft daaropvolgend deze definitie:

***informatieprivacy**; bescherming van persoonsgegevens, m.n. het recht om niet meer informatie over zichzelf te verstrekken en aan niet meer personen dan strikt noodzakelijk is, en het recht om te weten welke persoonlijke informatie er in omloop is, hoe die verzameld is en wat ermee gedaan wordt*

Hier is informatieprivacy redelijk volledig beschreven. Informatieprivacy komt echter steeds vaker in het geding ten bate van de nationale veiligheid. Vooral na de aanslag op 11 september 2001 komt dit vaker en op grotere schaal voor. Veiligheid en privacy staan nu regelmatig haaks op elkaar en hiermee dient rekening te worden gehouden. De bescherming van privacy is belangrijk maar veiligheid zeker ook. Individuele privacy zal dan ook moeten wijken voor nationaal belang. Belangrijk is ook het raakvlak van geldige wetgeving en de ethiek. Beiden zijn belangrijk en gaan soms samen maar staan soms ook tegenover elkaar.

Privacy, en dan specifiek informatieprivacy, is gebaseerd op al het voorgaande tegenwoordig dan ook als volgt te definiëren:

Informatieprivacy: het recht van en de mogelijkheid voor een persoon om zelf te bepalen welke en hoeveel informatie hij prijsgeeft aan anderen (individuele, organisaties, overheden) en kan aanpassen zolang dit voldoet aan:

- Geldende wetgeving en ethiek
- Waarborging van de (nationale) veiligheid
- Essentieel is voor een overeenkomst bij product of dienst
- De cultuur waarin het van toepassing is

Figuur 3.1.4 "Definitie van informatieprivacy"

Uitzonderingen en veranderingen in de maatschappij kunnen zorgen voor noodzakelijke aanpassingen hiervan. Gebaseerd op deze omgevingsvariabelen vinden ook de meeste voorvallen/problemen plaats met betrekking tot privacy. Wanneer bovenstaande correct wordt toegepast is verwerking en gebruik van informatie toegestaan maar zodra (onverwachte) gebeurtenissen optreden die niet stroken met wat verwacht wordt ontstaan er ongewenste situaties. Privacybescherming is dan ook van groot belang om mensen zelf te laten beslissen wat zij prijs geven aan informatie.

Privacybescherming

De bescherming van informatieprivacy is een complex vraagstuk. Wat privacy precies is en hoe veranderlijk dit is bleek uit de vorige paragraaf. Zowel in Nederland als andere landen in de wereld staat privacybescherming hoog in het vaandel. Het is van dusdanig belang dat de grondwet hierin voorziet. Uit de grondwet voor het Koninkrijk der Nederlanden, Hoofdstuk 1: Grondrechten, Artikel 10 blijkt het volgende:

- 1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
- 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
- 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.*

Het eerste punt gaat in op een ander soort privacy. Het tweede en derde punt hebben vooral betrekking op de bescherming van informatieprivacy maar hebben ook raakvlakken met de andere soorten privacy. Voernoot erbij is wel dat de wet opsporingsdiensten als politie bevoegdheid mag geven om gegevens toch in te zien en zo inbreuk te maken op privacy. Zonder deze bevoegdheid is dit absoluut niet toegestaan. Het handhaven hiervan zorgt soms ook voor moeilijke situaties en privacyorganisaties zetten hier vaak hun vraagtekens bij. Echter, in beginsel is de privacy van een persoon beschermd. Hij mag bepalen welke informatie hij prijsgeeft, wel met inachtneming van de voorwaarden genoemd in figuur 3.1.4.

Om toe te zien op de bescherming van informatieprivacy is in Nederland het College Bescherming Persoonsgegevens (CBP) in het leven geroepen. Kort gezegd houdt dit orgaan toezicht dat de volgende drie wetten nageleefd worden door organisaties, overheden en personen:

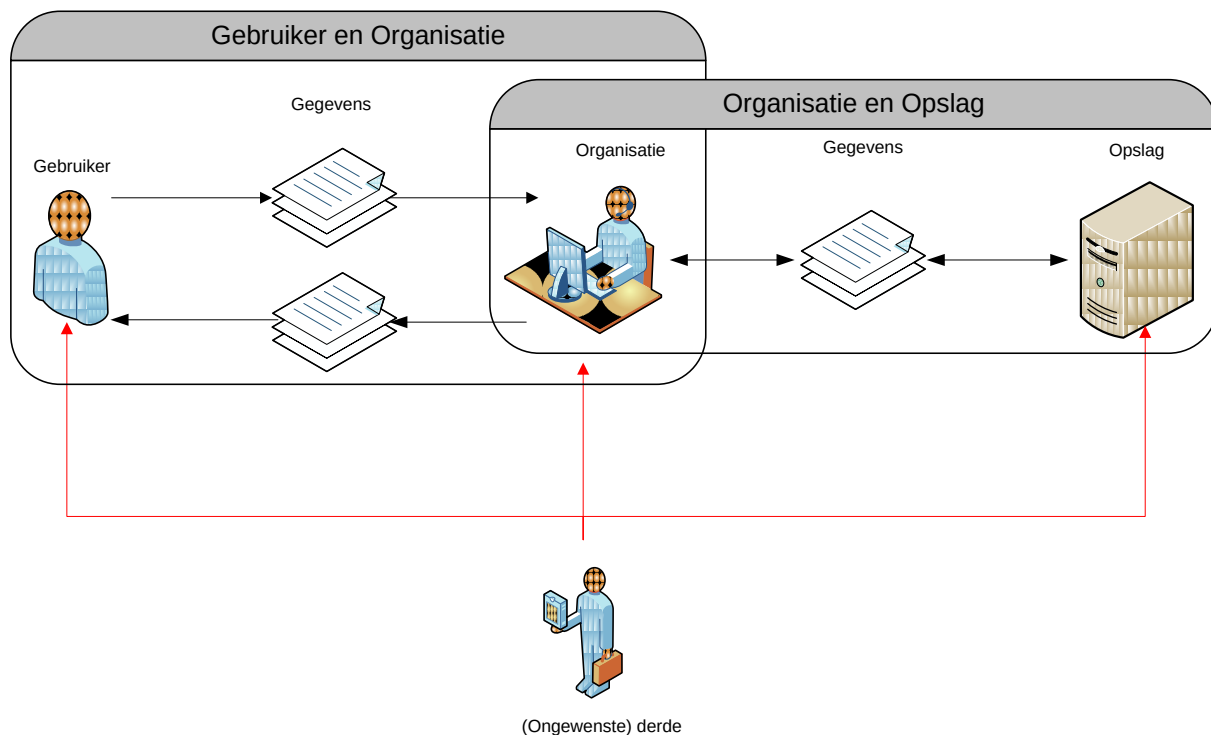
- Wet bescherming persoonsgegevens (Wbp)
- Wet politiegegevens (Wpg)
- Wet gemeentelijke basisadministratie (Wet GBA)

Deze drie uitgebreide wetten, welke elk uit meerdere hoofdstukken en artikelen bestaan, zijn dermate complex dat deze soms onbewust maar ook bewust overtreden worden. Aan het CBP de taak erop toe te zien dat dit niet gebeurt. Dat dit nodig is blijkt uit het jaarverslag 2009 van deze organisatie. Daarin

(9) komt naar voren dat in de sectoren internet en telecom, financiële gegevens, medische gegevens, politie en justitie en de private sector gegevens van miljoenen mensen niet op daarvoor bestemde wijze gebruikt zijn. Het gaat hier veelal om gebruik voor commerciële doeleinden waarbij gegevens aan derden worden doorverkocht.

De bescherming van privacy is zo goed mogelijk geregeld met deze wetten en controlerend orgaan. Privacybescherming is belangrijk voor de waarden van de mens maar de wet voorziet, zoals eerder aan bod gekomen, niet altijd. Veelal is het ook niet privacy maar een ander aspect, dat weliswaar voortvloeiend uit privacy, wat beschadigd wordt aldus Gavison (1980) (5). Inbreuk op privacy kan dus vergaande gevolgen hebben. In beginsel dient privacy daarom beschermd te worden want de gevolgen kunnen ernstig zijn voor zowel personen als voor organisaties. Het kan gaan van relatief onschuldige voorvallen als gebruik voor marketing tot aan een extreem geval als identiteitsdiefstal. Bij dit laatste is privacy dermate ondergeschikt geworden dat kwaadwillende over voldoende persoonlijke- en privé gegevens beschikken om een identiteit na te bootsen of aan te nemen.

Bij elke stap waarin informatie uitgewisseld wordt, opgeslagen wordt of op enigerlei wijze gebruikt wordt is bescherming nodig. Bescherming is op de volgende punten noodzakelijk:



Figuur 3.1.5 "Punten waar bescherming van informatieprivacy noodzakelijk is"

Bovenstaand figuur is een situatieweergave waarin informatie een essentiële rol speelt. Aan de hand van een voorbeeld kan dit geïllustreerd worden.

Bij de volgende deelvragen wordt meer ingegaan op de online en offline situaties. De 'gebruiker' is de afnemer van een dienst, in dit geval een verzekering. Voordat hij verzekerd is dient hij gegevens over zichzelf te verstrekken aan de 'organisatie'. In dit geval wordt er vanuit gegaan dat de overdracht van gegevens niet door derden onderschept kan worden. Vanaf dat moment is belangrijk dat de gebruiker op de hoogte is waarvoor de gegevens bestemd zijn, ofwel de organisatie dient een privacyverklaring beschikbaar te kunnen stellen. Hierin staat vermeld wat er met de gegevens gebeuren kan en mag. Ook aanmelding bij het College Bescherming Persoonsgegevens is nodig voordat een organisatie dergelijke gegevens mag gebruiken. De organisatie verwerkt deze gegevens en slaat deze vervolgens op in haar database/opslag. Ook vindt er terugkoppeling plaats naar de gebruiker in de vorm van een bevestiging of afhandeling van claims. Dit is een manier van werken die in heel veel situaties opgaat. In dit voorbeeld bij een verzekering afsluiten, maar ook bij het online kopen van een product, versturen van een brief aan een organisatie, een geldoverboeking of een telefoongesprek naar een helpdesk.

Bij elke stap kan echter een bedreiging optreden waarbij de privacy in het geding komt. De gegevens kunnen in handen van ongewenste derden vallen of niet op de manier gebruikt worden waarvoor deze bedoeld zijn. Situaties als persoonlijke marketing kunnen hieruit voortvloeien. De informatieprivacy kan in deze situatie (figuur 3.1.5) door de volgende voorvallen niet beschermd zijn:

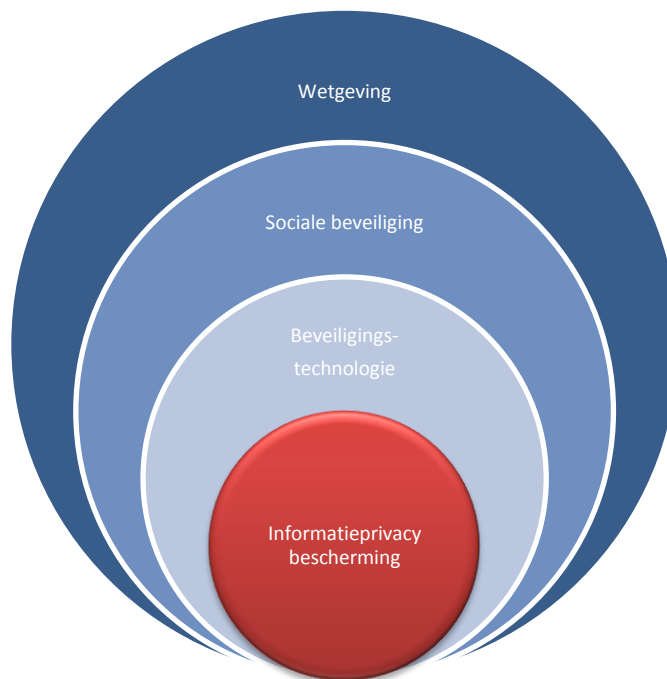
1. Gebruiker:
 - a. De gebruiker kan gegevens (onbewust) naar de onjuiste bestemming versturen.
 - b. Een persoon kan zich voordoen als iemand anders om zo gegevens te bemachtigen, dit wordt ook wel 'social engineering' genoemd. Dit kan zowel in het offline leven (door langs de deur te gaan of op te bellen), als in het online leven met bijvoorbeeld 'phishing' (dit gebeurt met nagemaakte websites waarmee gegevens onderschept worden).
2. Organisatie:
 - a. De organisatie kan de gegevens gebruiken voor niet bestemde interne doeleinden.
 - b. Medewerkers kunnen onzorgvuldig omgaan met persoonlijke gegevens.
 - c. De organisatie kan gegevens doorgeven of verkopen aan derden die daar hun voordeel mee kunnen doen.
 - d. Net als bij een gebruiker kan een persoon zich als iemand anders voordoen om gegevens te bemachtigen.
3. Opslag:
 - a. Geen of onvoldoende beveiliging en toegangscontrole.
 - b. Geen correcte datavernietiging bij vernieuwing apparatuur.

De wetgeving voorziet in dergelijke bedreigingen. Deze rol is essentieel aangezien de wet aangeeft wat illegaal, en dus strafbaar, is. Het CBP is naast justitie en politie zo'n controlerend orgaan dat erop toeziet dat de wetten nageleefd worden. Dit zou al in een groot deel van informatieprivacy moeten voorzien. Onder andere door de achteraf werkende sanctiefunctie.

De sociale beveiliging is tevens noodzakelijk. Naar Winkler en Dealy (1995) blijkt immers dat enkel vertrouwen op informatie beveiligingstechnologie zeer onverstandig is. Het sociale aspect is minstens zo

belangrijk. Door social engineering kunnen gegevens bemachtigd worden zonder ook maar een technologische beveiliging te omzeilen (10). Dit kan op veel niveaus en bij de verschillende partijen.

De derde schakel in de bescherming is beveiligingstechnologie. Technologieën als encryptie, firewalls, virusscanners, toegangscontrole (wachtwoord e.d.) en detectiealgoritmes voor ongebruikelijke gebeurtenissen maken hier deel van uit. Ook op deze schakel, en sociale beveiliging, is wetgeving van belang. Het geheel is te zien zoals weergegeven in figuur 3.1.6. Privacybescherming kent drie schakels, wetgeving is overal van toepassing, beveiligingstechnologie ligt het dichtst bij de gegevens en daaropvolgend is er de sociale beveiliging. Wanneer deze drie correct uitgevoerd worden, in relatie tot elkaar staan en continu up to date gehouden worden is er sprake van een zo goed mogelijke bescherming van informatieprivacy.



Figuur 3.1.6 “Drie schakels bij bescherming van informatieprivacy”

Informatieprivacy in het algemeen is nu aan bod gekomen. Nu zal specifiek in gegaan worden op online privacy en vervolgens offline privacy.

Deelvraag 2: Wat is online privacy en hoe gaat de gebruiker hiermee om?

Informatieprivacy is een veel omvattend begrip. Veel andere aspecten hangen er mee samen en ook online drukt het haar stempel op allerlei handelingen. Door online handelingen en gebeurtenissen treedt privacy, en de eventuele problematiek hiervan, steeds meer op de voorgrond. Door online toegang, verwerking en het beschikbaar stellen van gegevens is snelheid een groot gemak en risico geworden. Ook zijn er steeds meer apparaten met online toegang. Online is in de context van deze scriptie te kenmerken aan hand van de volgende eigenschappen:



Figuur 3.2.1 “Online eigenschappen”

Uit figuur 3.2.1 blijkt dat een eigenschap van ‘online’ is dat het in principe altijd bereikbaar is. Vanaf de hele wereld zijn gegevens en services 24 uur per dag te bereiken. Hiervoor is een digitaal apparaat benodigd, bijvoorbeeld een laptop of ook steeds vaker een mobiele telefoon. Alle gegevens zijn virtueel en dus niet tastbaar (tenzij gegevens geprint of opgeslagen worden en zo dus offline raken). Samenhangend hiermee is dat de ruimte voor data vrijwel onbeperkt is. Kostte een Megabyte vroeger nog honderden dollars, inmiddels is dit teruggelopen naar een paar cent. Mede door het virtuele aspect en vele mogelijkheden waardoor fouten en risico’s kunnen ontstaan zijn er beveiligingsaspecten aan te merken. Deze kunnen technisch zijn maar ook sociaal door het gevoel van online anonimiteit. In de realiteit is dit vaak anders. Personen en bewerkingen zijn gemakkelijk te loggen en dus op te slaan (ook vanwege vrijwel onbeperkte data opslag mogelijkheid). Tot slot is er de mindere controle. Ook dit vloeit voort uit de technologische bedreigingen. Aangezien het virtueel is, kan soms onbewust informatie verstuurd worden.

Online worden er dus steeds vaker en steeds meer gegevens verstuurd. Dit brengt immers namelijk veel gemak met zich mee. Men hoeft de deur niet meer uit, het gewenste is gelijk te raadplegen en contacten met andere personen kunnen gemakkelijk onderhouden worden. Vooral bij gebruik van persoonlijke gegevens beroept men zich op zijn privacy en gaan zij er vanuit dat deze beschermd worden. De afgelopen jaren is er ook een stijging te zien van handelingen met commerciële producten/diensten en persoonsgegevens (figuur 3.2.2). Vooral gegevens hiervan zijn interessant voor derden.

Soort	2005	2010
Bankieren via internet	58 %	81 %
Kopen/verkopen van goederen	45 %	58 %
Telefoneren via internet	6 %	19 %
Officiële documenten downloaden (overheid)	26 %	37 %
Ingevulde documenten versturen (overheid)	24 %	36 %

Figuur 3.2.2 “CBS: ICT gebruik van personen met internet naar persoonskenmerken; *bijgewerkt op 26 oktober 2010 (8)*”

Er is overal een stijgende lijn te zien. Dit draagt eraan bij dat informatieprivacy in de computer ethiek één van de meest evidente en urgente problemen is geworden, zo beweert ook Floridi (2006) (11). De extreem toegenomen verwerkingssnelheid van gegevens, ofwel capaciteit, en de kwaliteit en kwantiteit van gegevens zouden hier de aanwijsbare oorzaak van zijn. Floridi duidt dit aan als de ‘2P2Q hypothese’, gebaseerd op de Engelse termen ‘processing capacities’, ‘pace’, ‘quantity’ en ‘quality’. Dit zijn technieken om grote hoeveelheden gegevens snel en nauwkeurig te verwerken. ICT brengt daarom een radicale verandering te weeg in de online wereld welke op den duur ook in de offline wereld tot uiting zal kunnen komen.

