



De Privacy Clash

Is er een toekomst voor privacy?

Rotterdam School of Management
Erasmus University

Master of Science in Business Administration (MScBA)

Student	:	Marc Vuijk / 308878
Coach	:	Prof. Dr. R.J.M. van Tulder
Meelezer	:	Ass. Prof. R. van Wijk
Document	:	Master thesis
Versie	:	Definitief
Datum	:	1-9-2014

...and people never lonely, but living together and being so jolly and happy, like the summer dances here in Malpais, but much happier, and the happiness being there every day, every day...

Aldous Leonard Huxley, 'Brave New World'

You had to live — did live, from habit that became instinct — in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

George Orwell, '1984'

VOORWOORD

Met deze scriptie is een einde gekomen aan de parttime master bedrijfskunde studie aan de Rotterdam School of Management (RSM), Erasmus Universiteit te Rotterdam. Met voldoening kijk ik terug op twee intensieve jaren waarin ik veel leerde en beleefde. Uit je comfortzone treden, anders kijken, zelfreflectie, kritisch zijn; dat was de boodschap bij aanvang van de studie. Later verwoordde iemand dit als een 'herstructurering van de ziel' en na een college organisatiestudies of wetenschapsleer, kon dit gevoel je inderdaad bekruipen. De reden waarom ik voor deze studie koos, was het ontwikkelen van nieuwe 'bagage' voor de invulling van het tweede deel van mijn loopbaan. Nu terugkijkend meen ik in deze opzet geslaagd te zijn en kan ik niet anders zeggen dan dat het mijn leven heeft verrijkt.

Bijzonder dankbaar ben ik voor de steun van mijn gezin. Ze gunden mij de mogelijkheid om deze studie te doen en accepteerden dat ik minder tijd en aandacht voor ze had. Ik ben ze daarvoor veel dank verschuldigd en excuseer mij voor die momenten dat ik met mijn gedachten elders was.

Deze scriptie was eveneens niet tot stand gekomen zonder de hulp van Rob van Tulder, professor aan de Erasmus universiteit en mijn coach in het scriptietraject. De wijze waarop hij de begeleiding heeft gedaan, heb ik zeer gewaardeerd. Met veel plezier denk ik terug aan de besprekingen die als privé colleges aanvoelden. De altijd snelle reacties en de juiste sturing op het juiste moment, hebben ervoor gezorgd dat de ontdekkingsreis naar privacy goed is verlopen.

Voor zijn rol als meelezer dank ik Raymond van Wijk. Als laatste dank ook aan de programma managers voor hun faciliterende rol tijdens de studie.

Tenslotte, deze scriptie gaat over privacy. Een uitermate interessant onderwerp dat met de toenemende technische ontwikkelingen steeds meer relevantie lijkt te krijgen. In tijd en context geplaatst, krijgt privacy veel meer betekenis dat je zo op het eerste gezicht zou vermoeden. Graag neem ik u mee in mijn onderzoek naar dit thema en wens u daarbij veel leesplezier!

Marc Vuijk

Hendrik Ido Ambacht, September 2014

INHOUDSOPGAVE

VOORWOORD	3
SAMENVATTING	6
1 INLEIDING	7
1.1 Aanleiding	7
1.2 Probleemstelling	9
1.3 Doelstelling en centrale vraagstelling	10
2 PRIVACY NADER BEKEKEN	12
2.1 Wat is privacy	12
2.2 Relevantie van privacy	15
2.3 Belangenorganisaties	18
2.3.1 College bescherming persoonsgegevens (CBP)	18
2.3.2 DDMA	19
2.3.3 Nederlandse Vereniging voor Personeelsbeleid	19
2.3.4 Artikel 29-werkgroep	19
2.3.5 Global Privacy Enforcement Network	20
2.4 Conclusie	20
3 WAT STAAT ER OP HET SPEL	21
3.1 Privacy trade-off's	21
3.1.1 Rol van de overheid	21
3.1.2 Sociaal-maatschappelijke belangen	22
3.1.3 Economische belangen	25
3.2 Reacties op de trade-off's	27
3.3 Conclusie	31
4 METHODOLOGIE	34
4.1 Onderzoeksaanpak	34
4.2 Privacy taxonomie	34
4.3 Ontwikkelingsmodel	35
4.3.1 Gedragsdimensies	35
4.3.2 Fasering	36
4.3.3 Transitie en kantelpunten	38
4.4 Onderzoekspopulatie	38
4.5 Transitie management theorie	40
5 ONDERZOEKSRESULTATEN	42
5.1 Overzicht onderzoeksresultaten	42
5.2 Analyse onderzoeksresultaten	43
5.2.1 Grondhouding	43
5.2.2 Compliance	46

5.2.3	Communicatie en informatiedeling	49
5.2.4	Marketing.....	51
5.2.5	Personeelsbeleid (HRM).....	55
5.2.6	Innovatie en technologie	57
5.2.7	Society en instituties	60
5.2.8	Attitude per economie.....	62
5.2.9	Attitude per verdienmodel	64
5.3	Conclusie	67
6	CONCLUSIE EN DISCUSSIE	68
6.1	Conclusie.....	68
6.2	Discussie.....	72
6.2.1	Interpretatie van de resultaten.....	72
6.2.2	Kanttekeningen bij het onderzoek.....	72
6.2.3	Aanbevelingen voor vervolgonderzoek	73
7	BIJLAGEN	74
7.1	Bibliografie.....	74
7.2	Privacy taxonomie van Solove (2006)	77
7.3	Taken van het CBP	79
7.4	Privacy taxonomie.....	80
7.5	Taxonomie subindicatoren	83

SAMENVATTING

In dit onderzoek wordt de houding richting privacy bij vertegenwoordigers van de oude economie, nieuwe economie en enkele Telecom bedrijven onderzocht. In het bijzonder wordt gekeken naar hoe de verschillende visies op privacy doorwerken in de business modellen van deze ondernemingen. De olie van de nieuwe economie is data waaraan haar vertegenwoordigers hun bestaansrecht ontlelen. Gekeken naar de drie genoemde economieën, lijkt zich een strijd te ontwikkelen waarbij de toegang tot- en controle over persoonsgegevens de inzet is. Hoe deze strijd zich zal ontwikkelen en welke verschuivingen in de visies op privacy verwacht kunnen worden, komt eveneens in dit onderzoek aan de orde.

Teneinde de verschillende visies op privacy te duiden, is in dit onderzoek een taxonomie ontwikkeld op basis waarvan de attitude richting privacy kan worden vastgesteld. Vanuit verschillende perspectieven en management disciplines, zijn indicatoren gedefinieerd met per indicator vier formuleringen waarin de karakteristieken voor respectievelijk een inactieve, reactie, actieve en proactieve houding tot uiting komen.