In dit geval is online privacy dus informatieprivacy waar gebruik van gemaakt wordt in de online wereld. Hierbij kunnen gemakkelijk en zonder veel kosten veel gegevens verzameld en op onjuiste manier gebruikt worden. Zowel gebaseerd op de gestelde wetgeving als op het gevoel dat een persoon hierbij heeft. Vandaar dat regelgeving en ethiek, net als bij privacy in het algemeen, noodzakelijk is. Aangezien dit ten opzichte van offline privacy (zie volgende deelvraag) relatief nieuw is, is men (vooral in het begin) argwanend. Uit het voorgaande blijkt dat men eerst afwacht alvorens veelvuldig gebruik gaat maken van online technieken waarbij persoonsgegevens relevant zijn. Hiervoor dient eerst vertrouwen te worden opgebouwd. Gebaseerd op Koehn (2003) bestaan er de volgende soorten vertrouwen (12):

1. Doel-gebaseerd vertrouwen:

Vorm van vertrouwen waarbij twee of meer personen denken hetzelfde doel te hebben. Dit kan zowel een goed als slecht doel zijn. Propaganda en manipulatie kan dit soort vertrouwen versterken.

2. Calculerend vertrouwen:

Vorm van vertrouwen waarbij een persoon de betrouwbaarheid van de ander probeert te berekenen/achterhalen door op zoek te gaan naar bewijs voor elkaars betrouwbaarheid. Ook wel een 'utility-relation'.

3. Kennis-gebaseerd vertrouwen:

Vorm van vertrouwen waarbij personen elkaar vertrouwen op basis van gebeurtenissen uit het verleden of door eerdere omgang. Meer een 'friendship-relation' dan 'utility-relation'.

4. Respect-gebaseerd vertrouwen:

Vorm van vertrouwen dat ontstaat en versterkt wordt op basis van respect tussen personen. Zij hebben overeenkomsten en zijn bereid om te overleggen en elkaar te begrijpen. Meest geschikte vorm voor betrouwbare personen. (12)

Deze vier soorten van vertrouwen gaan zowel op in de online maar ook in de offline wereld. Koehn vat vertrouwen samen als een variëteit van verschillende vormen. Rode draad bij al deze vormen is echter dat vertrouwen van een persoon gebaseerd is op de verwachting van de goede wil van een bepaalde partij. Deze verwachting kan gedurende de omgang veranderen. Om online vertrouwen te winnen en personen dus een goed gevoel van bescherming van hun informatieprivacy te geven moet er volgens Koehn online aan het volgende voldaan zijn:

- Partijen moeten transparant zijn
- Websites en vermeldingen moet gebruikersvriendelijk zijn
- Leveranciers moeten kopers de keuze geven om geïnformeerd te worden
- Degene die vertrouwd willen worden moeten een goede reputatie hebben
- Degene die vertrouwd willen worden moeten maatwerk en feedback toestaan
- Degene die vertrouwd willen worden moeten wederzijdse betrekkingen initiëren
- Vertrouwde partijen moeten reageren op problemen en beschadigd vertrouwen herstellen
- Personen moeten nadenken over de redelijkheid van hun verwachtingen
- Personen moeten middelen voor een toevlucht hebben bij beschadiging van vertrouwen (12)

Dit is veelal een tijdrovend proces maar de omgang van de gebruiker is hierop gebaseerd. De andere partij raakt pas geaccepteerd bij de gebruiker indien een band van vertrouwen is opgebouwd. De gebruiker gaat daar eerst terughoudend mee om maar wanneer dit vertrouwen (in het meest ideale geval respect-gebaseerd vertrouwen) er is dan blijft deze gebruiker met de andere partij vertrouwd totdat dit eventueel beschadigd raakt. Soms heeft de gebruiker echter geen keuze en wordt hij gedwongen gebruik te maken van een dienst van een andere partij. Online en offline privacy hebben qua vertrouwen veel overeenkomsten, de volgende deelvraag gaat in op offline privacy waarna voor beide soorten een case over *betalen* uitgewerkt zal worden.

Deelvraag 3: Wat is offline privacy en hoe gaat de gebruiker hiermee om?

Informatieprivacy in de offline wereld neemt een andere plaats in dan die in de online wereld. Hier zijn geen technieken om grote hoeveelheden gegevens te verwerken (geen '2P2Q' (11)) en kost inbreuk maken op privacy simpelweg meer moeite. De gebruiker is met zijn gezond verstand ook eerder bewust van bedreigingen dan dat dit online het geval is. Dit heeft er mee te maken dat het tastbaarder is en niet zo zeer virtueel. Offline is in de context van deze scriptie te kenmerken aan hand van de volgende eigenschappen:



Figuur 3.3.1 "Offline eigenschappen"

Uit figuur 3.3.1 blijkt dat een eigenschap van 'offline' is dat het in principe niet altijd bereikbaar is. Alleen op bepaalde tijden kan communicatie plaatsvinden, bijvoorbeeld briefverkeer of telefoongesprekken. Daarnaast vinden de handelingen vaak op papier plaats. Of via gesprekken en beelden waarover de gebruiker direct controle uit kan oefenen aangezien dit tastbaar is. Dit brengt gelijk een stop met zich mee qua hoeveelheid gegevens en de opslag van data is dan ook beperkt. Ook hier zijn beveiligingsaspecten aan de orde. Voornaamste is hier de bedreigingen in de vorm van social engineering of onwetendheid/nalatigheid van de gebruiker. De technische bescherming is hier in ieder geval minder van belang maar de sociale des te meer.

De perceptie is wel anders dan die in de online wereld. Dezelfde vier soorten vertrouwen zijn van toepassing maar hier is de gebruiker nauwlettender en meer op zijn hoede. Het op straat uitdelen van persoonlijke gegevens zal iemand niet snel doen terwijl hij deze daarna maar al te gemakkelijk op social media als Twitter en Facebook plaatst. Het verschil in perceptie is dus anders. In de offline wereld ziet men zich meer als een daadwerkelijk persoon. Privacy staat daar dan ook hoger in het vaandel wanneer

gelet wordt op de uitgevoerde handelingen. Het te vertrouwen object is daar veelal een persoon of organisatie, ook wel een entiteit zo beschrijven Shankar, Urban en Sultan (2002) (13). Het is dus gelijk tastbaar, iets wat bij online privacy niet het geval is. De perceptie van offline privacy kan daarnaast wel voortvloeien uit online privacy. Wanneer beiden consistent zijn kan het vertrouwen groeien. Volgens Shankar, Urban en Sultan is online vertrouwen belangrijk maar offline vertrouwen ook. Er zijn overeenkomsten maar belangrijk is dat bij online vertrouwen de entiteit de technologie is, en dus abstract.

Online privacy en offline privacy en de omgang van de gebruiker zijn schematisch weergegeven in onderstaande tabel (figuur 3.3.2).

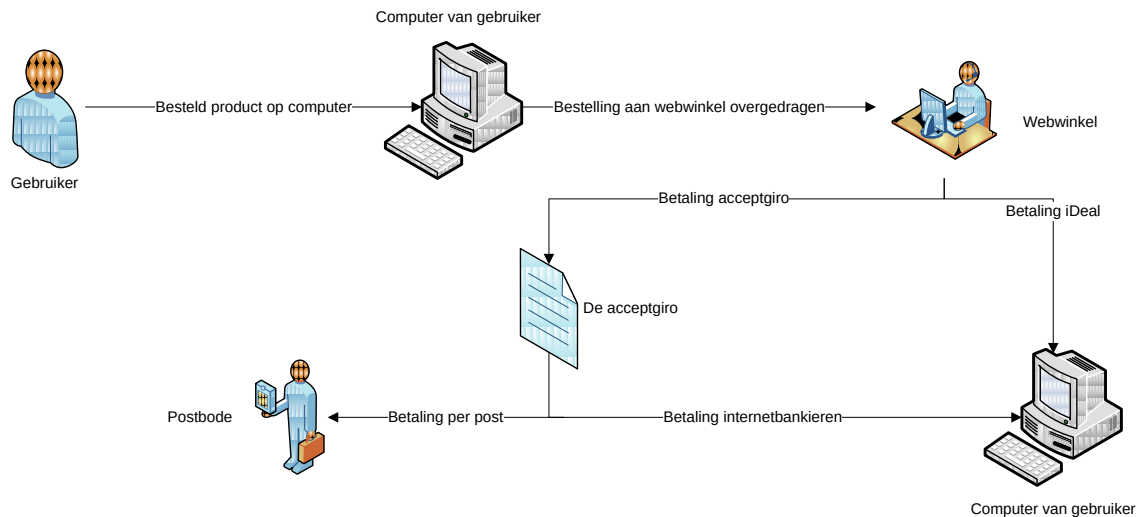
	Online Privacy	Offline Privacy
Definitie	Informatieprivacy waarbij gebruik wordt gemaakt van digitale communicatie via een apparaat door een persoon.	Informatieprivacy waarbij gebruik wordt gemaakt van spraak, beeld en schrijven van een persoon.
Andere partij	Gezien als technologie en niet direct tastbaar, dus abstracter	Gezien als een persoon of organisatie en dus concreter
Bereikbaarheid	Altijd bereikbaar	Op bepaalde tijden bereikbaar
Omgang	Gewenningsperiode doordat het relatief nieuw is en eerst minder vertrouwd	Eerder een vertrouwd gevoel (vanuit ervaringen)
Wetgeving	Wetgeving minder duidelijk	Wetgeving duidelijker
Proces	Snel grote hoeveelheden gegevens verwerken (onbeperkt)	Minder snel kleinere hoeveelheden gegevens verwerken (beperkt)
Beveiliging	Wetgeving, vooral technische en daarnaast ook sociale beveiliging	Vooraf wetgeving en sociale beveiliging

Figuur 3.3.2 “Online en offline privacy”

Case: Online en offline betalen

Om het verschil tussen online en offline privacy verder te verduidelijken zal nu een case uitgewerkt worden. De handeling voor de case is het betalen voor een besteld product. Dit product is besteld in een webwinkel. Uit figuur 3.2.2 blijkt al dat 58 procent van de Nederlanders producten via internet koopt (of verkoopt). Maar liefst 81 procent maakt gebruik van internetbankieren in de algemene zin van het woord. Online betalen in een webwinkel is voor sommigen echter een stap die zijn niet graag zetten. Webwinkels bieden dan ook verschillende manieren van betalen aan. Dit kan zowel direct online via iDeal als achteraf via een acceptgiro. Bij online betalen met iDeal speelt online privacy een rol. Bij offline betalen door middel van een acceptgiro gaat het om offline privacy.

De webwinkel biedt iDeal aan als betaalmiddel dat voordeliger is. Het bedrag staat dan immers op hun rekening en het proces is minder foutgevoelig. Aangezien niet iedereen beschikt over de kennis en motivatie om iDeal te gebruiken als betaalmiddel biedt de winkel ook betaling via acceptgiro aan. Dit gebeurt na of bij aflevering van het product. Dit is minder voordelig voor de webwinkel en zij brengt daarom vaak ook een klein bedrag in rekening bij betaling door middel van acceptgiro. Veel mensen zijn echter nog steeds bereid om dit te betalen. Dit kan vanuit verschillende motieven zijn, waaronder gemak maar ook minder vertrouwen in online privacy dan in offline privacy. Ook heeft de gebruiker bij de acceptgiro achteraf de keuze om het per post te versturen of per internetbankieren over te maken. De gang van zaken is weer te geven zoals in figuur 3.4.1.



Figuur 3.4.1 "Gang van zaken betaling webwinkel"

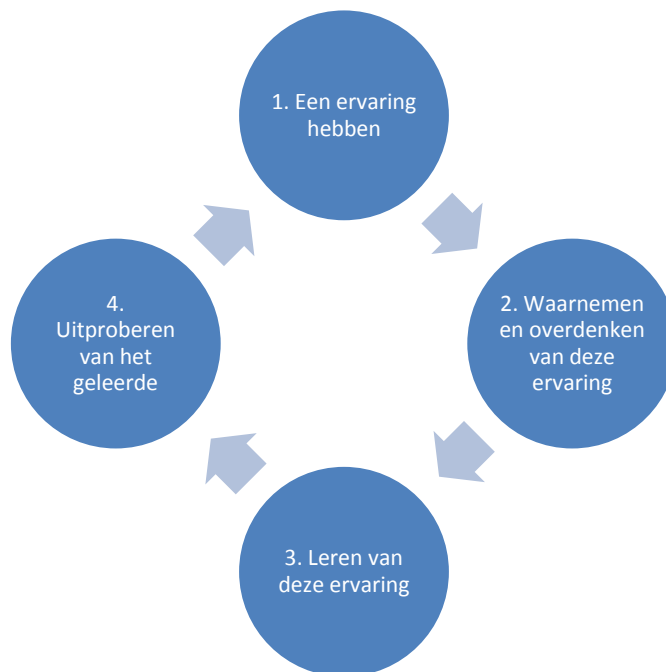
iDeal is volgens de ontwikkelaar Currence, een organisatie die zorgt voor het faciliteren van het betalingsverkeer in Nederland, een betaalmethode die meerdere voordelen heeft ten opzichte van andere methodes. Het blijkt dat hiermee ingespeeld wordt op gebruikersgemak en openheid maar vooral vertrouwen en veiligheid. Het bedrijf en alle deelnemende banken willen ervoor zorgen dat de veiligheid en online privacy door de gebruiker vertrouwd wordt. Betalen via de eigen bank en dus de

eigen internetbankier-omgeving is een belangrijk punt. Hierbij wordt ook voldaan aan de criteria volgens Koehn (12) uit deelvraag 2. In figuur 3.4.2 is het aantal transacties met iDeal en de acceptgiro uiteengezet. Deze zijn gebaseerd op gegevens van Currence (14).

	2006	2010	Vershil
iDeal	4,5	68,8	+ 64,3
Acceptgiro	174	152	- 22

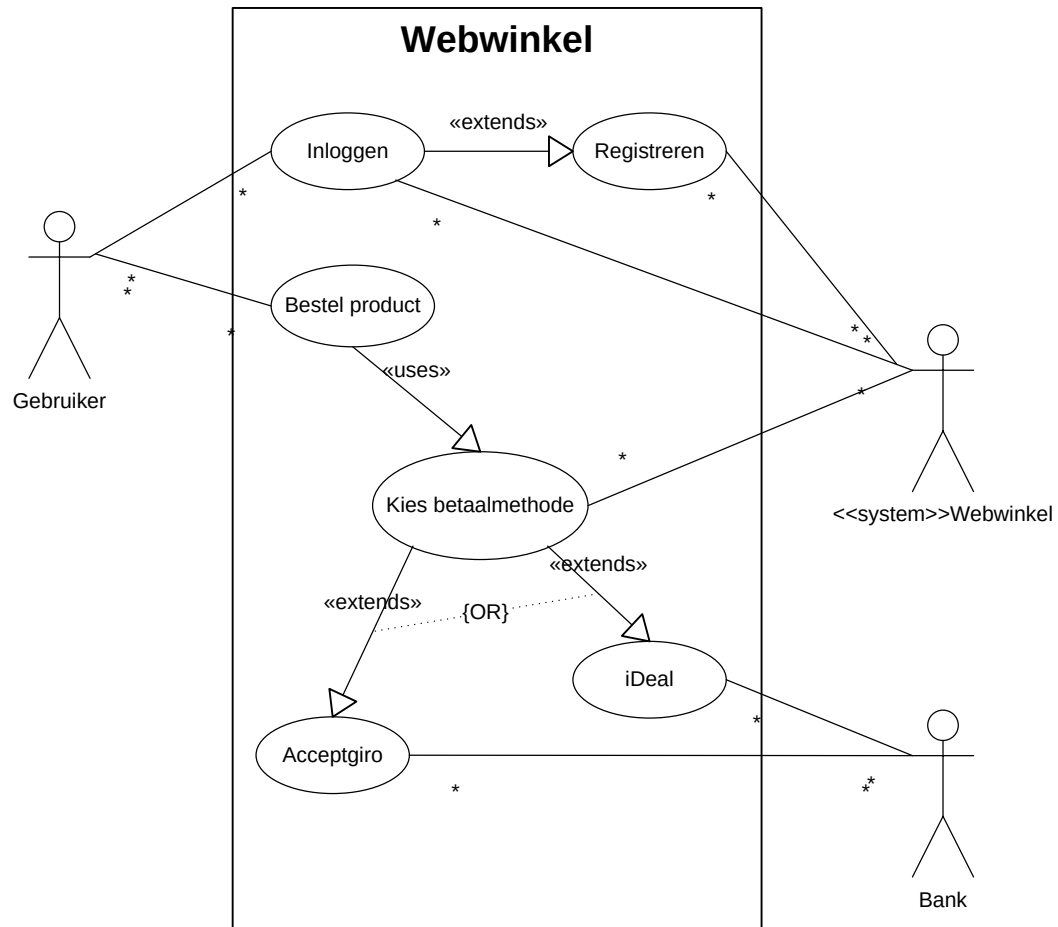
Figuur 3.4.2 “Transacties (in miljoenen) met iDeal en Acceptgiro (14)”

Daarnaast zijn er ook nog de volgende betaalmethoden: PIN, Chipknip en de incasso's/machtigingen. In deze case ligt de focus op iDeal en de acceptgiro. Opvallend is dat iDeal in een snel stijgende lijn zit en de acceptgiro in een licht dalende lijn. Een steeds groter aantal mensen is dan ook al te plaatsen in stap vier van de leercyclus van Kolb in figuur 3.4.3. Het is te stellen dat offline privacy zich al geheel in deze laatste fase bevindt. Online privacy is meer verspreid over de vier stappen. Sommige gebruikers bevinden zich ook al in deze stap terwijl anderen er nog een eerste ervaring mee moeten hebben, hier nog goed over na willen/moeten denken of eerst hiervan willen leren alvorens het uit te proberen. Hieruit kan een nieuwe ervaring voortvloeien waardoor het een continu proces is.