De onderzoekspopulatie bestaat uit elf bedrijven waarvan vier nieuwe economie, twee Telecom en vijf oude economie ondernemingen. Het onderzoek is uitgevoerd door het analyseren van jaarverslagen, privacy statements, 'codes of conduct' en andere openbare bronnen. Daarnaast zijn met een drietal ondernemingen interviews gehouden waarbij enerzijds de geldigheid van de taxonomie is getoetst en anderzijds de houding van de betreffende onderneming is geduid. Daarnaast is aan vijf ondernemingen gevraagd feedback te geven op hun classificatie.

De onderzoeksresultaten tonen aan dat een neutrale houding richting privacy bij nieuwe economie bedrijven onwaarschijnlijk is. De relevantie van persoonsgegevens is voor deze ondernemingen hoog hetgeen dientengevolge een stellingname vereist hetzij middels een anti-privacy hetzij middels een pro-privacy houding. De houding van de oude economie is reactief-actief hetgeen enerzijds tot uiting komt in het respecteren van wet- en regelgeving (reactief) en anderzijds in de pretenties om klantbelangen zwaar te laten wegen (actief). De houding van Telecom is actief; ze lijkt intrinsiek gemotiveerd om de privacy belangen te beschermen. Ook is Telecom het meest expliciet in haar uitingen over privacy. Gekeken vanuit de verschillende business modellen lijkt er in combinatie met welke economie wordt vertegenwoordigd, een samenhang te zijn met de visie op privacy. Ten aanzien van de verwachte verschuivingen in de visies op privacy, lijkt privacy een zogenaamd 'wicked problem' te zijn waarvoor een geïsoleerde oplossing niet mogelijk is. De uiteindelijke richting zal worden bepaald door de ontwikkelingen rondom met elkaar samenhangende sociaal-maatschappelijke, economische en politieke issues en thema's.

1 INLEIDING

1.1 Aanleiding

Parallel aan de opkomst van het informatietijdperk en het internet sinds de jaren 70 en 80 uit de vorige eeuw, is de maatschappelijke discussie rondom privacy fors toegenomen. Overheden en bedrijven blijken voor eigen doelen persoonsgegevens te gebruiken al dan niet rekening houdend met de privacy belangen van individuen. Doorgaans wordt privacy intuïtief geïnterpreteerd gerelateerd aan aspecten uit de persoonlijke levenssfeer. Uit de literatuur blijkt dat privacy een diffuus concept is waaraan vanuit meerdere invalshoeken betekenis kan worden gegeven. Nissenbaum (1998) ziet privacy als een veilige haven waarin mensen zich vrij weten van kritische blikken en invloeden van anderen. Ook schept het de condities voor een florierende democratie waarin mensen een waardig bestaan kunnen leiden. Tevens stelt privacy individuen in staat om intieme relaties te onderhouden en te controleren (Mooradian, 2009; Rachels, 1975).

Dat privacy inmiddels een ‘hot issue’ is, kan worden afgeleid uit de vele aandacht hiervoor in de media bijvoorbeeld rondom de onthullingen van Edward Snowden inzake de praktijken van de Amerikaanse National Security Agency (NSA). Het infiltreren in bedrijfs- en buitenlandse regeringsnetwerken, het afluisteren van telefoongesprekken en het aftappen van internetverkeer, blijkt sinds 2007 op grote schaal onder de codenaam PRISM te zijn toegepast. De woorden van president Obama dat Amerikanen hun privacy altijd hebben gekoesterd en zich hebben beschermd tegen onrechtmatige indringing in hun persoonlijke levens en privé-zaken, staan hiermee in schril contrast (MacDermott & Smith, 2013). In een reactie op deze onthullingen was het president Rousseff van Brazilië die deze praktijken in de algemene vergadering van de Verenigde Naties veroordeelde en opriep om de privacy rechten te respecteren. Zonder die, aldus Rousseff, “there can be no true freedom of expression and opinion, and therefore no effective democracy”¹. Een ander voorbeeld betreft de ophef in maart 2014 over het voornemen van ING om adverteerders inzicht te geven in klantgedrag (Financieel dagblad, 10-3-2014). Naast de reguliere banktaken wil ING aan klanten die daar prijs op stellen, op maat gesneden advertenties aanbieden. Op basis van het betalingsverkeer kan ING niet alleen vaststellen ‘waaraan’ klanten hun geld uitgeven, maar ook ‘wanneer’ en ‘waar’ ze dat doen. Lokale aanbieders kunnen deze informatie in samenspraak met ING gebruiken voor het identificeren van hun doelgroep teneinde hen concurrerende aanbiedingen te kunnen doen. Onder de vele negatieve reacties was het de Consumentenbond die de plannen zelfs in strijd met privacywetgeving achtte.²

Dat de sociaal-maatschappelijke relevantie van privacy toeneemt, lijkt te maken te hebben met een nieuwe sociale structuur die door Castells (2000) als de ‘network society’ wordt getypeerd. Een sociale structuur ziet hij als het geheel van organisatorische arrangementen waarin mensen betrokken zijn in relaties van productie/consumptie, belevingen en macht. Betekenis wordt daarbij oneindig geconstrueerd op basis van de interactie tussen de actoren. Daar waar in de tijd en ruimte clustering van gedeelde betekenissen plaatsvindt, ontstaat cultuur. Technologie is volgens Castells de derde fundamentele factor voor het menselijk handelen op basis waarvan een sociale structuur zoals de netwerksamenleving ontstaat. Naast technologie wordt de netwerksamenleving ook gekenmerkt door transformaties in de organisatie van de economie, werk, cultuur, politiek, overheid, tijd en ruimte. Voorbeelden waarin de netwerksamenleving zicht manifesteert zijn onder meer: (1) globalisering; (2) netwerken waarin bedrijven kennis, ervaring, creativiteit en kapitaal bundelen om met elkaar nieuwe innovaties te realiseren; (3) verhoogde arbeidsmobiliteit; (4) vervaging van de grens tussen werk- en privé-tijd; en (5) machtsdeling en onderhandelde besluitvorming bij met name overheden (Castells, 2000). In de netwerksamenleving gaan overheden, bedrijven en individuen dus allerlei vormen van relaties met elkaar aan en wisselen daarbij (persoons)gegevens uit. Teneinde het netwerk optimaal te laten functioneren,

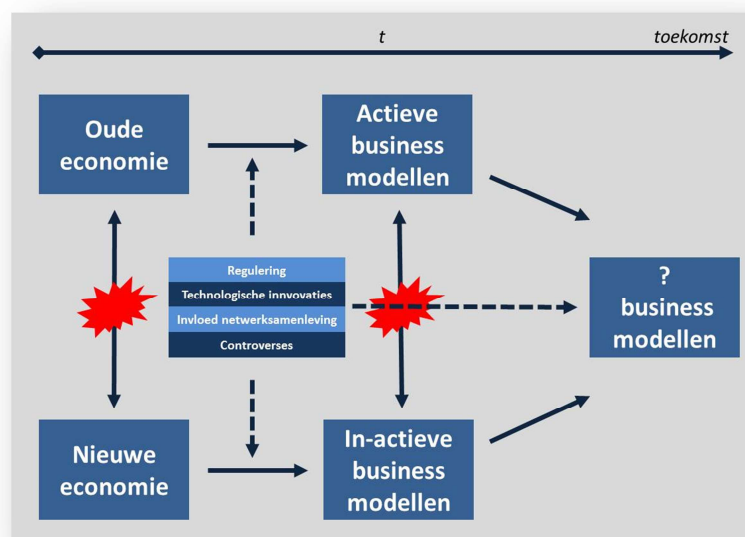
¹ <http://gadebate.un.org/68/brazil>

² <http://www.nrc.nl/nieuws/2014/03/10/consumentenbond-plannen-ing-in-strijd-met-privacywetgeving/>

lijkt het noodzakelijk dat gegevens maximaal worden gedeeld. Voor individuen impliceert dit dat zij hun gegevens ter beschikking stellen aan het netwerk en daarmee concessies doen aan de eigen privacy belangen.

Naast de sociaal-maatschappelijke belangen van privacy, wordt informationele privacy in een economische context vooral gerelateerd aan het gebruik van persoonsgegevens voor commerciële doeleinden (PRESCIENT, 2011). Mede dankzij de technologische ontwikkelingen, worden deze persoonsgegevens geëxploiteerd door bedrijven zoals Google, Facebook en Twitter. Gekeken naar deze zogenaamde 'nieuwe economie' ondernemingen, blijkt dat hun business modellen zijn gebaseerd op de beschikbaarheid van gratis persoonsgegevens en de verkoop hiervan voor bijvoorbeeld advertentiedoeleinden. Hiertegenover staan de business modellen van de 'oude economie' bedrijven zoals banken, retailers en bedrijven in de traditionele consumenten markt, allen vaak met een diepe worteling in de Nederlandse samenleving. Daar waar de 'nieuwe economie' de privacy belangen lijkt te ontkennen en negeren, lijkt de 'oude economie' deze juist te willen respecteren en wordt de bescherming van privacy door sommigen zelfs als 'unique selling point' in hun waardepropositie gepositioneerd. Naarmate de netwerksamenleving zich verder ontwikkelt en technologie innoveert, is het de vraag of de actieve- en inactieve houding richting privacy van respectievelijk de oude en nieuwe economie houdbaar is. Daar waar beide economieën elkaar nu bestrijden, is het voorstelbaar dat één van beide houdingen richting privacy de boventoon gaat voeren of dat gaandeweg de strijd een nieuwe visie op privacy wordt ontwikkeld.

Privacy heeft dus omwille van sociaal-maatschappelijke en economische belangen relevantie. Hieraan kunnen technologische belangen worden toegevoegd. De relatie tussen privacy en technologie was al in 1890 onderwerp van discussie, destijds vanwege het ongeautoriseerd publiceren van foto's van personen in kranten dankzij de technologische ontwikkelingen in de fotografie (Finn, Wright, & Friedewald, 2013). Naarmate de techniek zich sindsdien verder heeft ontwikkeld, is ook het besef van potentiële dreigingen voor privacyschendingen gegroeid (Finn, Wright, & Friedewald, 2013; Conger, Pratt, & Loch, 2013; Friedewald & Pohoryles, 2013). De almaar veranderende wereld als gevolg van deze technologische innovaties, betekent tevens dat effectieve wetgeving rondom privacy moeilijk realiseerbaar is (Solove, 2002). Ofwel, wetgeving die vandaag nog actueel is, kan vanwege technologische vooruitgang morgen achterhaald zijn.



Figuur 1. De strijd om privacy

Tenslotte, in het voorgaande is enkele malen gerefereerd aan business modellen. Shafer et al. (2005) definiëren een business model als "a representation of a firm's underlying core logic and strategic choices for

creating and capturing value within a value network". Teece (2010) definieert een business model als "the manner by which the enterprise delivers value to customers, entices customers to pay for value, and converts those payments to profit". Anders gesteld: het is de organisatorische en financiële architectuur waarmee een onderneming winst realiseert (Teece, 2010). Geprojecteerd op de strijd en controverses rondom privacy, zal de wijze waarop de vertegenwoordigers van de oude en nieuwe economie (onder invloed van de verschillende visies op privacy) hun business modellen en waardeproposities veranderen, bepalend zijn voor hoe deze strijd wordt beslist (figuur 1).

1.2 Probleemstelling

De huidige netwerksamenleving is de manifestatie van de nieuwe sociale structuur zoals die zich sinds de jaren tachtig uit de vorige eeuw heeft ontwikkeld. Een serie van transformaties op diverse sociale gebieden plus de ontwikkeling van verschillende dominante technologieën, hebben geleid tot de samenleving van nu. Inmiddels is er een maatschappelijk debat gaande over de impact van deze innovaties op de privacy van burgers. Sommigen (Bartels, 9-3-2014) menen dat privacy 'het issue' in de komende jaren zal zijn. Gevoed door de vele privacyschendingen en de aandacht daarvoor in de media, is inmiddels het beeld ontstaan dat burgers de controle over hun persoonsgegevens hebben verloren en overgeleverd zijn aan de praktijken van bedrijven zoals Facebook en Google. Is dit beeld terecht of zijn burgers vanuit een sociale behoefte om 'gezien' te willen worden, hier wellicht zelf debet aan? Innovaties waaraan volop wordt gewerkt zijn 'wearables' en 'big data'. De sociale gevolgen zijn nog onvoldoende duidelijk. Zo bestaat er een verbod op het zonder toestemming maken van opnames, maar hoe kan dit worden gehandhaafd in een wereld waarin iedereen met 'Google Glasses' rondloopt? De technologische ontwikkelingen dwingen tot een heroriëntatie op privacy. Kunnen we erop vertrouwen dat de wetgever in staat is om de privacy belangen van burgers te behartigen? Een eerste probleem is al dat een precieze definitie van privacy ontbreekt en iedereen daar een eigen beleving bij heeft. Eén van de gevolgen is dat privacy te pas en te onpas wordt gebruikt als argument voor bepaalde rechten of plichten.