Figuur 3.4.3 “De vier stappen gebaseerd op de leercyclus van Kolb (15)”

Zowel iDeal als acceptgiro hebben te maken met privacy, iDeal met online privacy en de acceptgiro met offline privacy. Aanvullend hierop blijkt echter dat dit ook te beschouwen is als een soort mengvorm aangezien de acceptgiro uiteindelijk ook online betaald kan worden. In figuur 3.4.1 zijn net als in figuur 3.1.5 plaatsen te herkennen waar (bescherming van) privacy belangrijk is. In figuur 3.4.4 is de UML use case te zien van de webwinkel.



Figuur 3.4.4 "Use case Webwinkel"

Online betalen

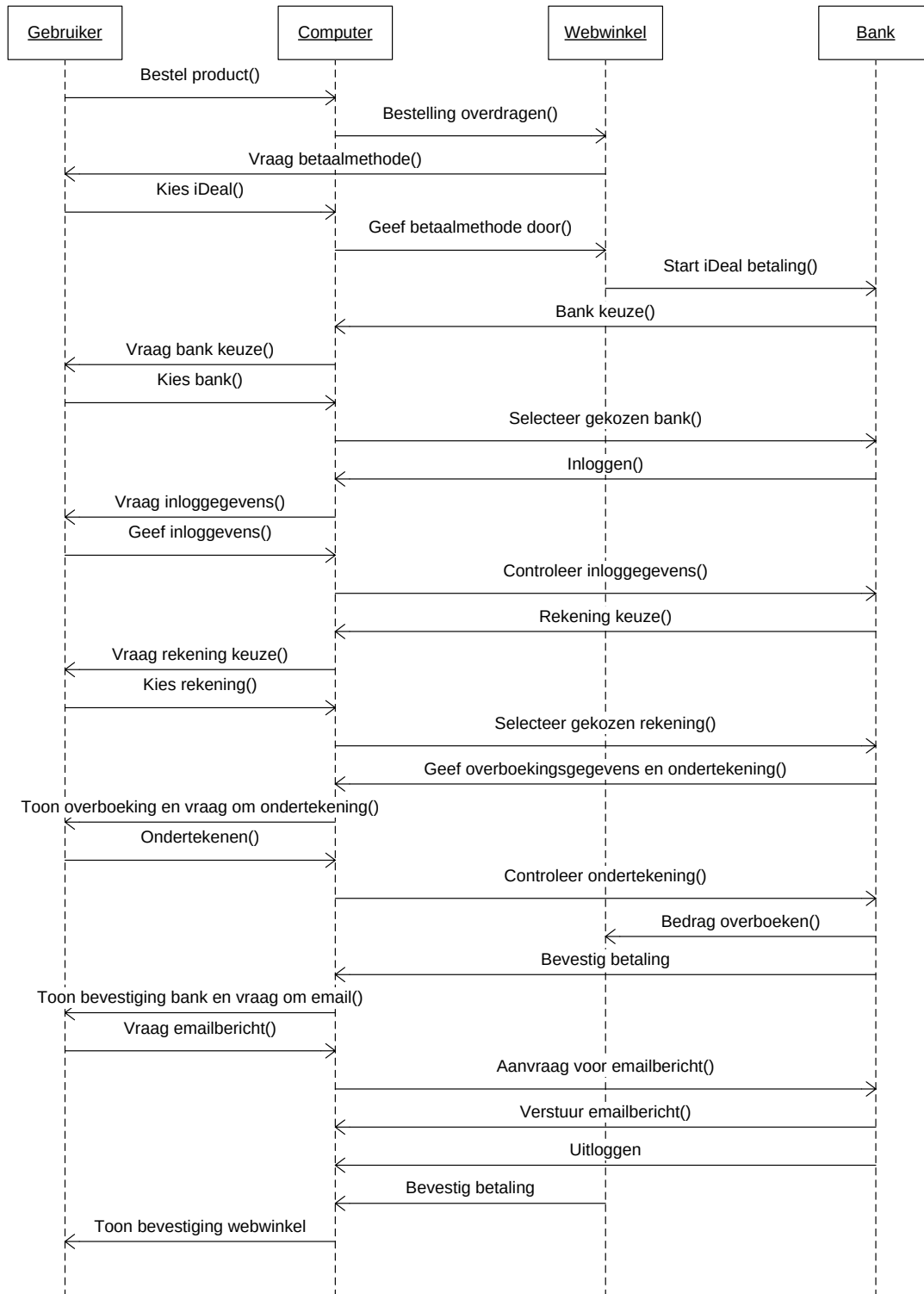
Het online betalen vindt plaats met iDeal en kent geen offline factoren. Online privacy is van groot belang. De gang van zaken bij een online betaling met al haar privacy aspecten is met behulp van de UML Use Case uiteen te zetten (figuur 3.4.4) vanaf 'iDeal'. Het voorgaande ('Inloggen', 'Bestel product' etc.) kent uiteraard ook online aspecten maar om het verschil te verduidelijken wordt dit buiten beschouwing gelaten. Vanaf het moment dat de betaalmethode is gekozen worden er persoonlijke gegevens verstuurd tussen gebruiker, webwinkel en de bank. Dit gebeurt via de computer over het internet.

Nadat het product besteld is en 'iDeal' als betalingsmethode is geselecteerd begint de uitwisseling van gegevens waar het bij online betalen om gaat. De gebruiker dient zijn bank te kiezen uit de lijst van banken (ABN AMRO, Frieslandbank, ING, Rabobank, SNS Bank of overige banken) waarna hij daar met de gebruikelijke manier in dient te loggen (met wachtwoord of random reader). Vervolgens kan indien de gebruiker meerdere rekeningen heeft, de juiste betaalrekening geselecteerd worden. De overboeking dient vervolgens ondertekend te worden waarna deze uitgevoerd wordt. Optioneel kan de gebruiker ervoor kiezen om per email de gegevens van de overboeking te ontvangen. De bank bevestigt de betaling aan de gebruiker en de webwinkel doet dit vervolgens ook. Bij deze handelingen wordt heel wat informatie uitgewisseld. In figuur 3.4.5 zijn de gegevensstromen weergegeven voor het pad waarbij geen complicaties optreden. Voorvallen als incorrecte inloggegevens of te weinig saldo zijn buiten beschouwing gelaten.

Informatieprivacy speelt hierbij een grote rol aangezien er veel privacygevoelige informatie tussen de partijen heen en weer gaat. Deze informatie mag enkel gebruikt worden voor dit doel, ofwel deze betaling, en niet voor andere handelingen. Informatieprivacy is hier beschermd door in de eerste deelvraag genoemde onderdelen. Opvallend is wel dat de webwinkel alleen de betaling start en vervolgens wacht totdat dit bevestigd is. Hierdoor wordt de gegevensstroom meer afgezonderd en bewaakt. De onderlinge verbindingen zijn als volgt op te delen:

▪ Gebruiker	↔	Computer:	verantwoordelijkheid van de gebruiker
▪ Computer	↔	Webwinkel:	verantwoordelijkheid van de webwinkel
▪ Computer	↔	Bank:	verantwoordelijkheid van de bank
▪ Webwinkel	↔	Bank:	verantwoordelijkheid van de webwinkel en de bank

Hierdoor is duidelijk gesteld wie waarvoor verantwoordelijk is en dit is ook traceerbaar door de gegevens die gelogd worden. Dit loggen kan echter de inbreuk op informatieprivacy bevorderen maar daarnaast dus ook functioneel zijn voor bescherming hiervan. Op elk moment van versturen kunnen de gegevens echter incorrect gebruikt worden of in verkeerde handen vallen. In figuur 3.1.5. is uiteengezet waar de bescherming van privacy tekort kan komen, ook dat is hier het geval.



Figuur 3.4.5 “Sequence diagram iDeal”

Offline betalen

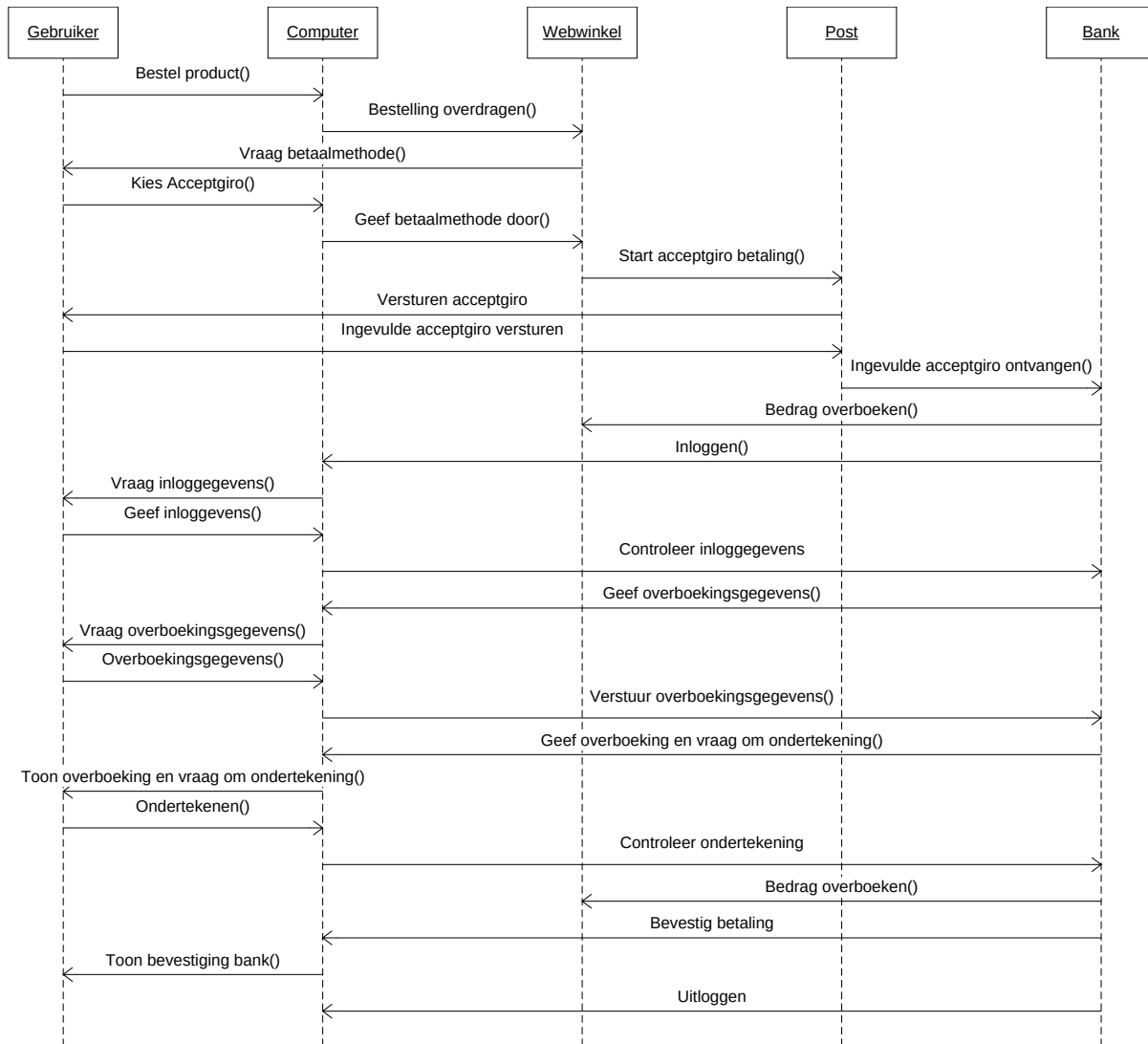
Het offline betalen vindt plaats met acceptgiro en kent geen directe online factoren. Offline privacy is dus waar het hier om draait. De gang van zaken bij een offline betaling met al haar privacy aspecten is met behulp van de UML Use Case uiteen te zetten (figuur 3.4.4) vanaf 'Acceptgiro'. Het voorgaande ('Inloggen', 'Bestel product' etc.) zijn online aspecten maar bij offline betalen gaat het om het moment vanaf waar er gekozen is voor de betaalmethode acceptgiro. Vanaf dan worden er persoonlijke gegevens verstuurd tussen gebruiker, webwinkel en de bank. Dit gebeurt via de computer of via de post.

Nadat het product besteld is en 'acceptgiro' als betalingsmethode is geselecteerd begint de uitwisseling van gegevens waar het bij offline betalen om gaat. De webwinkel stuurt hiervoor per post een acceptgiro naar de gebruiker toe. Hierop staan een aantal gegevens voorgedrukt. De gebruiker maakt dan de keuze om deze te betalen via de post of via internetbankieren. Voor de optie per post vult hij de acceptgiro kaart verder in met zijn persoonlijke gegevens en stuurt deze vervolgens naar zijn bank op. De bank verwerkt de betalingsopdracht nadat gecheckt is of het een geldige overboeking betreft en de gegevens van de gebruiker correct zijn. Voor de optie per internetbankieren logt de gebruiker via zijn computer in bij de bank, stelt de betalingsopdracht op en ondertekent deze. De bank verwerkt vervolgens de opdracht. Voor beide opties is de verdere gang van zaken gelijk. De gebruiker kan zijn rekening raadplegen om te zien dat de betaling is verwerkt. De webwinkel doet dit ook periodiek en wanneer de betaling is ontvangen wordt deze als betaald beschouwd. In figuur 3.4.6 zijn de gegevensstromen weergegeven voor het pad waarbij geen complicaties optreden. Voorvallen als incorrecte inloggegevens of te weinig saldo zijn buiten beschouwing gelaten. Wat opvalt is dat hier een extra partij is te bekennen, namelijk de 'Post'. Dit is het postbedrijf en de postbode die de acceptgiro aflevert tussen de partijen.

Informatieprivacy speelt ook hierbij een grote rol aangezien er veel privacygevoelige informatie tussen de partijen heen en weer gaat. Deze informatie mag enkel gebruikt worden voor dit doel, ofwel deze betaling, en niet voor andere handelingen. Informatieprivacy is hier tevens beschermd door in de eerste deelvraag genoemde onderdelen. Er is nu een partij meer en de onderlinge verbindingen zijn als volgt:

▪ Gebruiker	↔	Computer:	verantwoordelijkheid van de gebruiker
▪ Computer	↔	Webwinkel:	verantwoordelijkheid van de webwinkel
▪ Webwinkel	↔	Post:	verantwoordelijkheid niet geheel duidelijk
▪ Gebruiker	↔	Post:	verantwoordelijkheid niet geheel duidelijk
▪ Computer	↔	Bank:	verantwoordelijkheid van de bank
▪ Webwinkel	↔	Bank:	verantwoordelijkheid van de webwinkel en de bank
▪ Bank	↔	Post:	verantwoordelijkheid niet geheel duidelijk

Bij deze offline manier van versturen is niet altijd geheel duidelijk wie verantwoordelijk was aangezien niet te traceren is welke partij op welk moment de informatie in handen heeft. Wel is er aan de andere kant meer controle aangezien een deel nu offline en dus fysiek plaatsvindt en online bedreigingen deels weggenomen zijn. Massa verwerking van data is dus minder aan de orde dan bij online.



Figuur 3.4.6 “Sequence diagram Acceptgiro (Bij “Inloggen()” start de keuze voor internetbankieren)”

Het blijkt dat zowel online als offline betalen haar voor en nadelen heeft. In beide gevallen gaat er in ieder geval veel informatie over en weer welke idealiter beschermd zou moeten zijn. De uiteenzetting in figuur 3.3.2. blijkt van toepassing. Opvallend punt is nu al dat het vertrouwen in de acceptgirokaart boven iDeal vooral gebaseerd is op het gevoel en niet op feiten qua verantwoordelijkheid van de partijen. Daarom is het vooral aan de gebruiker en zijn perceptie om te bepalen wat in welk geval, en wat voor hemzelf, de meest veilige en optimale betaalmethode is. In het volgende hoofdstuk ‘Privacy in de praktijk’ zal een vooronderzoek gedaan worden naar de perceptie van de gekozen doelgroep naar online en offline privacy.

4. PRIVACY IN DE PRAKTIJK

In het vorige hoofdstuk is privacy in theoretische vorm aan bod gekomen. Nu volgt de praktijk om te onderzoeken in welke mate de doelgroep, bestaande uit studenten, zich bewust is van zijn of haar privacy en hoe zij zich ten opzichte hiervan gedragen. Vervolgens zullen de gegevens uit de praktijk in de volgende hoofdstukken vergeleken worden met de theorie. Om de benodigde gegevens te verkrijgen zal eerst een situatieschets gegeven worden om de wijze van ondervraging duidelijk te maken en hoe de gegevens geïnterpreteerd worden.

Situatieschets enquête

Voor het proces van deze kwantitatieve onderzoeksmethode zal de theorie gebruikt worden die hiervoor is beschreven. Naar Bryman (2008) (16) zijn op basis hiervan hypotheses en vervolgens stellingen te formuleren. De concepten hiervan worden uitgewerkt. De onderzoeksplaats is Nederland en de onderzoeksrespondenten zijn Nederlands sprekende studenten in de leeftijd van 18 tot en met 25 jaar. Het gekozen onderzoeksinstrument is een enquête. De hiermee verkregen resultaten worden verwerkt en geanalyseerd en er worden conclusies aan verbonden. Deze worden vergeleken met de theorie en uiteindelijk uitgeschreven.

De enquête (zie appendix “Enquête: Online & offline privacy”) is opgesteld om een vooronderzoek te doen naar perceptie van studenten van privacy, en dan specifiek gericht op *online* en *offline* privacy. Er zullen algemene vragen in naar voren komen maar vooral stellingen. De gekozen doelgroep is studenten. Redenen hiervoor zijn dat zij zowel kennis van online als offline handelingen zouden moeten hebben, goed bereikbaar zijn en daarnaast zichzelf veelal goed kunnen uitdrukken. De vragen in de enquête zijn terug te herleiden op de theorie zoals in het voorgaande hoofdstuk. Allereerst is er een deel waarbij gegevens van de persoon gevraagd worden, te weten leeftijd, opleiding en opleidingssoort. Vervolgens is er een deel waarbij privacy in het algemeen aan bod komt. Na deze negen stellingen volgen een aantal stellingen met betrekking tot eerst online privacy en dan offline privacy. Gecombineerd hierbij zijn er vergelijkingen tussen online en offline privacy. Enkele meerkeuzevragen bieden vervolgens ondersteuning hierbij of zullen nieuwe inzichten geven. Tot slot wordt om een algemeen oordeel gevraagd, of de enquête liever offline ingevuld was en als laatste een vraag om het e-mailadres invullen. Dit is natuurlijk interessant aangezien het de vraag is of de geënquêteerden dit doen na een vragenlijst over privacy.