Privacy creëert dus controverses tussen burgers, overheid en ondernemingen. In deze strijd speelt onder meer de waardering van privacy een rol. Wordt privacy als een mensenrecht gezien of is het een economisch goed? Daar waar het een mensenrecht zou zijn, gelden er fundamentele, morele waarden voor het beschermen van privacy en moet aantasting daarvan worden bestraft. Het is dan wel cruciaal dat we weten wat privacy is en wat de regels zijn waaraan iedereen zich moet houden. In het andere geval zijn economische principes het uitgangspunt waarbij er een kosten-/batenanalyse plaatsvindt van meer of minder privacy in ruil voor respectievelijk minder of meer voordelen. Dat data een economische waarde heeft, is goed ingeschat door Facebook en Google. In ruil voor hun diensten krijgen ze van gebruikers 'gratis' de persoonsgegevens die vervolgens worden doorverkocht voor advertentiedoeleinden. Niet verwonderlijk dat zij privacy niet zien zitten, het bedreigt immers hun business model. De vraag is hoelang een dergelijk business model nog te handhaven is bijvoorbeeld omdat consumenten inzien dat de waarde van hun persoonsgegevens meer is dan zij nu vergoed krijgen.

Een andere aspect in de privacy discussie gaat over de vraag in hoeverre we invloed willen hebben op technologische vooruitgang. Kiezen we daarbij voor liberalisering waarbij we ruim baan geven aan bedrijven om hun innovaties te ontwikkelen, en als hiervoor privacy moet worden ingeleverd dan is dat maar zo? Of kiezen we voor conservatisme waarbij we restricties en sancties opleggen, en op die manier de netwerksamenleving - inclusief de meningsvorming over privacy - in de gewenste richting sturen? Of is er een tussenweg, door te faciliteren waar mogelijk en te reguleren indien nodig? En, is het eigenlijk wel zo dat privacy technologische vooruitgang belemmert? Een ander scenario kan zijn dat de technologische ontwikkelingen zo krachtig en ingrijpend zijn, dat ze niet kunnen worden tegengehouden zoals dat ook gold voor de stoomkracht, elektriciteit en olie bij eerdere opgaande economische bewegingen (Devezas, Linstone, & Santos, 2005). Geldt niet hetzelfde voor IT, Nano technologie en biometrie waarbij er nadrukkelijk sprake is van privacy issues? Een

pro-privacy houding betekent zo bezien dat je tegen technologische voortuitgang bent. Omgekeerd betekent het dat als je technologie belangrijk vindt, privacy er eigenlijk niet toe doet. Er tekent zich dus een strijd af tussen zogenaamde privacy fundamentalisten en een stroming die stelt dat privacy niet meer bestaat. Is dat niet de aloude tegenstelling tussen conservatieven die het oude willen handhaven versus de progressieven die willen vernieuwen? Gelet op de ondertoon in de maatschappelijk discussie over privacy, lijkt de conservatieve gedachte de overhand te hebben en is er volop aandacht voor de privacy rechten van burgers. Maar, zijn deze conservatieven dan ook allemaal tegen technologische vernieuwing?

Hoe deze strijd zich verder zal ontwikkelen en wie de winnaars zullen zijn, is een nog onbeantwoorde vraag. De wijze waarop de maatschappij met tegenstellingen rondom privacy zal omgaan, zal hierbij richtinggevend zijn. Ongetwijfeld zal er vanuit overheden regelgeving worden verordend waarmee de richting voor een deel zal worden bepaald. Gegeven de internationale tegenstellingen bijvoorbeeld tussen Europa en Amerika, kunnen er vraagtekens worden geplaatst bij de effectiviteit hiervan. Komt de oplossing dan vanuit belangengroepen of zullen die de tegenstellingen alleen maar vergroten? Of is het mogelijk dat ondernemingen de door henzelf gecreëerde tegenstellingen zullen oplossen en er een herdefiniëring van privacy plaatsvindt waarin met de privacy belangen van burgers terdege rekening wordt gehouden? Vooralsnog laten met name de dragers van de internet revolutie niet blijken dat ze privacy serieus nemen en is het voorstelbaar dat de overgang naar het nieuwe technologische paradigma gepaard zal gaan met conflict, confrontatie of zelfs vernietiging. De oude industrieën lijken zich gematigder op te stellen in die zin dat privacy er voor hen toe doet, wellicht vanuit een ethisch motief maar ook eigen belangen zijn daarin niet uit te sluiten.

Geconcludeerd kan worden dat privacy een 'hot issue' is en in relatie tot de verdere ontwikkeling van de netwerksamenleving een prominente plaats zal opeisen.

1.3 Doelstelling en centrale vraagstelling

De controverses tussen overheid, ondernemingen en burgers rondom privacy lijken beïnvloed te worden door: (1) verschillende interpretaties van het begrip privacy; (2) verschillende visies op privacy; (3) verschillende belangen; (4) verschillende visies op technologie; en (5) verschillende visies op de netwerksamenleving. Sinds de opkomst van de nieuwe economie en de ontwikkeling van 'big data', lijkt er een heroriëntatie op het concept privacy gaande. In deze discussie claimen de verschillende stakeholders uit de oude en nieuwe economie hun gelijk echter een wetenschappelijke onderbouwing ontbreekt. Zolang de strijd tussen de oude en nieuwe economie voortduurt, is het voorstelbaar dat de heroriëntatie zal leiden tot nieuwe visie(s) op privacy. De doelstelling in dit onderzoek is derhalve te komen tot gefundeerde verwachtingen ten aanzien van welke visie op privacy zal gaan domineren.

De centrale vraagstelling in dit onderzoek is dientengevolge:

Hoe manifesteren de verschillende visies op privacy zich in de business modellen van de oude en nieuwe economie en welke verschuivingen in deze visies kunnen worden verwacht in de strijd tussen vertegenwoordigers van beide economieën?

Teneinde een antwoord op deze vraag te kunnen geven, worden de volgende deelvragen behandeld:

1. Ten aanzien van het concept privacy komen de volgende vragen aan de orde:
 - a. Wat is (informatie) privacy?
 - b. Wat is de relevantie van privacy?
 - c. Welke belangenorganisaties zijn er en wat is hun rol?
2. Ten aanzien van de belangen rondom privacy worden de volgende vragen gesteld:
 - a. Welke trade-off's rondom informatieve privacy kunnen worden onderkend in de wisselwerking tussen overheid, ondernemingen en burgers?

- b. Hoe gaan ondernemingen om met de tegenstellingen rondom de privacy trade-off's?