Dit onderzoek kan gezien worden als een vooronderzoek om inzicht te krijgen in welke mate studenten zich bewust zijn van hun privacy en hoe zij zich ten opzichte hiervan gedragen. Het verschil in online en offline privacy zal hier tevens in naar voren komen. Om een representatief beeld te krijgen is er een minimum aantal benodigde respondenten nodig. Hoeveel dit is, is onder meer afhankelijk van tijd en bereidheid van de doelgroep. Daarnaast zijn er verschillende soorten studenten, te kenmerken aan de hand van opleiding en bijbehorend opleidingsniveau.

Het aantal benodigde respondenten is te bepalen aan de hand van een formule (gebaseerd op statistiek):

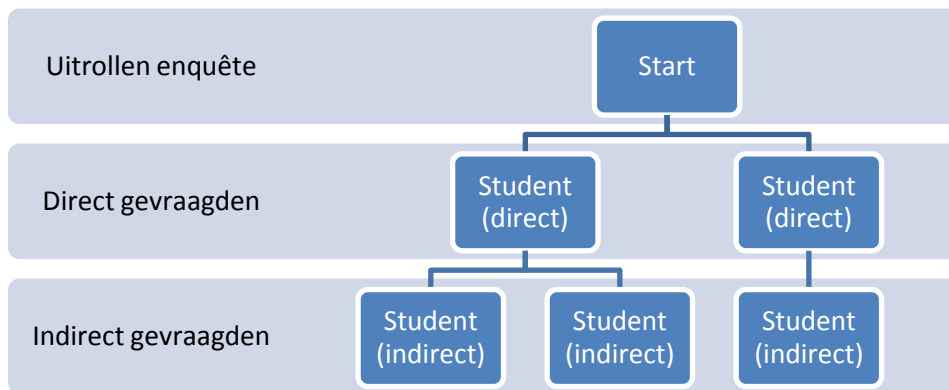
$$\text{benodigd aantal studenten} = \frac{\text{grootte populatie} \times \text{standaardafwijking}^2 \times \text{kans bepaald antwoord} \times (1 - \text{kans bepaald antwoord})}{\text{standaardafwijking}^2 \times \text{kans bepaald antwoord} \times (1 - \text{kans bepaald antwoord}) + (\text{grootte populatie} - 1) \times \text{foutmarge}^2}$$

De grootte van de populatie is in dit geval onbekend groot maar wel eindig. Vanaf populatie grootte 20000 is de verandering nihil waardoor dit getal gebruikt zal gaan worden. Door middel van statistiek blijkt dat de standaardafwijking 1,96 is aangezien een betrouwbaarheid van 95 procent gebruikt wordt. De kans op een bepaald antwoord is vooraf niet aan de hand van een hypothese te noemen, daarom is dit 0,5. Tot slot is er nog de foutmarge welke de bepalende rol zal gaan spelen. Aangezien dit een vooronderzoek betreft en binnen de scope van deze scriptie moet passen is gekozen voor een foutmarge van 0,10. Invullen van de formule geeft:

$$\frac{20000 \times 1,96^2 \times 0,50 \times (1 - 0,50)}{1,96^2 \times 0,50 \times (1 - 0,50) + (20000 - 1) \times 0,10^2}$$

Benodigd aantal studenten $\approx 95,95 = \underline{\underline{96}}$

Om een correcte steekproef te selecteren is diversiteit van belang. Studenten van verschillende opleidingen kijken immers op andere wijze tegen privacy aan. Vandaar dat de enquête dusdanig verspreid wordt dat deze groepen, te verdelen naar opleidingssoort, een gelijke kans krijgen om deze in te vullen. Daarnaast is aan de studenten gevraagd om de enquête aan anderen door te geven. Hierdoor ontstaat een aselechte steekproef welke gerealiseerd is door middel van de ‘snowballing-techniek’, weergegeven in figuur 4.1.1. De verscheidenheid wordt op deze wijze divers en dus niet select.



Figuur 4.1.1 “Snowballing-techniek voor uitrollen van de enquête”

De verspreiding van de vragenlijst geschiedde via het internet (via ThesisTools (17)). Reden hiervoor is dat elke student daardoor op dezelfde wijze gemakkelijk te bereiken is. Hierdoor is er in zekere zin een voorkeur voor online gecreëerd. Door de verscheidenheid aan studenten en enkele vragen die dit controleren is dit echter als dusdanig klein te beschouwen dat hier geen daadwerkelijke aanpassing voor nodig is. In dit vooronderzoek wordt dit dan ook achterwege gelaten.

Voor de analyse van de data zijn er verschillende soorten variabelen. Zo is de leeftijd een numerieke variabele, opleiding en opleidingsniveau zijn beschrijvend net als de open vragen aan het einde van de enquête. De data verkregen met de stellingen is tevens numeriek waarbij 1=geheel oneens, 2=oneens, 3=deels oneens, 4=neutraal, 5=deels eens, 6=eens, 7=geheel eens. De gedetailleerde resultaten zijn te vinden in de appendix “Verzamelde gegevens”). Hieronder volgt het eerste resultaat van de enquête.

Resultaat

Uiteindelijk is het aantal studenten dat bereid was gevonden om de enquête in te vullen 138. De foutmarge is daarom neergekomen op iets minder dan negen procent. De “response rate” (16) is uitgekomen op ongeveer zeventig procent. Er waren immers 201 ingevulde enquêtes waarvan er 138 bruikbaar waren. De overigen hadden namelijk de vragenlijst niet volledig doorlopen of waren niet daadwerkelijk student. In figuur 4.1.2 zijn de algemene gegevens van de studenten weergegeven.

Totaal aantal enquêtes:	138
Correcte response rate:	Bijna 70 %
Leeftijden van de studenten:	18-25 jaar
Aantal verschillende opleidingen:	45 opleidingen
Opleidingsniveaus:	Voornamelijk WO (127), ook HBO (11)

Figuur 4.1.2 “Gegevens van de studenten”

Het aantal uiteindelijk bruikbare enquêtes ligt dus hoger dan het benodigde minimum aantal studenten wat de nauwkeurigheid vergroot. Wat opvalt is dat slechts drie mensen aangaven de enquête offline willen invullen, elf hadden geen mening en de rest (124 personen) had er geen problemen mee dat dit online gebeurde. Een duidelijke reden hiervoor was er niet. De volgende twee deelvragen geven aan in welke mate studenten zich bewust zijn van hun privacy en hoe zij zich hier ten opzichte van gedragen. Hierin komen de specifieke resultaten ook aan bod.

Deelvraag 4: In welke mate is de doelgroep zich bewust van zijn privacy?

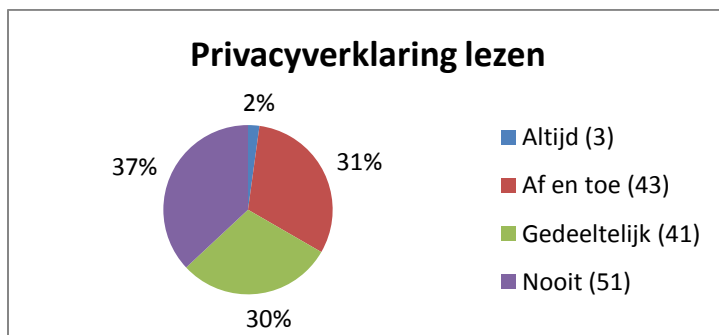
In het voorgaande is informatieprivacy uitvoerig aan bod gekomen. Om te onderzoeken of dit strookt met de resultaten die verkregen zijn met de enquête zal dit vergeleken worden. Om te bepalen of studenten zich bewust zijn van hun privacy zijn een aantal specifiek hieraan gerelateerde vragen opgenomen in de enquête. De gegevens dienen geïnterpreteerd te worden aan de hand van de volgende schaal (indien het laagste gekozen antwoord niet 1 is en hoogste niet 7 dan is dit vermeld bij de resultaten):

1	Geheel oneens
2	Oneens
3	Deels oneens
4	Neutraal
5	Deels eens
6	Eens
7	Geheel eens

De meest directe vraag is de eerste: “Ik ben mij er bewust van wat privacy inhoudt”. Het resultaat (gemiddelden en de standaarddeviatie zijn op twee decimalen afgerond) hiervan is als volgt:

	Gemiddelde	Standaarddeviatie	Laagste	Hoogste
▪ Ik ben mij er bewust van wat privacy inhoudt	5,92	0,86	2	7

Hieruit blijkt dat de verscheidenheid niet heel groot is aangezien de standaarddeviatie relatief laag is. Het gemiddelde ligt wel hoog namelijk $5,92 \approx 6$ en staat gelijk aan ‘eens’. Dit ondersteunt het feit dat opvattingen over privacy uiteenlopen maar over het algemeen wel van zichzelf gedacht wordt er bewust van te zijn. Ondanks dat tegenwoordig bijna alles met betrekking tot informatieprivacy vastgelegd wordt in een privacyverklaring/disclaimer lezen slechts drie studenten van de 139 ondervraagden deze altijd en grootste deel nooit (zie figuur 4.2.1).



Figuur 4.2.1 “Lezen van de privacyverklaring”

Voorgaande maakt de vraag interessanter in hoeverre studenten daadwerkelijk bewust zijn van hun privacy. Uit de gegevens blijkt namelijk ook dat 16 personen dagelijks aan hun privacybescherming denken, 40 wekelijks, 44 maandelijks en 38 (bijna) nooit. Dat dit relatief laag is ten opzichte van het aantal momenten op een dag dat zij er mee te maken hebben, denk aan gebruik van de ov-chipkaart, social media en dergelijke, is te verklaren aan de hand van twee redenen. Ten eerste omdat sommige handelingen dusdanig gewoon zijn geworden dat er gewenning optreedt. Ten tweede omdat sommige dingen simpelweg opgedrongen zijn en deze niet veranderd kunnen worden, ze leggen zich er dan bij neer. Een tweetal stellingen uit de enquête geeft daarnaast de volgende inzichten:

	Gemiddelde	Standaarddeviatie	Laagste	Hoogste
▪ Ik wil graag altijd weten welke gegevens van mij bij een organisatie bekend zijn en wat daar mee gebeurt	5,06	1,47	1	7
▪ Wanneer blijkt dat een organisatie niet zorgvuldig omgaat met mijn gegevens verlies ik mijn vertrouwen	5,91	1,15	2	7

Over het algemeen wil het grootste deel dus wel weten wat er met zijn of haar gegevens gebeurt en welke gegevens er bekend zijn. Bijna elke student zegt ook zijn vertrouwen te verliezen wanneer de omgang niet zorgvuldig verloopt. Dit komt overeen met de theorie van Koehn (12) en de punten waar een andere partij aan moet voldoen. Vertrouwen is namelijk gebaseerd op de reputatie en doel van de andere partij en de student. De leercyclus van Kolb (15) komt ook naar voren. Bij een slechte ervaring verliest de student namelijk zijn vertrouwen en begint deze cyclus, welke eerst al (deels) doorlopen is, weer van voor af aan.

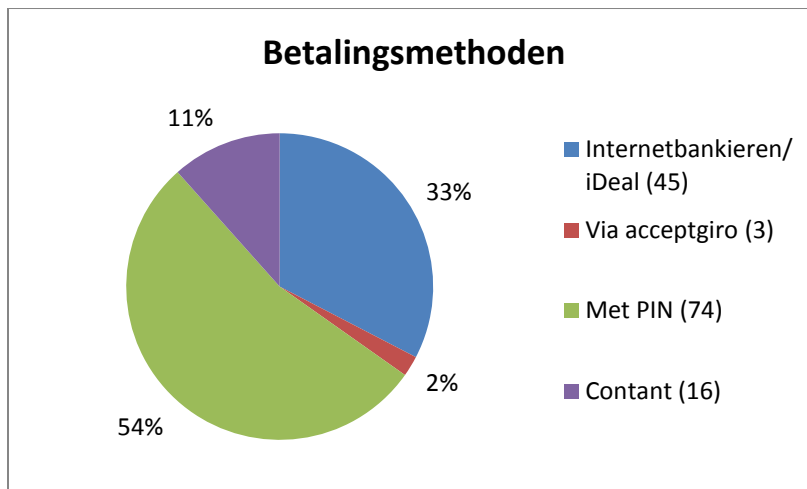
Het blijkt dat de studenten ook een verschillende perceptie van privacy hebben in de online en offline wereld, zij gaan met beiden verschillend om. De enquête vroeg voor een aantal stellingen vanaf beide zijden, zowel vanuit de offline kant als de online kant, naar het beeld wat de studenten hierbij hebben.

	Gemiddelde	Standaarddeviatie
▪ Online heb ik meer grip op het verstrekken van mijn gegevens dan offline	3,06	1,41
▪ Bij online handelingen voel ik mij anoniemer dan bij offline handelingen	4,43	1,33
▪ Ik denk dat mijn gegevens online gemakkelijker verkeerd gebruikt worden dan offline	5,50	1,26
▪ Mijn gegevens worden op social media (Facebook, Twitter etc.) gebruikt door andere (ongewenste) partijen voor marketing doeleinden	4,88	1,67
▪ Wanneer ik online betaal met iDeal acht ik dit minstens net zo vertrouwd als wanneer ik offline betaal met een acceptgiro	5,42	1,51

Wat gelijk opvalt is dat de ondervraagden gemiddeld een 3 (= deels oneens) toekennen aan de stelling of zij online meer grip hebben op het verstrekken van hun gegevens dan offline. Online is er dus een gevoel van minder controle. Daarentegen voelen zij zich iets meer dan neutraal anoniemer bij online handelingen dan offline handelingen. Dit komt overeen met de eerdere theorie aangezien online een groter gevoel van anonimiteit gecreëerd zou moeten zijn.

Wel hebben de ondervraagde studenten het idee dat hun gegevens online gemakkelijker verkeerd gebruikt worden. Over het geheel gezien geven zij dit gemiddeld een 5,5 wat precies tussen 'deels eens' en 'eens' in ligt. Overeenstemming met de theorie is hier aanwezig aangezien ondersteunt wordt dat online gemakkelijker gegevens verkeerd gebruikt kunnen worden, hierbij is ook de '2P2Q hypothese' van belang. Opvallend is dat maar weinig (4,88 ligt tussen neutraal en 'deels eens') maar wel met een grote standaarddeviatie, denken dat hun gegevens op social media gebruikt worden door andere partijen voor marketing doeleinden. Dit is namelijk iets wat op grote schaal plaatsvindt en de gebruiker via de privacyverklaring (welke weinig gelezen wordt) ook toestemming voor heeft gegeven. De gegevens bij deze twee stellingen spreken elkaar dus enigszins tegen.

Online betalen met iDeal wordt minstens net zo veilig beschouwd als offline betalen met een acceptgiro. De ondervraagden kozen voor de volgende betaalmethoden op de vraag welke zij het liefst gebruiken (figuur 4.2.2):



Figuur 4.2.2 "Welke betaalmethoden worden het liefst gebruikt"

Contant wordt nog maar beperkt gekozen en op de acceptgiro valt de keuze al helemaal weinig. Het liefst kiest de student voor betaling via PIN en daaropvolgende via internetbankieren/iDeal. Een verklaring hiervoor kan zijn dat gezien de leeftijd van de ondervraagden zij met de pinpas en later internetbankieren/iDeal zijn opgegroeid en er gewenning is opgetreden. Dit komt overeen met de ontwikkeling weergegeven in figuur 3.4.2.

Bij het bewust zijn van privacy speelt de bescherming hiervan ook een belangrijke rol. In het theoretische deel is privacybescherming uitvoerig aan de orde gekomen. Of het gevoel (de perceptie) van de studenten hiermee overeen komt is af te leiden uit de volgende resultaten:

	Gemiddelde	Standaarddeviatie
▪ De Nederlandse wet voorziet in mijn ogen goed in de bescherming van mijn informatieprivacy (zowel online als offline)	3,96	1,42
▪ Ik heb er geen probleem mee als mijn gegevens gebruikt/bekeken worden ten bate van de (nationale) veiligheid	4,38	1,75
▪ Organisaties (telecomprovider, bank etc.) gaan vertrouwd met mijn gegevens om door toezicht van overheid en het College Bescherming Persoonsgegevens	4,20	1,43
▪ Ik ben mij ervan bewust dat er altijd iemand mee kan kijken bij verzending van gegevens, zowel online per internet als offline per post	4,71	1,54
▪ Online wordt veel gelogd (alles wordt bijgehouden) waardoor illegale handelingen makkelijker zijn op te sporen, dit geeft mij een veilig gevoel	3,49	1,36
▪ De technologie beschermt mijn privacy beter dan de wetgeving	3,46	1,40
▪ De mens is een zwakkere schakel dan technologie bij bescherming van informatieprivacy	4,99	1,36
▪ Bij een offline handeling (bijv. betalen) denk ik altijd aan mijn privacybescherming	3,90	1,83
▪ Ik denk dat wetgeving online en offline uit dezelfde onderdelen bestaan	2,99	1,31

Studenten denken niet positief en niet negatief over de vraag of de Nederlandse wet voorziet in de bescherming van hun informatieprivacy. In het kader van wetgeving bleek dat opsporingsdiensten wel inzage hebben mits hiervoor een goede reden is. Ongeveer de helft heeft van de ondervraagden heeft er niet zozeer een probleem mee wanneer dit gebeurt. Wel zijn de meningen erg verdeeld, deze lopen immers van 'geheel oneens' tot aan 'geheel eens'. Vertrouwen in organisaties is neutraal qua het vertrouwd omgaan met gegevens. Dergelijke organisaties spelen echter wel in op de eigenschappen, zoals in de theorie naar voren is gekomen, om vertrouwen op te bouwen en te handhaven. Het gaat dus niet altijd op dat de gebruiker dit zo ziet. Hetzelfde niveau is te herkennen bij de vraag of de student zich bewust is dat er altijd iemand mee kan kijken.