De beantwoording van deze vragen zal worden gedaan op basis van literatuuronderzoek, deskresearch en media analyse.

3. Welke visies op privacy kunnen in de huidige discourse bij vertegenwoordigers van de oude en nieuwe economie worden waargenomen?

De methodologische aanpak van deze vraag wordt toegelicht in hoofdstuk 4.

2 PRIVACY NADER BEKEKEN

In dit hoofdstuk zal het concept privacy nader worden uitgewerkt waarbij antwoord wordt gegeven op de volgende vragen: (1) wat is privacy?; (2) wat is de relevantie van privacy?; en (3) welke belangenorganisaties rondom privacy springen in het oog en wat is hun rol? Hiervoor zal gebruik worden gemaakt van literatuuronderzoek, deskresearch en media analyse.

2.1 Wat is privacy

Het concept privacy laat zich niet gemakkelijk definiëren. In het algemeen heeft iedereen wel een bepaalde voorstelling van haar betekenis, echter een eenduidige definitie is niet voorhanden. Zo kan iemand vinden dat zijn privacy wordt geschonden als je fysiek te nabij komt en de persoonlijke, intieme ruimte binnendringt. Het schenden van de privacy kan ook worden ervaren als je indringend wordt bekeken. Daar waar dit echter met een snelle oogopslag gebeurt, wordt dat niet als een probleem gezien. Het onbevoegd betreden van een huis schendt eveneens de privacy. Een ruzie die door een open raam hoorbaar is, en waarvan je toevallig in het voorbijgaan getuige bent, raakt wel iemands privacy maar van een schending kun je niet spreken. Het met buitengewone belangstelling volgen van dezelfde ruzie, lijkt echter weer wel op het overschrijden van een bepaalde grens. Ook het zonder toestemming openbaar maken van persoonlijke gegevens zoals inkomen, vermogen, medicaties, schulden, seksuele geaardheid en vriendenkring, wordt als een schending van de privacy gezien.

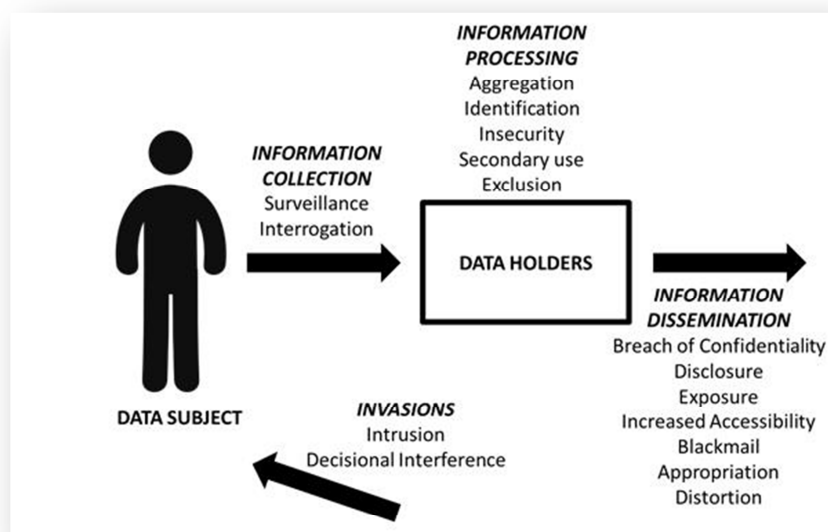
De voornoemde voorbeelden tonen aan dat privacy een breed begrip is dat meerdere facetten in zich heeft zoals toegankelijkheid van plaats en persoon, controle over informatie, geheimhouding en onafhankelijkheid. Daarnaast lijkt het cultuurafhankelijk te zijn en is bijvoorbeeld het zonder te kloppen openen van een deur in de ene cultuur een serieuze inbreuk op de privacy terwijl dit in een andere cultuur normaal wordt gevonden (Kemp & Moore, 2007). Een bekende definitie van privacy is die van Warren en Brandeis (1890) die privacy als “the right to be let alone” definieerden. Kenmerkend hierbij is dat privacy als een recht van het individu wordt gezien hetzij van morele aard of bij wet geregeld (Bélanger & Crossler, 2011). Anderen, zoals Jim Harper, betwisten dit en zien privacy veelmeer als een subjectieve conditie of beleving: “Privacy is the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and value” (Harper, 2004). De voorgaande definitie beperkt zich tot informatie over het individu zoals ook in de volgende definities van Bélanger en Crossler (2011): “Information privacy is one’s ability to control information about oneself” en; “Information privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves”. Ook de volgende definities handelen over informationele privacy: “Privacy is the condition of not having undocumented personal knowledge about one possessed by others” (Kemp & Moore, 2007) en; “Privacy is the capacity to negotiate social relationships by controlling access to personal information”³ en tot slot; “Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967).

Privacy wordt ook wel geassocieerd met vrijheid en autonomie zoals door Hirshleifer (1980) in de volgende definitie: “Privacy is autonomy within society” en; “Privacy consists of a form of autonomy over personal matters” door Kemp en Moore (2007) waarbij autonomie opgevat kan worden als de mate waarin iemand vrij is van manipulaties en invloeden van anderen. Beide definities zijn abstracter en laten veel ruimte voor eigen interpretaties bijvoorbeeld ten aanzien van de ‘personal matters’. Artikel 12 van de ‘Universele Verklaring van de Rechten van de Mens’ expliciteert dit enigszins met de volgende formulering: “No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or

³ <http://polaris.gseis.ucla.edu/pagre/landscape.html>

reputation”⁴. In deze context kan privacy als een belang van het individu worden gezien ten behoeve van een bescherming tegen ongewilde inmenging zoals ook duidelijk wordt uit de volgende definitie: “The interest of a person in sheltering his or her life from unwanted interference or public scrutiny” (Kuner, Cate, Miljard, & Svantesson, 2011). Privacy kan eveneens worden gezien als een universele morele waarde voor het beschermen van privé bezit zoals onder andere Fuchs (2012) claimt.

Een andere manier voor het definiëren van privacy is het concreet benoemen van de functie die het vervult en welke doelstellingen worden beoogd. Verschillende definities spreken daarbij over bescherming en controle zoals: “De bescherming van privacy omvat alle activiteiten en maatregelen, gericht op de regulering van de toegang tot het individu in ruimtelijke, relationele en informationele zin. Dat gaat dus verder dan de bescherming van persoonsgegevens ofwel dataprotectie” (Bloem, Doorn, Duivestein, Manen, & Ommeren, 2013). De functie van privacy volgens Posner (1981) is: “Privacy is used today in at least three senses. First, it is used to mean the concealment of information; indeed, this is its most common meaning today. Second, it is used to mean peace and quiet, as when someone complains that telephone solicitations are an invasion of his privacy. Third, it is used as a synonym for freedom and autonomy”. Het idee dat de controle over privacy bij het individu ligt, komt nadrukkelijk aan de orde in de volgende definities: “Privacy is the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate actions” (Kemp & Moore, 2007) en; “Privacy relates to material that so closely pertains to a person to his[/her] innermost thoughts, actions and relationships that he[/she] may legitimately claim the prerogative of deciding whether, with whom and under what circumstances he[/she] will share it” (Kuner, Cate, Miljard, & Svantesson, 2011).



Figuur 2. Privacy Taxonomie (Solove, 2006)

Om het concept privacy beter te begrijpen heeft Daniel J. Solove (2006) een taxonomie ontwikkeld waarbij hij zich focust op activiteiten die de privacy kunnen schenden. Privacy ziet hij daarbij als een bescherming tegen allerlei vormen van sociale spanningen en fricties waardoor mensen terughoudend zijn om betrokken te worden in voor hun waardevolle activiteiten. De taxonomie onderkent vier activiteitengroepen te weten: (1) informatie verzameling; (2) informatie verwerking; (3) informatie verspreiding; en (4) invasie. Figuur 2 bevat de schematische weergave van de taxonomie waarin ook het data subject, de data houders en de sub-activiteiten

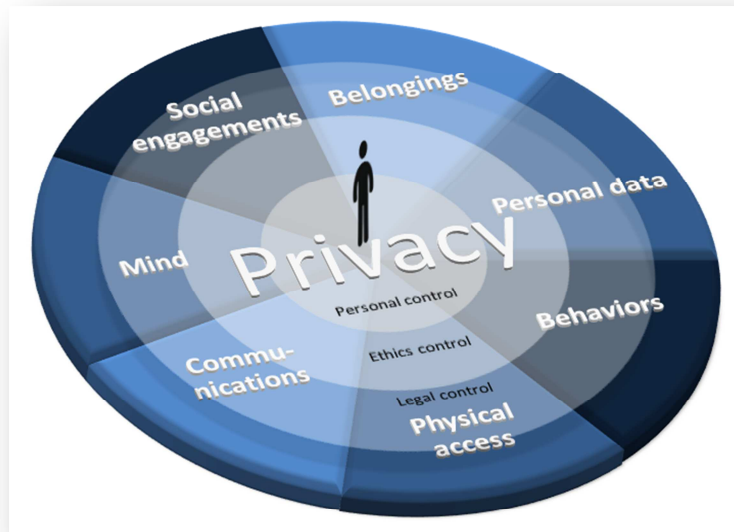
⁴ <http://www.un.org/en/documents/udhr/index.shtml#a12>

zijn weergegeven. In bijlage 2 is de taxonomie van Solove verder uitgewerkt. Het bezwaar tegen de taxonomie van Solove is dat deze zich concentreert op activiteiten die privacy kunnen schenden en de mogelijke gevolgschade daarvan. Een typologie van privacy ontbreekt echter waardoor het onvoldoende basis biedt om tot een overkoepelend concept van privacy en de bescherming daarvan te komen (Finn, Wright, & Friedewald, 2013). In een eerdere publicatie onderkende Solove (2002) wel een bepaalde typering van privacy namelijk: (1) het recht om alleen gelaten te worden; (2) beperking van de toegankelijkheid tot jezelf; (3) geheimhouding; (4) controle over persoonlijke informatie; (5) identiteit, persoonlijkheid en waardigheid; en (6) intimiteit.

Een andere indeling van privacy is van Roger Clarke die uitgaat van vier categorieën namelijk privacy van: (1) de persoon; (2) gedrag; (3) communicatie; en (4) gegevens (Finn, Wright, & Friedewald, 2013). Privacy van de persoon betreft de integriteit van het lichaam en de fysieke bescherming tegen bijvoorbeeld marteling, ongewenste medische praktijken, visitaties en surveillance. Privacy van gedrag voorkomt het ontsluiten van gevoelige en vertrouwelijke gedragingen gerelateerd aan religieuze en politieke overtuigingen maar ook seksuele voorkeuren. Privacy van communicatie voorkomt het onderscheppen en monitoren van telefoongesprekken, e-mails, internet activiteiten en 'face-to-face' contacten. Privacy van persoonlijke gegevens richt zich op de bescherming van persoonlijke informatie en gegevens. Recente technologische ontwikkelingen zoals 'body scanners', 'drones', 'radio frequency identification' (RFID), DNA en biometrie technieken, waren voor Finn et al. (2013) aanleiding om de taxonomie van Clarke uit te breiden tot zeven categorieën te weten privacy van: (1) de persoon; (2) gedrag en actie; (3) communicatie; (4) gegevens en afbeeldingen; (5) gedachten en gevoelens; (6) locatie en ruimte; en (7) sociale relaties. De eerste vier categorieën hebben een grote overlap met de indeling van Clarke alhoewel Finn et al. wel enkele aspecten hebben toegevoegd zoals acties in combinatie met gedrag, en afbeeldingen in combinatie met gegevens. Privacy van gedachten en gevoelens is het recht om deze voor jezelf te houden of alleen te delen met wie jij dat wilt. Privacy van locatie en ruimte is het recht om je anoniem te bewegen in de publieke ruimte zonder daarbij geïdentificeerd, gemonitord of getraceerd te worden. Privacy van sociale relaties is het recht om contacten te leggen en te onderhouden zonder daarbij gemonitord te worden.

In een poging om de vele classificaties, definities en typologieën van privacy te duiden, benadert Allmer (2011) privacy vanuit bestaande sociale theorieën waarbij hij een structuralistische, individualistische en integratieve benadering onderkent. De structuralistische benadering ziet privacy als een moreel en wettelijk recht dat individuen in staat stelt om de toegang tot zichzelf te limiteren ('restricted access') en te beschermen tegen ongewenste indringing. Optimale privacy in deze benadering wordt bereikt als iemand volledig onbenaderbaar is voor anderen. De individualistische benadering veronderstelt privacy als een persoonlijk belang waarbij individuen zelf bepalen wanneer, hoe en in welke mate persoonlijke informatie met anderen wordt gedeeld ('limited control'). Hoe meer controle iemand daarbij heeft, hoe meer privacy wordt genoten. De integratieve benadering ziet privacy enerzijds als een wettelijk recht dat beschermd moet worden en anderzijds als een persoonlijk belang waarover individuen zelf controle moeten kunnen uitvoeren ('restricted access & limited control').