Online wordt er veel gelogd en is verantwoordelijkheid van partijen makkelijker te traceren (zie ook case: online en offline betalen). Gemiddeld zien de studenten dit niet als iets wat een veilig gevoel geeft. Opsporingsdiensten en organisaties voeren dit echter wel als zodanig aan en dus verschilt de perceptie hierin. Aanvullend hierbij denkt de doelgroep dat de technologie de privacy niet beter beschermd dan de wetgeving. Het algehele vertrouwen in de technologie ligt dus tussen 'deels oneens' en 'neutraal'. Gemiddeld gezien is er gekozen voor 'deels eens' bij de stelling dat de mens een zwakkere schakel is dan technologie bij de bescherming van informatieprivacy. Uit de theorie bleek dat de bescherming inderdaad staat of valt door het gedrag van de mens. Al met al is te stellen dat de studenten wel

vertrouwen hebben maar dit gevoel voor bescherming niet direct terug te leiden is op één of meerdere van de drie factoren (zie figuur 3.1.5). Wel zien zij een verschil tussen online en offline. Zo wordt er offline door de meesten iets minder aan privacy gedacht (wel een hoge standaarddeviatie) en met het onderwerp of wetgeving online en offline uit dezelfde onderdelen bestaan zijn zij het 'deels oneens'. De basis van wetgeving is gezien de theorie hetzelfde maar voor beiden zijn inderdaad specifieke onderdelen opgesteld. Voor de offline wereld zijn deze duidelijker dan voor de 'nieuwere' online wereld.

Ondanks dat het gros van de ondervraagde studenten aangeeft zich bewust te zijn van hun privacy blijkt dit uit de gegeven antwoorden niet altijd zo te zijn. Veel aspecten zijn vanwege veelal gewenning niet meer interessant om bij na te denken en er is dan ook weinig bewustwording. Informatieprivacy staat echter wel redelijk hoog in het vaandel maar alleen wanneer dit niet aanzienlijk meer moeite kost of voor minder gemak zorgt. Wat opvalt is dat er vanaf het begin een vrij hoog niveau van vertrouwen is en dat verwacht wordt dat alles correct zal verlopen. Hier tegenover staat dat wanneer naar de bescherming gevraagd wordt niet duidelijk aan te geven is waarop het veilige gevoel gebaseerd is. Ook handelen zij online anders dan offline terwijl hetzelfde principe hier de overhand heeft, naar de theorie zou dit rationeel gelijk moeten zijn maar gevoel (en ethiek) hebben dus de overhand.

De doelgroep is zich dus wel degelijk bewust van privacy maar dit is zeer situatiespecifiek en dit is niet gebaseerd op een specifieke soort van bescherming. De volgende deelvraag geeft meer inzicht hoe de student zich ten opzichte van dit niveau qua bewustzijn gedraagt ten aanzien van zijn privacy.

Deelvraag 5: Hoe gedraagt de doelgroep zich ten opzichte van zijn privacy?

Omgang met privacy en de perceptie daarvan is afhankelijk van het bewustzijn hiervan maar ook van het gedrag van de doelgroep. Om te bepalen of studenten zich op een bepaalde wijze gedragen ten opzichte van hun privacy zijn ook hiervoor een aantal specifiek hieraan gerelateerde vragen opgenomen in de enquête. De meest opmerkelijke vraag om hun gedrag aan te tonen is misschien wel de allerlaatste vraag van de enquête:

	E-mailadres ingevuld	E-mailadres <i>niet</i> ingevuld
Bedankt voor je medewerking! Mocht je geïnteresseerd zijn in het eindresultaat, geef dan hier je e-mailadres op:	35 (25,36 %)	103 (74,64 %)

Ondanks dat deze vraag voor velen bij de enquête (na afloop) leek te behoren was het interessant om te bepalen hoeveel studenten na een enquête specifiek over privacy nog hun e-mailadres in zouden vullen. Uiteindelijk bleken 35 studenten (25,36 procent), ofwel één op de vier studenten dit te doen. Dus of ze hechten niet veel waarde aan de bescherming van hun e-mailadres, hebben een tijdelijk account alhoewel dit gebaseerd op de naamgeving zeer onwaarschijnlijk is of zijn zich er niet van bewust deze gegevens op deze wijze prijs te geven. Een oorzaak kan ook blijken uit de volgende stellingen:

	Gemiddelde	Standaarddeviatie	Laagste	Hoogste
▪ Via email/websites verstrek ik mijn gegevens eerder dan aan een echt persoon	3,21	1,40	1	6
▪ Ik verstrek mijn gegevens alleen indien dit noodzakelijk is	5,46	1,25	2	7

De ondervraagden zijn het dus deels oneens met de stelling dat zij gegevens eerder verstrekken via email/websites (online) dan aan een echt persoon (offline). Voor het grootste deel van de ondervraagden strookt dit ook met het feit dat één op de vier studenten hun e-mailadres aan het einde van de enquête (op een website) invulden. De verdeling ligt ook dicht bij elkaar aangezien 7 (= 'geheel eens') niet is gekozen. Dit is waarschijnlijk gebaseerd op vertrouwen en interesse want een hoge waarde (5,46) is te zien op de stelling 'Ik verstrek mijn gegevens alleen indien dit noodzakelijk is'. Dit komt overeen met de theorie dat alleen wanneer dit noodzakelijk is, en de gebruiker dus een doel ziet, hij zijn gegevens verstrekt.

Privacy en gedrag gaan dus samen maar zijn gebaseerd op gevoel en ethiek van de gebruiker. De mate van bewustzijn uit de vorige deelvraag conflicteert met de volgende twee stellingen:

	Gemiddelde	Standaarddeviatie	Laagste	Hoogste
▪ Ik ben bereid meer moeite voor iets te doen als ik dan minder persoonlijke gegevens hoeft af te staan	4,97	1,36	1	7
▪ Ik ben bereid meer gegevens te verstrekken als ik daar voordelen mee krijg	4,38	1,21	1	6

Dit tweetal stellingen spreken elkaar onderling ook deels tegen. Het bleek namelijk dat studenten zich bewust zijn van hun privacy maar dit zeer situatiespecifiek is. Vooral gemak staat in veel gevallen hoger in het vaandel. Uit deze stelling blijkt echter dat studenten met een niveau van 'deels eens' meer moeite willen doen om zo minder gegevens af te hoeven staan. Dit terwijl moeite en gemak tegenstrijdig aan elkaar zijn. Opvallend is dat de stelling 'Ik ben bereid meer gegevens te verstrekken als ik daar voordelen mee krijg' dan relatief laag is beoordeeld met een 4,38. Dit geeft aan dat het gedrag in dit geval niet op rationaliteit gebaseerd is. Dit kan ook samen hangen met het feit dat de student snel vertrouwen heeft totdat het tegendeel bewezen is en het vertrouwen geheel verdwijnt.

Dat het gedrag niet altijd overeen komt met het bewustzijn blijkt ook uit de volgende serie stellingen:

	Gemiddelde	Standaarddeviatie
▪ Bij online handelingen denk ik meer na over verstrekking van mijn gegevens dan bij offline handelingen	4,50	1,59
▪ Online kijk ik altijd naar de reputatie van de andere partij voordat ik gegevens verstrek	4,43	1,54
▪ Bij een online handeling (bijv. betalen) denk ik altijd aan mijn privacybescherming	5,07	1,33
▪ Ik ben bereid online meer gegevens af te staan wanneer ik de organisatie offline ook ken	5,30	1,19
▪ Offline zal ik meer gegevens verstrekken wanneer ik het bedrijf ook online ken	3,87	1,45
▪ Als een organisatie mijn vertrouwen online heeft gewonnen dan vertrouw ik deze ook offline	4,73	1,23

Online en offline wordt in sommige gevallen gezien als iets geheel anders maar soms ook als gelijken. Dit komt overeen met de theorie waaruit al bleek dat de grens steeds minder expliciet is (figuur 3.1.1). Er wordt dan ook neutraal gedacht over de stelling of de student bij online handelingen meer nadenkt over verstrekking van zijn gegevens dan bij offline handelingen. Zoals al bleek is online vertrouwen snel gecreëerd totdat het tegendeel blijkt. Er wordt dan ook niet altijd gekeken naar de reputatie van de andere partij voordat online gegevens verstrekt worden. Aan privacybescherming wordt met iets meer dan 'deels eens' wel gedacht. Het bewustzijn en het gedrag zijn dus niet geheel in overeenstemming wat theoretisch gezien ook realistisch is.

Het vertrouwen wordt daarnaast wel aanzienlijk versterkt omdat er meer bereidheid is om online gegevens af te staan wanneer de organisatie (de andere partij) ook offline bekend is. Op basis van de

soorten vertrouwen (12) is te stellen dat dit een calculerend vertrouwen is, wat is, of kan doorgroeien naar kennis-gebaseerd vertrouwen. Het online gevoel van anonimiteit (7) wordt op deze wijze bij de andere partij weggenomen. Andersom gezien is dit een stuk minder wat blijkt uit de laatste twee van bovenstaande stellingen. De basis dient offline gelegd te worden alvorens online echt op feiten gebaseerd vertrouwen te wekken. Van online naar offline is een stuk minder gemakkelijk.

	Gemiddelde	Standaarddeviatie	Laagste	Hoogste
▪ Ik bestel online producten net zo makkelijk als dat ik producten in de winkel koop	4,22	1,88	1	7
▪ Ik ben bereid een kleine vergoeding te betalen om offline(contant/acceptgiro) te kunnen betalen in plaats van op een online manier	2,27	1,31	1	6

Het neutrale resultaat en de hoge standaarddeviatie op de vraag of producten online net zo gemakkelijk in de winkel worden gekocht bevestigt de online drempel niet. Reden hiervoor is dat de ondervraagde generatie, zo bleek ook al eerder, gewend is aan het online tijdperk en niet meer anders kent. Meer betalen voor een betaling op een offline manier (contant/acceptgiro) dan online te moeten betalen is er dan ook niet meer bij. Met een duidelijke 2,27 en relatief lage standaarddeviatie komt dit bijna neer op 'oneens'. Met een lichte neiging naar 'deels eens' bevestigt de volgende stelling dit ook:

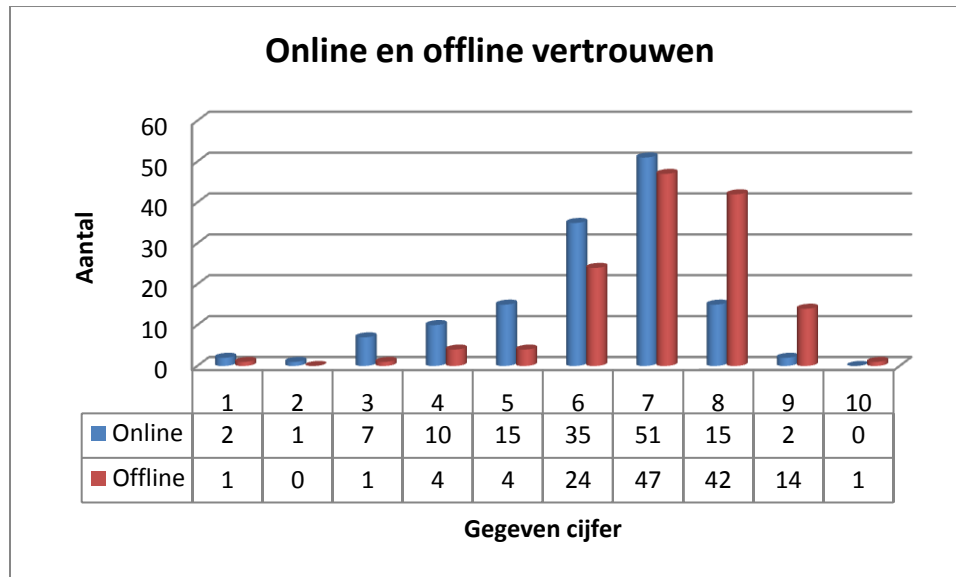
	Gemiddelde	Standaarddeviatie
▪ Ik vind het belangrijk om te kunnen kiezen of ik een handeling online of offline uitvoer	4,86	1,42

Of een handeling online of offline gebeurd is dus gebaseerd op gevoel en gemak in plaats van een bewuste keuze. In sommige gevallen is er een duidelijk verschil tussen online en offline privacy. Twee vragen in de enquête vroegen expliciet naar een cijfer tussen de 1 en 10 waarbij 1=zeer slecht en 10=zeer goed. Het resultaat is als volgt:

	Gemiddeld cijfer
▪ Bij verstrekking van mijn gegevens <i>online</i> geef ik mijn vertrouwen hierin een:	6,12
▪ Bij verstrekking van mijn gegevens <i>offline</i> geef ik mijn vertrouwen hierin een:	7,14

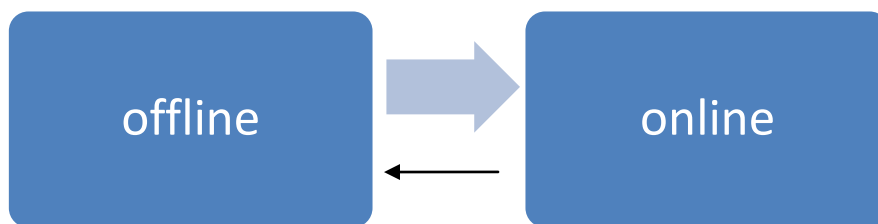
Wat gelijk opvalt is dat het gemiddelde gegeven cijfer door de studenten bij offline (7,14 met standaarddeviatie 1,30) ruim een punt hoger ligt dan bij online (6,12 met standaarddeviatie 1,51). Dit komt overeen met de theorie waarin beweerd werd dat men offline het gevoel heeft van betere controle en dus meer vertrouwen om gegevens te verstrekken. In figuur 4.3.1 is weergegeven hoe de spreiding van waardering tot stand is gekomen. Er is een duidelijk overgang te zien na het cijfer 7. Voor 1

tot en met 6 (de lagere waarderingen) krijgt online een hoger aantal toekenningen. Bij de 7 is het aantal bijna gelijk en vanaf 8 tot en met 10 ligt de waardering voor offline vertrouwen beduidend hoger.



Figuur 4.3.1 “Vertrouwen in het verstrekken van gegevens, zowel online als offline”

Al met al is dus te stellen dat de student zich qua gedrag laat leiden door wat op dat moment het gemakkelijkste is maar wel met enige argwaan. De argwaan is echter snel weggenomen maar wordt daarentegen enorm versterkt als er ook maar iets mis gaat. Het gedrag wordt daar direct op aangepast. Het gedrag offline is wel stabiel en dit sluit aan bij de theorie. Daaruit (13) bleek dat bij online de andere partij gezien wordt als een technologie en dus niet gelijk tastbaar (abstract) is en bij offline als een persoon of organisatie (concreter). Ook zou volgens de theorie de perceptie voor offline privacy kunnen voortvloeien uit die van online privacy. Ondanks dat dit weinig gebeurt is te stellen dat vooral de offline perceptie invloed uitoefent op de online perceptie, zo bleek uit de voorgaande enquêteresultaten. Dit is schematisch weergegeven in figuur 4.3.2.



Figuur 4.3.2 “Beïnvloeding van perceptie; veel van offline naar online en in geringe mate van online naar offline”

5. ONLINE EN OFFLINE PRIVACY

In de theoretische fase en in de praktijkfase is een brede uiteenzetting gegeven van informatieprivacy. Hierbij werd aandachtig gekeken naar online privacy, offline privacy en de verschillen daartussen. Er waren zowel aspecten uit de theorie en de praktijk die bij elkaar aansloten maar ook waren er tegenstrijdigheden. In dit hoofdstuk zal de eerder geformuleerde hoofdvraag beantwoord worden:

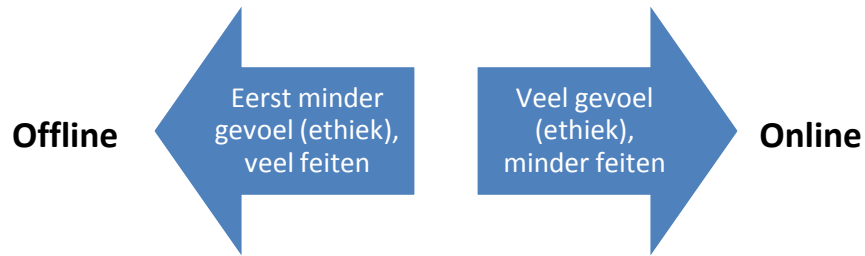
“Welke perceptie hebben studenten bij online privacy en welke bij offline privacy, welke verschillen zijn er en hoe zijn deze te verklaren?”

Een groot aantal factoren speelt hier een rol bij, het is erg situatiespecifiek en tevens persoonlijk. De ondervraagden zijn bezig met hun privacy en geven te kennen hier ook regelmatig over na te denken en stil bij te staan. Sterke kanttekening hierbij is wel dat het niet teveel tijd en moeite mag kosten. Zowel online als offline zijn er kenmerken aan te wijzen, soms komen deze overeen soms geheel niet.

Studenten zien online privacy iets als wat belangrijk is mits het niet in de weg staat van gemak en uit te voeren handelingen. Daarnaast blijkt dat hun perceptie hiervan niet erg concreet is en sterk gebaseerd is op gevoel. De ondervraagden zijn zich er dus bewust van en geven aan er over na te denken maar gedragen zich niet overeenkomstig met dit beeld. Zij gaan er vrij snel vanuit dat alles veilig is en goed verloopt totdat blijkt dat het niet zo is. Online bereiken zij snel een hoger niveau van vertrouwen maar waarop dit gebaseerd is, is niet duidelijk aan te geven. Hiervoor is geen basis vanuit technologische of sociale beveiliging en ook de wet is volgens hen niet altijd toereikend. Theoretisch gezien zou perceptie en gedrag overeen moeten komen wat in de praktijk dus anders blijkt te zijn. Reden hiervoor is dat de generatie studenten opgegroeid is met de online wereld welke steeds meer invloed krijgt. Zij kunnen blijven meegroeien en hebben dan wellicht stappen over geslagen in de perceptievorming zoals deze in de theorie naar voren is gekomen.