Privacy is een multidimensionaal concept waarover in de wetenschappelijke literatuur uiteenlopende definities bestaan. Ondanks de vele pogingen om tot een universele definitie van privacy te komen, bestaat een dergelijke definitie niet. Veelal benadrukt een definitie slechts een deelaspect of worden er formuleringen gebruikt die voor meerdere uitleg vatbaar zijn. Typerend is dat voor elke definitie uitzonderingen bedacht kunnen worden waarmee de onvolledigheid van de definitie wordt aangetoond. Zo definieerden Bélanger en Crossler (2011) informationele privacy als het vermogen om informatie over jezelf te controleren (d.w.z. te beheersen). De betekenis van 'controleren' wordt echter niet uitgewerkt evenals dat onduidelijk is welke informatie wordt bedoeld.

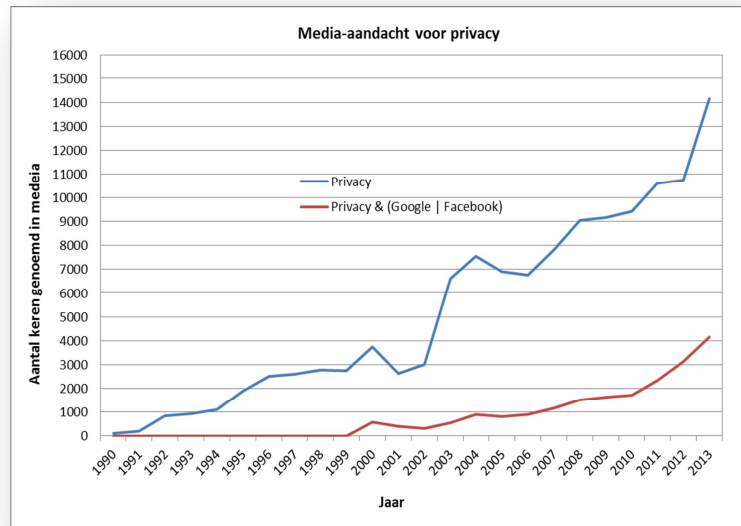


Figuur 3. Privacy Conceptualisatie

Door de verschillende definities van privacy complementair aan elkaar te beschouwen, kunnen wel enkele algemene kenmerken worden onderscheiden. Een eerste kenmerk is dat privacy een fenomeen is dat zich in een maatschappij manifesteert, immers de behoefte aan privacy zou niet bestaan als je alleen op de wereld zou zijn. Een tweede kenmerk is dat privacy betrekking heeft op 'iets' dat verweven is met een individu. Figuur 3 visualiseert op basis van de voornoemde definities en taxonomieën de verschillende domeinen van wat dat 'iets' kan zijn. Een derde kenmerk is dat dit 'iets' of delen daarvan, bescherming verdient én krijgt waarmee ongewenste indringing of ontsluiting wordt voorkomen. Het vierde kenmerk is dat deze bescherming een wettelijke, ethische of persoonlijke argumentatie heeft als reden waarom zij bestaat. Kenmerk 5 is dat privacy tijdperk-, cultuur-, context- en persoonsgebonden is, en daarmee een vloeibaar begrip is.

2.2 Relevantie van privacy

Sinds het begin van het nieuwe millennium is de aandacht voor privacy in de Nederlandse media fors toegenomen terwijl twintig jaar geleden hiervoor nog nauwelijks aandacht was zoals uit figuur 4 blijkt. De internetrevolutie, de externe dataopslag van persoonsgegevens en het ontstaan van 'social network sites' (SNS), zijn hiervoor logische redenen. Dit geeft echter geen antwoord op de vraag waarom privacy belangrijk wordt gevonden. Het was James Rachels die zich in 1975 dezelfde vraag stelde en betoogde dat er verschillende belangen zijn die door privacyschendingen geschaad kunnen worden (Rachels, 1975). Een inbreuk in iemands privacy zou bijvoorbeeld kunnen leiden tot voorkennis waardoor de competitieve positie van die persoon wordt verzwakt. Een ander belang is dat privacy aspecten van iemands leven beschermt die beter niet geweten kunnen worden. Ter illustratie hiervan citeert Rachels uit een novelle waarin een vrouw op aandringen van een ander, stiekem haar man observeert die in de huiskamer een fictief peloton soldaten commandeert. Andere voorbeelden van belangen zijn het behouden van een baan en het verkrijgen van leningen en verzekeringen zonder dat beslissingen hierover worden beïnvloed door niet-relevante (medische) persoonsgegevens. Het bijzondere karakter van deze voorbeelden is voor Rachels echter reden om ze als antwoord op zijn vraag af te wijzen omdat ze voorbijgaan aan normale, algemeen geaccepteerde en alledaagse situaties die anderen desondanks niets aangaan.



Figuur 4. Media aandacht voor privacy⁵

Het antwoord waarom privacy belangrijk is, moet volgens Rachels worden gezocht in de sociale relaties die mensen aangaan en de controle over de informatie die daarbij wordt uitgewisseld. Zo zullen vrienden onderling andere informatie uitwisselen dan patiënten met dokters. En, iemands diepste gevoelens, verlangens, ambities, problemen en frustraties zullen niet direct met een collega worden gedeeld maar veel eerder met een partner. Volgens Nissenbaum (1998) zijn mensen zich bewust van de relevantie en toepasselijkheid van informatie in dergelijke situaties. Het is de context van een situatie, transactie of relatie die bepaalt hoeveel en welke informatie wordt gedeeld. Mensen hebben daarbij een besef van contextuele integriteit waarin impliciete en expliciete normen liggen besloten (Nissenbaum, 1998). Privacy is dus belangrijk omdat het ons in staat stelt om selectief informatie te ontsluiten en gedrag te vertonen dat hoort bij de verschillende soorten sociale relaties (Rachels, 1975). Privacy is daarmee een voorwaarde voor het kunnen onderhouden van sociale relaties (Mooradian, 2009). Anders gesteld: omdat individuen in staat zijn om persoonlijke informatie achter te houden en de (fysieke) toegang tot zichzelf te verbieden, zijn ze eveneens in staat om die aan anderen te ontsluiten en zo intieme relaties te onderhouden (Reiman, 1976). Dat, ten diepste, is de reden waarom privacy volgens Rachels belangrijk is.