Bij offline privacy ligt het anders. Studenten hanteren hierbij strengere eisen voor wat betreft hun informatieprivacy. Ook hier heeft het gevoel sterk de overhand voor de gevormde perceptie maar wordt er meer nagedacht over het handelen. Een offline partij wordt gezien als betrouwbaarder maar er is meer voor nodig om een hoger niveau van vertrouwen te bereiken. Eenmaal hierop aangekomen is het lastig om dit vertrouwen te verliezen. Het is te stellen dat gevoel hier minder de overhand heeft dan bij online privacy. Offline privacy lijkt hoger in het vaandel te staan en een constructievere eigenschap te hebben. Uit het onderzoek blijkt ook dat het vertrouwen in offline privacy gewaardeerd werd met een 7,14 en in offline privacy met een 6,12. Met de gegevens wordt in de perceptie van de ondervraagden dus vertrouwd om gegaan.

Er zijn dus verschillen tussen de perceptie bij online privacy en offline privacy. Vooral datgene waarop het vertrouwen gebaseerd is verschilt (figuur 5.1.1).



Figuur 5.1.1 “Beïnvloeding van perceptie; offline veel op feiten en minder gevoel; online veel op gevoel en minder op feiten”

Het blijkt dat de perceptie verschilt op basis van hoe dit ontstaat. Perceptie is namelijk voor een groot deel gebaseerd op vertrouwen maar online is dit minder gebaseerd op feiten en meer op gevoel. Dit is te verklaren aan de hand van gewenning binnen deze leeftijdsgroep. Offline is er eerst minder gevoel (later aanzienlijk meer) en is het meer gebaseerd op feiten. Dit is niet overeenkomstig met de theorie. Daarin komt naar voren dat online privacy een gewenningsperiode kent omdat het relatief nieuw is en eerst minder vertrouwd. Offline privacy zou daarentegen eerder een vertrouwd gevoel moeten geven uit ervaringen.

De studenten bevestigen met hun antwoorden wel dat bij online privacy zij het als techniek zien en bij offline meer als een persoon. Ook blijkt dat zij meer controle denken te hebben bij offline privacy dan bij online privacy. Tevens zien zij het online altijd beschikbaar zijn als voordeel ten opzichte van de beperkte beschikbaarheid in de offline wereld.

De perceptie van studenten bij online en offline privacy kan weergegeven worden aan de hand van een tijdslijn. Hierin zijn meerdere fases te onderscheiden. De tijdsduur van een fase is online en offline verschillend en relatief. De verschillen kunnen, uitzonderingen daargelaten, als volgt uiteengezet worden:

	Offline	Online
Fase 1	Kennismaking met offline situatie	Kennismaking met online situatie
Fase 2	Situatie beoordelen en afwegen	Snel vertrouwen opgebouwd
Fase 3	Voorzichtig gebruik op basis van feiten en deels gevoel, vertrouwen ontstaat geleidelijk	Gebruik op basis van goed gevoel, hoog niveau van vertrouwen is snel ontstaan
Fase 4	Volledig gebruiken en vertrouwen op gemiddeld niveau	Blijvend gebruiken zonder daadwerkelijk bewustzijn en gemak wordt belangrijker dan informatieprivacy (gegevens worden makkelijker verstrekt)
Fase 5	Blijvend gebruiken met daadwerkelijk bewustzijn en afweging tussen gemak en informatieprivacy (gegevens worden minder makkelijk vertrekt)	“

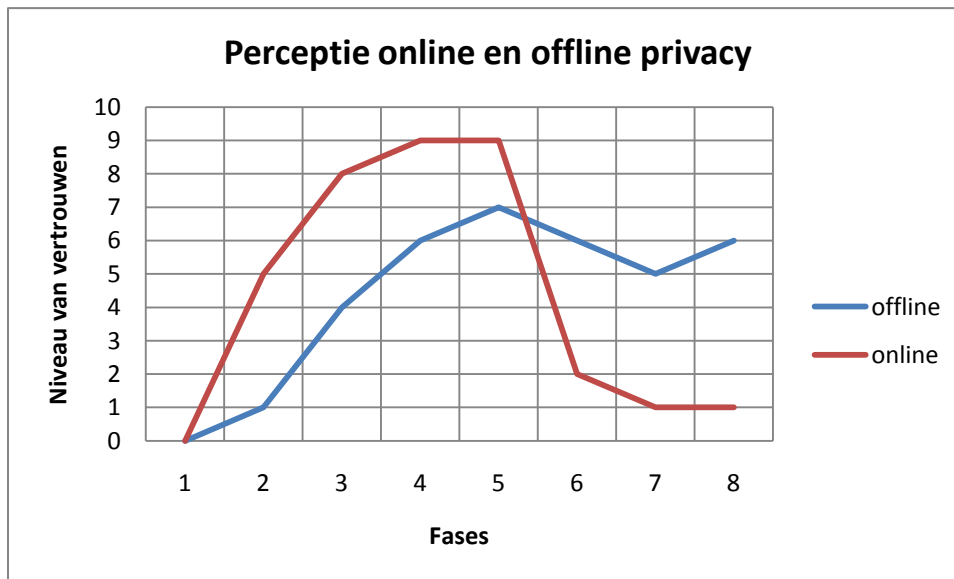
Figuur 5.1.2 “Fases die de perceptievorming doorloopt”

Het vertrouwen is nu opgebouwd en bij online privacy geschiedde dit erg snel en naar een hoog niveau. Bij offline privacy duurt het opbouwen langer en blijft het vertrouwen steken op een gemiddeld niveau. Bij een voorval waarbij het vertrouwen beschadigt raakt en de perceptie dus veranderd is de gang van zaken als volgt:

	Offline	Online
Fase 6	Vertrouwen neemt deels af	Vertrouwen is vrijwel geheel weg
Fase 7	Perceptie is licht negatief en offline privacy is in twijfel gekomen	Perceptie is negatief en online privacy is in het specifieke geval verdwenen
Fase 8	Controle kan teruggevonden worden en perceptie raakt weer positief	Controle is niet sterk terug te vinden en perceptie blijft negatief

Figuur 5.1.3 “Fases die de perceptievorming doorloopt in geval van beschadiging van het vertrouwen”

Het is dus te stellen dat studenten bij online privacy een beginnend positieve perceptie hebben welke op dit niveau blijft zolang alles correct verloopt. Er is veel afhankelijkheid van situaties en de perceptie kan snel van positief naar negatief schieten. De offline perceptie is wat ‘stroperiger’. Een positieve perceptie bereiken heeft meer tijd nodig maar is ook stabiel en zal niet snel heen en weer schieten. De verschillen hiertussen zijn te verklaren aan de hand van een aantal eigenschappen. Meest belangrijke is dat er geen sterke scheiding meer is tussen online en offline privacy in hun perceptie. Ze zijn immers veelal opgegroeid met de moderne online technologieën. De theorie komt dan voor offline privacy ook goed overeen maar voor online privacy niet. De gevormde perceptie hierbij wordt ook niet op dusdanige wijze gevormd zoals de theorie beschrijft.



Figuur 5.1.4 “Het verloop van de perceptievorming gebaseerd op figuur 5.1.2 en 5.1.3 (de horizontale as geeft de acht fases aan)”

6. CONCLUSIE

In deze scriptie is een brede uiteenzetting gegeven over informatieprivacy. Zowel voor de online als de offline variant. Ook is er uitgebreid stilgestaan bij de uitwerking van de case waarbij online en offline betaald werd. Tussen het eerste theoretische deel en het daaropvolgende praktijk gedeelte zijn verrassende overeenkomsten en verschillen gevonden. Het blijkt dat er gezien het bewustzijn en gedrag van de ondervraagde studenten wel degelijk een verschil is tussen online en offline privacy en dat dit erg veranderlijk is. De theorie voorziet vooral bij de offline perceptie op goede wijze, online is er nog de nodige aanvulling mogelijk.

Het vooronderzoek in de vorm van de enquête biedt echter nog veel mogelijkheden voor verder onderzoek. Naar voren is gekomen dat de leeftijd van de ondervraagden invloed heeft op de perceptie. Daarom is het interessant om het onderzoek voort te zetten met meerdere uit elkaar liggende leeftijdsgroepen. Bijvoorbeeld scholieren, studenten, leeftijdsgroep tussen de 26-35, 36-50, 51-64 en 65-plussers (ouderen). Hierbij zou een grotere groep ondervraagden nog meer inzicht geven. De verschillende resultaten kunnen duidelijker inzicht geven in perceptievorming en standvastigheid hiervan. De toevoeging van verschillende culturen kan, overeenkomend met de theorie, ook opmerkelijke inzichten bieden. Ook tussen opleidingen onderling kunnen verschillen en overeenkomsten ontdekt worden. Deze scriptie is gericht op de kant van de gebruiker en dan specifiek de student. Onderzoek naar de kant van de aanbieder (en hoe vertrouwen gewonnen kan worden) heeft ook potentie.

Bij het onderzoek naar informatiestromen en handelingen bij online en offline betalen is tevens een interessant inzicht ontstaan. De acceptgiro kan immers zowel via de post (offline) als alsnog via de computer (internetbankieren) betaald worden. Het verschil hiertussen en de omgang van zowel de gebruiker als de aanbieder zijn relevant voor verder onderzoek. Evenals in welke mate en op welke manier online en offline privacy elkaar beïnvloeden (zie figuur 4.3.2).

7. BIBLIOGRAFIE

Overzicht van gebruikte literatuur en andere bronnen.

1. *Is Privacy Relative?* **Räikkä, Juha.** sl : Journal of social Philosophy, Vol. 39 No. 4, Winter 2008, 534–546, Wiley Periodicals, Inc, 2008, pp. 534–546.
2. *Users' Perspective on Regulation to Protect Privacy on the Web.* **Lee, Byung.** sl : The International Information & Library Review, vol. 32 (2000), afl. 3/4, pag. 379-402 (24), Academic Press, 2000.
3. *Security in the wild: user strategies for managing security as an everyday, practical problem.* **Dourish, Paul, et al.** sl : Springer-Verlag London Limited 2004, Pers Ubiquit Comput (2004) 8: 391–401, 2004.
4. *Why Privacy Is Important.* **Rachels, James.** sl : Philosophy & Public Affairs, Vol. 4, No. 4 (Summer, 1975), pp. 323-333, Blackwell Publishing, 1975.
5. *Privacy and the Limits of Law.* **Gavison, Ruth.** sl : The Yale Law Journal, Vol. 89, No. 3 (Jan., 1980), pp. 421-471, 1980.
6. *The right to privacy.* **Warren, Samuel D. en Brandeis, Louis D.** sl : Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220, The Harvard Law Review Association, 1890.
7. *Privacy, emotional closeness, and openness in cyberspace.* **Ben-Ze'ev, Aaron.** Israel : Department of Philosophy, University of Haifa, Israel, Computers in Human Behavior 19 (2003) 451–467, Elsevier Science Ltd, 2003.
8. *ICT gebruik van personen.* **(CBS), Centraal Bureau voor de Statistiek.** 10-5-2011, Den Haag/Heerlen : CBS, 2011.
9. *Het CBP in 2009.* **Persoonsgegevens, College Bescherming.** 2009.
10. *Information Security Technology?...Don't Rely on It A Case Study in Social Engineering.* **Winkler, Ira S. en Dealy, Brian.** Salt Lake City : Proceedings of the Fifth USENIX UNIX Security Symposium, Salt Lake City, Utah, June, 1995.
11. *The ontological interpretation of informational privacy.* **Floridi, Luciano.** Bari : Ethics and Information Technology (2005) 7:185–200, Springer, 2006.
12. *The Nature of and Conditions for Online Trust.* **Koehn, Daryl.** sl : Journal of Business Ethics 43: 3–19, 2003. Kluwer Academic Publishers, 2003.
13. *Online trust: a stakeholder perspective, concepts, implications, and future directions.* **Shankar, Venkatesh, Urban, Glen L. en Sultan, Fareena.** sl : Journal of Strategic Information Systems 11 (2002) 325–344, 2002, Elsevier Science B.V., 2002.

14. *iDeal en Acceptgiro*. **B.V, Currence Holding**. 2011.

15. *Learning Styles and Learning Spaces: Enhancing Experiential Learning in Higher Education*. **Kolb, Alice Y. en Kolb, David A.** sl : Academy of Management Learning & Education, 2005, Vol. 4, No. 2, 193–212, 2005.

16. *Social Research Methods*. **Bryman, Alan**. United States, New York : Oxford University Press, 2008.

17. *ThesisTools*. **Rixtel, Joan van**. sl : www.thesistools.com (laatst geraadpleegd op: 17 juni 2011).

8. APPENDIX

In deze scriptie is veel informatie gebruikt. De appendix geeft hier een overzicht van. De gebruikte enquête is er te vinden evenals alle verzamelde data van dit onderzoek.

Enquête: Online & offline privacy

Voor mijn bachelorscriptie aan de Radboud Universiteit in Nijmegen voer ik een onderzoek uit naar studenten en hun beeld bij privacy, zowel in online (digitaal met een computer of telefoon) als offline (fysiek per brief of op papier) situaties. Het gaat hierbij om *informatieprivacy*, dat wil zeggen privacy met betrekking tot je (persoonlijke) gegevens.

Graag wil ik je vragen om de volgende vragen te beantwoorden. Alvast bedankt voor je medewerking!

Algemeen

1. Wat is je leeftijd? ____
2. Welke opleiding volg je momenteel? _____
 - a. Dit is een WO/HBO/MBO opleiding: ____

De volgende stellingen zijn te beantwoorden op een schaal van 1 tot en met 7 (1=geheel oneens, 2=oneens, 3=deels oneens, 4=neutraal, 5=deels eens, 6=eens, 7=geheel eens)

- | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1. Ik ben mij er bewust van wat privacy inhoudt | | | | | | | |
| 2. Ik verstrek mijn gegevens alleen indien dit noodzakelijk is | | | | | | | |
| 3. Ik ben bereid meer moeite voor iets te doen als ik dan minder persoonlijke gegevens hoeft af te staan | | | | | | | |
| 4. Ik ben bereid meer gegevens te verstrekken als ik daar voordelen mee krijg | | | | | | | |
| 5. Ik wil graag altijd weten welke gegevens van mij bij een organisatie bekend zijn en wat daar mee gebeurt | | | | | | | |
| 6. De Nederlandse wet voorziet in mijn ogen goed in de bescherming van mijn informatieprivacy (zowel online als offline) | | | | | | | |
| 7. Ik heb er geen probleem mee als mijn gegevens gebruikt/bekeken worden ten bate van de (nationale) veiligheid | | | | | | | |
| 8. Organisaties (telecomprovider, bank etc.) gaan vertrouwd met mijn gegevens om door toezicht van overheid en het College Bescherming Persoonsgegevens | | | | | | | |
| 9. Wanneer blijkt dat een organisatie niet zorgvuldig omgaat met mijn gegevens verlies ik mijn vertrouwen | | | | | | | |

Online & offline

- | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1. Online heb ik meer grip op het verstrekken van mijn gegevens dan offline | | | | | | | |
| 2. Bij online handelingen denk ik meer na over verstrekking van mijn gegevens dan bij offline handelingen | | | | | | | |

3. Bij online handelingen voel ik mij anoniemer dan bij offline handelingen	0 0 0 0 0 0 0
4. Ik bestel online producten net zo makkelijk als dat ik producten in de winkel koop	0 0 0 0 0 0 0
5. Ik ben mij ervan bewust dat er altijd iemand mee kan kijken bij verzending van gegevens, zowel online per internet als offline per post	0 0 0 0 0 0 0
6. Ik ben bereid online meer gegevens af te staan wanneer ik de organisatie offline ook ken	0 0 0 0 0 0 0
7. Ik denk dat mijn gegevens online gemakkelijker verkeerd gebruik worden dan offline	0 0 0 0 0 0 0
8. Mijn gegevens worden op social media (Facebook, Twitter etc.) gebruikt door andere (ongewenste) partijen voor marketing doeleinden	0 0 0 0 0 0 0
9. Online wordt veel gelogd (alles wordt bijgehouden) waardoor illegale handelingen makkelijker zijn op te sporen, dit geeft mij een veilig gevoel	0 0 0 0 0 0 0
10. De technologie beschermt mijn privacy beter dan de wetgeving	
11. Online kijk ik altijd naar de reputatie van de andere partij voordat ik gegevens verstrek	0 0 0 0 0 0 0
12. Bij een online handeling (bijv. betalen) denk ik altijd aan mijn privacybescherming	0 0 0 0 0 0 0
	1 2 3 4 5 6 7
13. De mens is een zwakkere schakel dan technologie bij bescherming van informatieprivacy	0 0 0 0 0 0 0
14. Via email/websites verstrek ik mijn gegevens eerder dan aan een echt persoon	0 0 0 0 0 0 0
15. Offline zal ik meer gegevens verstrekken wanneer ik het bedrijf ook online ken	0 0 0 0 0 0 0
16. Bij een offline handeling (bijv. betalen) denk ik altijd aan mijn privacybescherming	0 0 0 0 0 0 0
17. Wanneer ik online betaal met iDeal acht ik dit minstens net zo vertrouwd als wanneer ik offline betaal met een acceptgiro	0 0 0 0 0 0 0
18. Ik ben bereid een kleine vergoeding te betalen om offline(contant/acceptgiro) te kunnen betalen in plaats van op een online manier	0 0 0 0 0 0 0
19. Als een organisatie mijn vertrouwen online heeft gewonnen dan vertrouw ik deze ook offline	0 0 0 0 0 0 0
20. Ik denk dat wetgeving online en offline uit dezelfde onderdelen bestaan	0 0 0 0 0 0 0
21. Ik vind het belangrijk om te kunnen kiezen of ik een handeling online of offline uitvoer	0 0 0 0 0 0 0

Nu volgen enkele meerkeuzevragen.

22. Bij een aankoop betaal ik het liefst:
- Via internetbankieren/iDeal
 - Via acceptgiro

- c. Met PIN
- d. Contant

23. Ik lees de privacyverklaring (document waarin beschreven staat waarvoor mijn gegevens gebruikt worden) voordat ik een product bestel of dienst aan ga:

- a. Altijd
- b. Af en toe
- c. Gedeeltelijk
- d. Nooit

24. Aan mijn privacybescherming denk ik:

- a. Dagelijks
- b. Wekelijks
- c. Maandelijks
- d. (Bijna) nooit

Tot slot

- 1. Bij verstrekking van mijn gegevens online geef ik mijn vertrouwen hierin een (cijfer van 1 tm 10 waarbij 1=zeer slecht en 10=zeer goed): ____
- 2. Bij verstrekking van mijn gegevens offline geef ik mijn vertrouwen hierin een (cijfer van 1 tm 10 waarbij 1=zeer slecht en 10=zeer goed): ____

3. Je hebt deze enquête online ingevuld, deed je dit liever offline:

- a. Ja
- b. Nee
- c. Geen mening

Zo ja, waarom?

Heb je nog opmerkingen en/of aanvullingen?

Bedankt voor je medewerking! Mocht je geïnteresseerd zijn in het eindresultaat, geef dan hier je e-mailadres op: _____

Verzamelde gegevens

Alle verzamelde gegevens met behulp van de enquête. Eerst de algemene gegevens en vervolgens de specifieke antwoorden op de stellingen.

Enquête gegevens: algemeen

nr	leeftijd	opleiding	soort	opmerkingen	e-mailadres
1	24	Informatiekunde	WO		Ja
2	22	Informatica	WO		Ja
3	23	Informatiekunde	WO		Nee
4	20	Accountancy	HBO		Ja
5	21	Informatica	WO		Nee
6	20	Biomedische Technologie	WO		Nee
7	21	International Business and Management	HBO		Nee
8	23	Informatiekunde	WO	Bij het online invullen van deze enquête heb ik geen verdere gegevens hoeven invullen. Hierdoor is enkel mijn leeftijd en studie bekend waardoor er weinig vertrouwelijke persoonsinformatie bekend is.	Nee
9	22	Informatica	WO		Nee
10	21	SPH	HBO		Ja
11	21	Informatiekunde	WO		Ja
12	25	Informatica	WO		Nee
13	19	Griekse en Latijnse Taal en Cultuur	WO		Nee
14	22	Informatiekunde	WO		Ja
15	23	informatiekunde	WO		Nee
16	22	Informatiekunde	WO		Nee
17	19	Kunstmatige Intelligentie	WO		Nee
18	24	Rechtsgeleerdheid	WO		Nee
19	22	Informatiekunde	WO	Het feit dat de enquête alleen online verspreid wordt kan natuurlijk de resultaten wel beïnvloeden.	Ja
20	22	Bedrijfskunde	WO		Nee
21	22	Opleidingskunde	HBO		Ja
22	22	Orthopedagogiek	WO		Ja
23	24	Informatiekunde	WO		Nee
24	22	Bedrijfseconomie	HBO		Ja
25	21	Lerarenopleiding Nederlands	HBO		Nee
26	22	Verpleegkunde	HBO		Ja

27	19	Bedrijfsinformatietechnologie	WO		Ja
28	23	Kunstmatige intelligentie	WO		Nee
29	21	Taalwetenschap	WO		Nee
30	20	Informatiekunde	WO		Ja
31	25	Informatica	WO		Nee
32	20	Verloskunde	HBO		Ja
33	21	Taalwetenschap	WO		Nee
34	18	Accountancy	HBO		Nee
35	20	Geneeskunde	WO		Nee
36	21	Engelse Taal en Cultuur	WO		Nee
37	20	Bedrijfskunde	WO		Nee
38	21	Informatiekunde	WO		Ja
39	20	Bedrijfskunde	WO		Nee
40	20	Voeding & gezondheid	WO		Nee
41	24	Informatiekunde	WO	Bij vraag 12. Nee, omdat ik dan fysiek aanwezig zou moeten zijn ergens, nu kon het gewoon thuis.	Nee
42	19	Informatica	WO		Nee
43	20	Informatica	WO		Nee
44	20	Recht en Management	WO		Nee
45	20	Kunstmatige Intelligentie	WO		Ja
46	20	Bedrijfscommunicatie	WO		Nee
47	19	Recht&Management	WO		Nee
48	21	Informatiekunde	WO		Nee
49	22	Bedrijfskunde	WO		Nee
50	19	Economie	WO		Nee
51	20	Bedrijfskunde	WO		Nee
52	18	Bedrijfscommunicatie	WO		Nee
53	23	Informatica	WO		Nee
54	23	Pedagogische Wetenschappen en Pre-master Bedrijfskunde	WO		Nee
55	25	Communicatie- en informatiewetenschappen	WO		Nee
56	19	Bedrijfscommunicatie	WO		Nee
57	19	Communicatie- en informatiewetenschappen	WO		Nee
58	21	Communicatiewetenschap	WO		Ja
59	21	Bedrijfskunde	WO		Nee
60	19	Bedrijfscommunicatie	WO		Nee
61	20	Economie en recht	WO		Nee
62	22	Informatica	WO		Nee
63	24	Bedrijfskunde	WO		Nee
64	20	Economie	WO		Nee
65	20	Bedrijfskunde	WO		Nee
66	22	Bedrijfskunde	WO		Nee
67	21	Bachelor Informatica	WO		Ja
68	21	Informatica	WO		Ja
69	20	Financiële Economie	WO		Nee
70	18	Pedagogiek	HBO		Ja

71	22	WO Accountancy	WO		Ja
72	18	TCS	WO		Nee
73	19	Bedrijfscommunicatie	WO		Nee
74	19	CIW	WO		Nee
75	19	Bedrijfscommunicatie	WO		Nee
76	20	Bedrijfskunde	WO		Nee
77	19	Communicatie & Informatiewetenschap: bedrijfscommunicatie	WO		Nee
78	20	Communicatie- en informatiewetenschappen	WO		Ja
79	22	Informatiekunde	WO		Nee
80	20	Biologie	WO		Nee
81	22	Bedrijfseconomie	WO		Nee
82	21	Politicologie	WO		Nee
83	19	Bedrijfskunde	WO		Nee
84	20	Scheikunde	WO		Ja
85	19	Bedrijfscommunicatie	WO		Nee
86	21	Bedrijfscommunicatie	WO		Ja
87	20	Economie	WO		Ja
88	22	Bedrijfskunde	WO		Ja
89	21	Bestuurskunde	WO		Nee
90	23	Business Administration - International Management	WO		Nee
91	19	Bedrijfscommunicatie	WO		Nee
92	19	Bedrijfscommunicatie	WO		Nee
93	20	Internationale economie	WO		Ja
94	24	Bedrijfskunde	WO		Nee
95	23	Romaanse talen & culturen	WO		Nee
96	21	Economie	WO		Nee
97	23	Romaanse Talen en Culturen	WO		Nee
98	21	Biology	WO		Nee
99	19	Communicatie- en Informatiewetenschappen	WO	Online handelen kost vaak minder tijd/moeite en alles wordt geregistreerd. Een nadeel hiervan is dat je gevolgd en gecontroleerd kan worden door de overheid of door derden (hackers). Een klein voordeel is dat je je geldzaken goed op rij kunt hebben door digitale overzichten ivm registratie van alle handelingen.	Nee
100	20	recht & management	WO		Nee
101	21	communicatie- en informatiewetenschappen	WO		Nee
102	19	Economie	WO		Nee
103	18	Informatica	WO		Nee
104	23	Communicatiewetenschappen	WO		Ja

				Voor vertrouwen in online transacties (zoals bijvoorbeeld iDeal) is voor mij ook belangrijk dat er fatsoenlijke encryptie wordt gebruikt (SSL). Verder is het ook belangrijk dat er voldoende aan authenticatie wordt gedaan; bijvoorbeeld dat er bij betaling via iDeal authenticatie via SMS of iets dergelijks plaats vindt. Alleen gebruikersnaam+wachtwoord acht ik onvoldoende.	
105	23	Wiskunde	WO		Ja
106	23	Bedrijfskunde	WO		Nee
107	22	Spaanse taal en cultuur	WO		Ja
108	23	Bedrijfskunde	WO		Nee
109	21	Bedrijfskunde	WO		Nee
				Zowel online als offline heb ik het gevoel dat ik soms op een bazaar rondloop. Overal zie ik advertenties van sites waar ik net ben geweest (online) en overal waar je bent wordt je achterna gezeten door instellingen om je maar geld uit te laten geven (offline). Je kunt hierbij bijvoorbeeld denken aan de vriendenloterij, daar kun je zgn een keer gratis meespelen, ook wanneer je aangeeft niet meer benaderd te willen worden, blijven ze je gegevens toch gebruiken om je een lidmaatschap aan te smeren. Ik erger me er kapot aan en ben hierdoor zowel online als offline behoorlijk op mijn hoede m.b.t. het vertrekken van mijn gegevens.	
110	23	Bedrijfskunde WO	WO		Nee
111	22	Psychologie	WO		Nee
112	21	Bedrijfseconomie	WO		Nee
113	21	Bedrijfskunde	WO		Nee
114	20	Bedrijfskunde	WO		Nee
115	21	Pedagogische Wetenschappen	WO		Nee
116	23	Information Science	WO		Nee
117	20	Bedrijfskunde	WO		Nee
118	19	CIW-BC	WO		Nee
119	20	Informatiekunde	WO		Nee
120	20	Bedrijfseconomie	WO		Nee
121	21	Bedrijfskunde	WO		Nee
122	22	Bedrijfskunde	WO		Ja

123	20	Pedagogische wetenschappen	WO		Nee
124	20	Bedrijfskunde	WO		Nee
125	23	HRM	WO		Ja
126	21	Bedrijfscommunicatie	WO		Nee
127	19	Bedrijfskunde	WO		Ja
128	23	Informatica	WO		Ja
129	22	Bedrijfskunde Marketing Management	HBO		Nee
130	22	Informatiekunde	WO		Nee
131	20	Bedrijfskunde	WO		Ja
132	21	Economie	WO		Nee
				Vertrouwen hangt behoorlijk af van de omgevingsfactoren, bijvoorbeeld de aanwezige actoren. Daarbij speelt gevoel een grote rol.	
133	21	Bedrijfskunde	WO		Nee
134	20	Bedrijfskunde	WO		Nee
				Ik vond de vraag over IDeal en de vraag daarna niet goed. Je vraagt eerst naar betaling via IDeal en daarna over betaling online in het algemeen, dan zeg je er niet bij dat het om IDeal gaat. Dit terwijl je volgens mij in de tweede vraag wel bedoelt dat het om IDeal gaat, of juist in de eerste vraag om betaling online in het algemeen. Dit heeft mijn antwoorden beïnvloed. Ik denk dat jij die vragen positief gekoppeld hebt, dus dat je op allebei eens of op allebei oneens moet antwoorden. Maar ik heb ze dus zeer verschillend beantwoord, omdat ik veel vertrouwen heb in de veiligheid van IDeal, maar juist niet in betaling met bijvoorbeeld een creditcard (ben ik laatst nog door belazerd zelfs). Succes met je onderzoek!	
135	21	Bedrijfskunde	WO		Nee
136	19	Bedrijfskunde	WO		Nee
137	25	Informatiekunde	WO		Nee
138	23	Bedrijfscommunicatie	WO		Nee

Enquête gegevens: stellingen

	privacy algemeen										online en offline privacy												deel II							meerkeuzevragen									
nr	1	2	3	4	5	6	7	8	9		1	2	3	4	5	6	7	8	9	10	11	12		1	2	3	4	5	6	7	8	9		1	2	3	4	5	6
1	6	6	5	4	5	4	5	5	7		6	6	7	7	3	5	6	7	2	6	5	5		4	4	5	3	6	1	6	3	6		1	2	2	7	8	2
2	5	6	5	6	4	4	6	4	6		5	6	4	6	5	4	6	6	5	3	5	5		6	2	5	5	7	2	5	2	3		1	4	4	5	7	2
3	6	4	3	5	4	5	3	6	7		3	4	6	6	1	6	1	7	1	4	3	3		7	5	5	1	7	1	4	1	4		1	4	2	7	7	2
4	4	5	6	5	3	5	6	6	7		1	2	6	5	2	4	6	6	2	6	1	1		4	4	5	1	6	1	1	4	5		4	3	4	7	9	2
5	7	2	2	5	5	2	2	1	4		5	3	3	6	7	7	7	7	2	5	6	6		7	6	4	4	6	1	4	1	2		3	4	2	7	8	2
6	6	5	6	4	4	5	5	5	5		5	6	5	7	6	6	5	2	4	5	5	5		6	3	6	6	7	2	5	4	5		1	3	2	6	7	2
7	5	5	4	3	7	2	4	6	7		4	6	3	6	5	4	4	6	5	5	5	7		4	3	5	6	6	1	6	2	4		1	3	2	7	7	2
8	6	7	6	4	5	3	2	3	5		3	4	5	5	6	5	6	7	5	4	5	5		7	5	4	3	3	3	4	2	4		4	3	3	6	7	2
9	7	5	6	6	5	5	4	6	6		4	5	5	6	6	6	6	5	4	4	7	5		7	2	5	2	6	1	6	2	4		3	3	2	7	8	2
10	6	3	4	5	6	4	5	4	5		4	1	1	6	5	3	2	5	5	3	4	6		4	5	3	2	6	1	2	2	5		3	4	3	8	8	2
11	6	5	5	2	3	6	6	6	6		2	2	5	7	3	6	6	1	5	4	6	6		6	2	4	7	7	1	5	5	1		3	2	4	8	8	2
12	6	5	6	3	6	3	3	2	6		4	5	2	6	6	4	5	6	2	4	6	6		7	2	2	6	5	3	2	4	5		1	1	1	7	6	2
13	5	3	4	3	6	4	3	6	3		3	5	5	2	5	6	6	4	3	2	5	6		6	3	2	2	5	5	4	4	6		3	4	4	6	8	2
14	6	6	7	5	7	1	5	3	5		3	3	5	7	7	6	7	6	1	7	3	7		7	4	7	5	6	1	4	1	5		1	2	3	7	9	2
15	6	5	5	6	4	5	5	5	7		2	4	4	5	5	5	3	6	5	5	5	5		5	3	4	4	5	3	4	4	4		3	4	4	6	6	2
16	6	5	6	5	6	4	2	4	6		3	3	2	6	7	5	6	2	2	5	6	6		3	2	3	6	6	2	4	2	4		1	3	2	7	7	2
17	5	5	3	4	6	3	5	5	6		3	5	5	3	4	6	3	5	5	6	5	7		5	4	5	7	6	2	5	4	4		1	2	2	7	8	3
18	7	6	6	3	4	5	3	2	6		1	5	5	7	5	6	2	3	4	4	3	3		5	3	2	1	7	1	5	3	6		3	4	4	7	7	2
19	6	7	6	3	6	2	2	2	6		6	2	6	6	6	4	3	6	1	2	4	5		6	3	3	2	7	2	6	3	6		3	2	2	6	7	2
20	2	6	6	6	5	4	2	4	7		1	6	5	6	2	7	6	2	2	2	3	2		5	2	2	2	4	1	2	4	4		1	4	4	9	9	1
21	7	6	7	5	6	1	1	1	7		2	1	3	6	6	5	6	7	2	4	7	7		7	1	6	7	6	1	6	1	5		1	3	1	6	7	2
22	6	4	5	4	4	3	4	3	3		3	5	5	6	5	5	5	3	3	3	3	5		5	3	3	3	6	3	4	3	5		1	2	2	6	6	2
23	6	5	6	5	3	3	5	2	5		2	5	5	4	5	5	6	5	3	5	5	4		6	3	3	1	6	1	6	2	3		3	3	1	5	6	2
24	6	4	3	6	3	3	5	3	6		2	5	4	7	6	6	6	4	5	4	4	6		4	5	4	6	7	1	6	2	3		1	4	4	8	7	2
25	5	6	5	5	4	4	3	4	6		4	3	5	5	3	6	6	7	3	2	4	5		6	3	2	3	6	2	5	5	5		4	3	4	7	8	2
26	6	6	5	4	6	5	5	5	6		2	6	4	3	3	5	6	3	3	4	6	6		3	3	5	5	6	5	5	3	6		3	3	3	7	8	2

27	6	3	5	5	7	1	1	2	3		3	3	6	3	6	6	5	2	1	1	4	3		4	2	4	2	7	6	4	1	6		4	4	1	8	9	1
28	7	5	2	6	3	3	3	4	6		2	3	4	2	4	7	6	3	4	4	3	4		3	5	3	1	7	2	6	3	7		3	3	4	5	5	2
29	6	5	6	5	7	5	5	5	7		2	5	5	3	5	6	6	4	3	3	3	5		3	5	4	3	6	4	7	1	6		3	4	3	6	7	2
30	5	5	3	5	2	4	5	5	3		5	4	5	3	4	5	4	5	4	4	3	2		5	6	4	4	6	5	5	4	4		1	2	3	7	5	2
31	5	5	6	6	6	3	5	4	6		2	3	4	6	3	6	6	4	3	5	6	5		5	2	4	2	6	2	4	2	3		3	2	3	6	6	2
32	6	7	5	5	4	6	6	6	6		4	3	3	1	6	6	6	4	4	2	5	6		3	1	6	5	5	4	5	3	5		3	3	3	7	8	2
33	5	5	4	4	4	4	3	4	6		3	5	1	6	5	5	5	5	1	4	5	3		4	5	4	2	4	2	5	3	3		3	3	3	6	7	2
34	7	7	7	3	6	4	4	7	7		4	6	7	5	5	5	6	4	4	5	5	4		5	4	3	4	7	2	5	4	4		1	3	4	6	6	2
35	6	6	5	6	7	4	6	6	6		2	3	6	3	3	5	6	6	4	4	5	6		1	5	5	3	4	3	5	4	6		3	4	3	7	8	2
36	5	5	6	5	7	6	7	4	7		3	5	5	1	2	6	7	2	3	3	5	4		7	5	3	1	7	1	7	5	3		1	4	4	8	0	2
37	7	7	3	5	6	7	6	6	2		6	6	6	1	3	6	6	5	5	4	4	3		6	5	5	4	5	3	5	3	5		1	3	4	8	7	2
38	5	2	5	4	2	4	5	4	6		1	3	6	7	2	6	6	5	5	5	3	2		6	4	6	2	7	1	5	3	4		3	4	4	5	9	2
39	6	6	6	5	3	4	3	6	7		2	3	5	6	5	6	7	6	5	2	1	5		2	2	3	5	6	3	4	2	6		3	2	4	7	9	2
40	6	6	6	4	5	5	5	3	6		4	6	3	3	5	5	6	6	3	3	4	5		3	3	4	3	6	3	4	5	5		1	2	2	7	8	2
41	6	4	7	3	5	2	1	1	7		4	3	5	2	4	4	5	7	1	2	6	5		7	3	5	3	4	4	4	3	6		3	2	1	2	3	2
42	7	6	7	3	7	4	1	5	6		6	6	5	6	7	3	6	6	2	5	4	7		7	5	1	3	6	2	5	5	2		1	2	1	5	5	2
43	7	5	3	6	7	2	3	4	2		2	2	2	7	7	7	5	6	3	2	1	3		6	2	2	2	6	1	4	2	5		1	4	4	7	8	2
44	6	7	7	5	7	2	5	2	7		6	7	7	5	7	7	7	5	5	3	7	5		6	1	4	1	7	1	7	3	7		1	3	3	7	8	2
45	6	7	1	2	7	5	1	2	6		1	6	5	4	5	6	6	7	2	1	3	2		7	3	3	1	4	2	6	1	7		3	4	2	4	8	2
46	7	5	5	4	6	5	6	3	6		4	6	5	5	5	7	7	6	6	3	5	5		5	3	4	3	5	1	3	3	3		1	4	3	6	8	2
47	7	6	6	6	7	7	7	7	7		2	6	4	4	4	6	7	7	4	1	1	5		7	4	4	6	7	1	6	4	4		3	2	1	8	9	3
48	6	4	3	4	6	4	7	6	6		3	3	5	6	6	6	5	7	2	4	3	6		6	2	5	7	6	2	6	3	5		1	2	1	8	8	2
49	6	6	6	4	5	4	2	5	6		2	4	2	5	6	4	7	6	3	3	6	6		5	4	5	6	2	1	5	1	5		2	1	2	7	8	3
50	7	5	6	5	7	6	4	4	7		2	7	2	6	6	6	7	5	3	3	6	6		6	2	4	1	7	2	4	4	6		4	4	4	7	8	2
51	7	6	6	5	6	3	3	5	6		2	5	4	2	5	6	6	4	5	5	4	5		5	3	3	6	6	3	3	4	5		3	3	2	7	8	2
52	5	7	2	6	4	6	5	5	7		1	7	5	2	3	5	6	6	5	4	5	6		6	3	3	1	7	5	6	2	6		2	4	3	9	7	2
53	7	6	6	2	5	4	3	2	7		5	3	5	3	5	1	2	7	3	4	5	6		6	4	1	1	3	5	4	2	7		4	2	1	5	4	2
54	7	6	6	5	3	5	6	5	6		1	2	5	3	1	5	7	4	2	1	3	3		4	4	2	7	3	2	5	6	7		1	4	4	4	7	2
55	7	5	3	5	4	5	6	4	4		3	5	4	3	5	4	5	6	3	2	4	5		4	3	3	4	4	2	5	4	3		3	2	3	7	8	2
56	2	4	5	3	4	4	5	4	6		2	2	5	5	4	5	5	5	3	3	3	3		4	4	5	4	5	3	5	4	5		3	3	2	6	7	2
57	6	7	6	6	4	4	7	3	6		2	6	5	5	4	6	6	6	5	3	2	6		6	2	4	3	5	2	5	2	5		3	3	4	6	7	2
58	6	4	5	5	4	5	6	5	7		2	3	4	3	7	7	6	7	2	4	5	7		6	1	1	7	3	1	4	2	6		3	2	1	7	8	2
59	6	5	4	5	5	4	5	4	5		3	4	2	6	6	5	5	7	4	4	5	5		4	3	5	5	5	2	4	5	5		1	4	2	4	6	2
60	6	5	4	4	5	6	6	6	6		4	4	2	6	6	4	5	6	4	2	6	6		6	2	4	6	6	2	5	4	2		3	2	2	8	8	3

61	7	7	6	6	3	6	7	6	5		2	5	5	2	2	6	5	1	3	3	4	3		2	4	3	7	7	1	6	2	3		3	4	4	8	8	2
62	7	4	3	4	7	1	1	1	7		1	2	5	3	6	6	7	7	3	2	6	6		7	6	2	6	1	5	4	1	7		2	4	2	3	4	2
63	6	5	6	5	6	3	4	2	6		4	5	4	6	5	6	6	6	7	3	4	5		5	4	4	3	4	2	5	1	5		3	2	3	7	8	2
64	6	7	5	5	6	5	3	5	7		4	6	5	3	4	5	5	2	4	2	2	5		4	2	4	2	6	2	4	3	5		3	2	3	6	7	2
65	6	6	5	4	6	6	6	5	6		3	5	3	6	5	5	6	3	4	4	5	6		3	3	4	3	5	3	5	4	5		3	3	2	7	8	2
66	6	3	3	5	4	5	5	4	5		1	2	5	4	5	5	5	5	4	2	3	5		4	3	4	3	6	2	4	1	5		3	4	3	5	7	3
67	6	5	6	5	5	4	5	6	7		4	4	6	6	6	3	5	5	3	1	5	6		6	5	3	5	5	3	5	2	5		1	2	2	7	8	2
68	7	5	5	3	6	1	4	5	6		5	2	6	7	6	3	6	3	3	5	7	5		6	5	6	3	6	2	5	2	5		1	2	3	6	7	2
69	7	5	6	6	6	4	6	4	6		3	5	5	6	7	7	7	7	4	4	4	5		3	5	4	4	7	1	7	4	5		1	4	4	8	8	2
70	6	7	4	4	3	4	6	4	6		2	5	6	3	2	2	6	3	4	5	1	5		3	1	6	5	6	1	5	2	6		3	4	4	7	9	2
71	6	6	3	3	2	5	6	5	6		3	1	5	3	3	6	6	6	6	3	2	2		5	2	2	3	6	1	5	5	2		1	4	4	7	7	2
72	6	6	6	3	7	1	4	3	7		4	4	2	1	6	5	6	7	2	5	1	7		5	4	4	3	4	2	6	2	7		4	3	1	4	7	2
73	5	7	2	3	4	4	3	4	6		4	5	4	3	4	4	5	4	4	5	5	5		4	3	4	5	5	4	5	4	6		1	2	3	6	6	3
74	6	5	7	5	4	4	7	5	6		4	6	2	2	6	6	4	7	7	6	6	7		4	3	4	3	6	2	4	4	5		1	3	2	1	7	2
75	5	3	3	5	5	3	6	4	5		1	6	2	3	3	5	7	5	5	2	6	5		4	2	5	1	5	1	4	2	6		3	3	4	7	7	2
76	6	5	6	4	6	3	1	2	6		4	6	6	2	5	5	5	4	3	2	5	5		5	3	2	1	6	1	5	3	5		3	2	3	5	7	2
77	7	5	3	6	1	6	6	5	4		1	7	5	3	5	7	6	2	3	2	2	5		6	2	1	2	2	1	5	1	5		4	4	4	5	7	2
78	6	6	4	5	3	6	7	7	7		3	5	5	2	6	7	6	7	4	4	5	7		4	3	3	1	3	3	6	5	4		3	4	3	6	8	2
79	6	4	3	5	3	5	3	6	6		2	3	4	5	3	3	5	4	2	2	5	6		6	2	2	3	6	2	6	2	6		3	4	4	6	6	2
80	6	6	7	2	6	3	2	6	6		2	5	3	1	6	2	7	4	2	4	4	6		5	5	5	4	3	6	4	2	7		4	2	2	4	7	3
81	6	4	5	4	7	3	2	7	7		4	4	5	3	4	5	5	5	2	4	4	7		4	4	6	7	7	4	6	4	3		3	3	2	6	8	1
82	6	2	3	5	4	2	5	2	3		1	4	3	2	6	5	7	6	3	4	2	4		6	2	3	3	6	2	5	1	4		3	4	4	4	6	2
83	5	6	4	4	3	6	6	4	7		2	6	3	1	5	6	6	3	2	2	4	5		3	2	3	4	6	1	4	4	5		3	4	3	5	7	2
84	6	5	3	5	6	5	3	5	7		5	4	4	5	5	6	4	2	4	2	3	4		5	5	5	4	7	2	5	5	5		1	4	3	7	6	2
85	6	7	5	5	7	6	3	4	7		5	3	6	2	3	6	6	4	4	4	7	4		4	5	6	3	7	2	4	4	6		3	2	3	7	7	2
86	6	7	6	2	4	2	5	3	7		2	7	5	1	7	6	6	7	4	1	6	5		5	5	7	3	5	1	7	1	7		3	3	3	6	7	2
87	6	5	4	6	7	2	6	6	7		4	5	5	6	5	7	6	5	5	6	6	6		6	3	7	6	4	2	7	3	5		3	3	4	7	8	2
88	6	6	3	5	6	3	5	5	6		2	2	3	6	6	5	5	7	4	1	3	4		6	4	3	2	7	3	4	3	3		3	2	3	7	7	2
89	6	3	3	5	2	4	6	5	5		1	5	5	7	3	6	6	5	4	3	2	5		6	4	5	5	6	2	1	2	3		3	4	4	5	7	2
90	6	6	6	3	5	5	3	5	6		6	2	3	3	3	7	6	2	5	4	3	5		5	3	3	2	6	2	6	2	5		1	3	4	7	9	2
91	6	6	6	6	4	4	4	3	3		2	4	3	2	6	5	6	5	2	2	3	3		6	2	3	3	5	1	3	2	6		3	4	3	3	7	2
92	5	7	7	3	7	4	5	6	7		3	6	5	3	6	6	7	6	6	4	6	7		5	1	3	2	3	4	6	2	7		1	1	2	7	9	2
93	6	6	6	2	6	1	3	3	7		7	7	6	1	5	7	5	7	4	6	4	5		6	1	7	5	2	2	5	1	7		4	2	2	3	8	2
94	7	6	3	5	4	4	6	3	5		2	3	5	3	5	5	6	7	6	4	3	6		5	2	5	5	7	1	5	3	5		3	2	3	6	7	2
95	7	4	4	5	3	3	2	4	6		4	2	2	5	5	5	6	4	2	1	2	4		3	5	5	4	6	1	7	2	6		4	4	4	4	6	2

96	6	7	6	5	6	6	6	5	6		4	5	5	5	5	5	6	4	5	3	5	5		4	5	5	5	6	3	5	4	3		3	3	3	7	7	2
97	4	6	3	5	5	4	4	4	5		3	3	5	3	4	5	4	3	4	4	4	4		4	4	6	3	3	3	5	5	5		3	4	3	6	7	2
98	6	6	5	4	5	3	5	4	6		3	6	5	3	4	5	6	5	4	3	5	3		4	2	2	3	6	3	6	3	6		1	2	4	7	9	2
99	6	5	6	6	7	4	2	5	7		6	6	6	7	7	7	6	7	2	2	7	7		3	3	1	2	6	1	2	3	5		4	3	3	6	7	2
100	7	6	6	5	7	6	5	6	7		3	5	6	6	6	7	6	5	4	3	6	7		3	1	7	6	5	1	4	3	3		3	2	2	6	7	2
101	6	7	6	5	7	6	6	5	7		3	5	4	2	3	6	6	6	4	4	6	5		6	2	3	2	1	4	5	4	5		3	3	3	7	8	2
102	6	5	5	5	5	4	3	6	5		1	4	5	2	4	6	6	3	5	5	4	5		6	2	5	2	4	1	5	2	5		3	4	2	7	8	2
103	5	5	3	3	5	4	3	5	5		1	2	5	5	3	3	3	2	5	5	2	3		6	5	2	3	1	2	5	7	6		3	4	3	7	4	2
104	6	4	5	5	4	4	5	6	6		2	6	4	6	2	6	6	5	3	3	6	6		5	6	5	3	6	5	6	6	3		3	4	2	8	9	2
105	7	7	6	2	6	1	4	1	2		4	2	3	2	6	2	1	7	1	1	6	6		7	1	2	6	6	1	1	1	7		3	4	1	1	1	2
106	6	4	5	3	5	3	3	3	5		4	5	3	5	4	5	5	4	3	3	3	4		4	3	5	4	6	2	6	3	3		1	3	2	7	9	2
107	6	7	5	5	6	3	4	5	5		3	6	3	3	4	5	6	3	3	4	4	5		5	3	5	6	6	3	5	3	5		3	4	4	6	7	2
108	5	7	5	4	3	1	7	4	6		2	7	6	7	7	7	3	2	2	3	6	7		5	2	3	7	7	2	7	3	6		3	3	2	6	8	2
109	6	7	5	5	6	4	3	5	6		3	1	5	6	7	5	6	5	2	5	7	7		6	4	5	6	6	2	4	2	6		3	2	3	8	9	2
110	6	5	5	5	6	4	7	5	7		2	6	2	6	6	6	4	3	3	2	7	6		4	2	4	5	6	3	6	4	5		3	3	1	6	6	2
111	5	6	5	3	4	4	5	4	5		3	4	4	3	6	5	6	6	3	4	6	7		5	3	4	5	7	2	4	4	6		4	3	2	3	6	2
112	6	6	6	4	6	5	2	4	6		2	6	4	5	5	5	6	4	3	3	4	6		6	1	5	5	6	3	4	4	5		1	2	2	5	6	2
113	6	4	4	6	3	2	2	2	6		4	6	5	6	4	3	4	6	4	5	5	7		5	5	4	6	6	1	5	5	6		1	2	3	7	6	2
114	6	6	6	3	2	6	6	4	7		2	7	5	3	3	5	7	5	4	4	6	5		6	1	3	7	7	2	6	4	6		1	4	4	6	7	2
115	7	7	6	6	5	3	6	3	6		4	6	4	4	6	6	4	7	5	4	6	5		2	2	1	4	1	6	4	2	6		4	3	2	7	6	3
116	6	5	6	6	6	4	5	5	6		5	3	4	5	6	6	5	6	4	4	5	5		5	5	5	5	5	2	4	2	4		3	2	1	6	6	2
117	7	7	4	3	3	5	5	4	7		3	6	3	3	3	5	7	5	3	2	7	6		5	4	3	6	5	2	4	3	4		3	4	3	6	7	2
118	6	7	5	3	6	5	6	5	6		5	6	5	2	6	5	5	4	3	4	4	6		6	4	4	6	2	5	3	2	6		3	3	1	5	8	2
119	5	6	7	6	7	2	6	4	6		3	6	7	4	5	6	7	6	3	1	3	5		6	6	3	7	6	3	5	2	5		3	4	3	6	8	2
120	6	6	5	4	5	3	3	4	6		2	2	6	6	5	3	6	3	5	4	3	4		6	5	3	2	6	2	4	2	1		3	4	3	8	6	2
121	5	6	3	5	4	4	6	4	6		2	3	5	3	3	6	7	5	3	2	6	3		4	5	6	6	7	1	6	1	6		3	2	4	6	7	2
122	6	6	6	3	6	4	5	4	6		2	5	5	3	6	5	5	6	3	4	4	5		5	4	4	4	5	3	5	4	4		3	2	3	4	7	2
123	5	6	6	3	6	5	3	5	7		5	6	5	3	2	5	3	4	5	4	3	5		5	5	6	5	6	1	4	3	3		3	2	4	7	6	2
124	6	6	5	4	5	5	5	4	4		3	5	5	3	3	5	5	6	3	4	5	4		5	3	3	2	5	2	3	4	4		3	2	3	7	7	2
125	6	6	6	6	6	6	5	3	7		2	4	5	3	2	6	5	3	2	1	6	7		6	1	5	6	7	2	5	1	3		3	4	2	7	8	2
126	5	6	6	2	6	4	1	4	7		5	6	5	2	6	6	6	5	4	3	5	6		4	2	3	5	3	2	4	4	6		4	3	2	3	6	2
127	5	2	3	6	3	4	7	4	6		3	3	5	6	2	6	6	5	4	3	1	5		5	5	3	3	6	1	5	3	3		1	4	4	7	7	2
128	6	6	6	3	5	4	3	4	5		6	6	3	6	6	6	5	4	2	2	5	3		6	2	5	2	4	3	6	3	5		3	2	3	7	8	2
129	7	6	6	3	5	4	2	2	6		3	5	3	5	6	4	4	1	6	6	4	4		4	2	3	6	6	1	4	4	4		3	3	3	5	5	3
130	7	6	6	5	6	5	7	3	5		1	7	1	7	6	4	7	1	1	7	5	6		7	1	3	7	7	1	4	4	1		1	4	1	8	7	2

131	6	7	5	3	6	5	4	3	7		2	6	5	3	2	5	5	6	2	3	5	4		3	1	2	3	7	1	6	5	7		3	4	2	3	6	2
132	5	7	6	1	7	2	1	1	7		5	4	5	1	5	5	6	7	1	5	6	5		2	2	1	5	2	5	4	2	7		3	2	2	3	4	3
133	6	6	6	3	7	5	7	5	7		3	3	5	6	5	5	6	4	5	4	5	7		3	3	3	6	5	5	3	3	3		1	3	2	6	7	3
134	3	7	4	4	5	4	6	3	6		3	6	6	2	3	5	6	4	3	2	4	5		3	2	4	5	6	3	5	2	4		1	4	3	6	8	2
135	6	2	6	6	2	4	7	6	6		1	6	6	1	1	7	7	7	2	1	3	5		6	1	1	4	7	2	3	6	7		1	3	3	4	8	2
136	5	5	4	3	5	5	6	3	6		3	4	3	2	5	5	5	4	4	2	5	4		4	3	5	4	6	2	3	2	5		3	2	4	5	6	2
137	6	6	6	3	6	1	1	4	7		4	5	5	7	7	4	3	3	5	5	5	6		7	3	3	3	5	1	4	4	6		1	2	2	4	6	2
138	6	6	6	5	6	5	5	5	7		2	6	6	6	5	7	7	6	6	5	6	6		7	5	6	3	6	5	6	3	7		4	3	2	7	8	2