Alhoewel de theorie van Rachels aannemelijk klinkt, is ze niet krachtig genoeg om een universeel en absoluut antwoord te geven op de vraag waarom privacy belangrijk is. Eén van de bezwaren is dat er andere variabelen zijn waarom sociale relaties worden aangegaan zoals zorg voor de ander, affectie, vertrouwen en andere emotionele factoren. Met name de zorg voor de ander bepaalt de intensiteit en waarde van een sociale relatie ongeacht de informatie die daarbij wordt uitgewisseld (Mooradian, 2009). Een ander punt van kritiek betreft de veronderstelling dat naarmate meer persoonsgegevens openbaar komen, dit andere sociale relaties ondermijnt en uitvlakt. Zo zal een persoon de relatie met zijn vriend anders waarderen wanneer hij merkt dat zijn vriend persoonlijke, intieme informatie ook met anderen deelt. Het ontsluiten van persoonsgegevens is echter de praktijk van alle dag op 'social network sites' zoals Facebook. Het idee dat daardoor andere sociale relaties minder diepgang krijgen, gaat voorbij aan de voorwaarde dat intieme relaties de fysieke aanwezigheid van de betrokkenen vereist (Mooradian, 2009). Precies dit argument is voor anderen overigens de reden om te stellen dat SNS contacten essentiële kenmerken van vriendschap missen.

⁵ www.eur.nl/ub

Naast de voorgaande verklaringen noemt Boudewijn de Bruin (2010) enkele andere argumenten voor het belang van privacy zoals de perspectief wijziging, de menselijke waardigheid en het autonomie argument. De perspectief wijziging duidt op het ongewenste verschijnsel dat iemand in een bepaalde situatie van deelnemer in waarnemer verandert zodra hij merkt dat hij wordt geobserveerd. In lijn met deze gedachte is het al genoemde voorbeeld van de man die het fictieve peloton commandeert wat voor zijn vrouw nog nooit vertoond gedrag was. In 1881 beklagde een vrouw zich over een schending van haar waardigheid omdat een onbekende man onder het voorwenden van een valse medische identiteit, aanwezig was geweest bij de geboorte van haar kind. Het autonomie argument veronderstelt dat autonomie wordt bevorderd als je de informatie die anderen over jou hebben, kunt controleren.

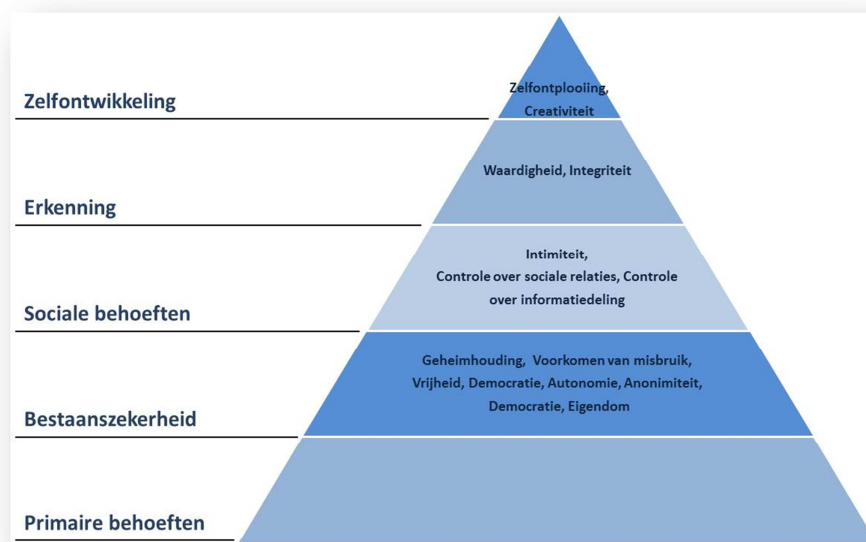
Een andere meer algemene motivatie waarom privacy belangrijk is, heeft te maken met het recht op vrijheid. De liberale kijk op vrijheid lijkt privacy echter te ondermijnen. In hun visie is privacy vooral gericht op eigenbelangen en niet de liberale waarden zoals vrijheid van mening, vrije markt en veiligheid (Bruin, 2010). Zij vinden het dan ook niet nodig om privacy als zodanig te beschermen. Dit omdat er andere mechanismes zijn (zoals wetgeving en morele waarden) die de handelingen die tot privacyschendingen leiden, veroordelen of aanpakken. Toch is deze argumentatie discutabel onder andere omdat handelingen door een collectief kunnen worden ondernomen zoals in het geval van een Koreaanse studente die, als gevolg van de massale verontwaardiging voor het feit dat zij de uitwerpselen van haar hond niet had opgeruimd, zich gedwongen zag om de universiteit te verlaten. Haar negatieve vrijheid, ofwel de mate waarin zij vrij was van de invloeden van anderen, werd hierdoor beperkt. Ook goedgelovigheid, generaliseren en vooroordelen, kunnen bepaalde handelingen uitlokken en bevorderen waarmee de negatieve vrijheid wordt beperkt. Een voorbeeld hiervan is de vermeende uitspraak van Tommy Hilfiger waarin hij zegt dat hij kleding minder mooi ontworpen zou hebben als hij vooraf had geweten dat het zou worden gekocht door onder andere Aziaten en Joden. Alhoewel het om een vals gerucht ging, werd het door velen geloofd en waren de kosten voor het bedrijf aanzienlijk.

Een veel gehoord argument waarmee het belang van privacy wordt ondermijnd, is dat men 'niets te verbergen' heeft waardoor men bijvoorbeeld geen moeite heeft met camera's op straat en het aftappen van telefoongesprekken en e-mails. De onderliggende aanname hierbij is dat privacy bedoeld is om 'bad things' te verbergen (Solove, 2008). De onuitputtelijke mogelijkheden om data te verzamelen, te aggregeren en te interpreteren, betekent echter dat individuen de controle over wat anderen van hen weten, verliezen. Zo werd een vader in Amerika onaangenaam verrast door de zwangerschap van zijn tienerdochter. Op basis van haar koopgedrag voorspelde een bedrijf haar zwangerschap en had haar daarop afgestemde reclames gestuurd (Bloem, Doorn, Duivesteyn, Manen, & Ommeren, 2013). Dat je niets te verbergen hebt is ook moeilijk voorstelbaar als je vanwege incontinentieproblemen luiers moet dragen en dit bij het inchecken voor een vlucht door een bodyscanner of fysieke foullering wordt geconstateerd (Bird, 2013). Al verschillende malen heeft dit geleid tot vernederende situaties waarbij medewerkers van TSA meenden deze constatering luidkeels met anderen te moeten delen.⁶ Goold (2009) koppelt privacy aan autonomie, waardigheid maar ook aan een florerende en robuuste democratie. Die kan alleen worden gerealiseerd als burgers vrijheid van meningsuiting hebben en naar eigen keuze sociale relaties kunnen aangaan. Privacy heeft daarmee een politieke waarde omdat het de condities schept waaronder een democratie kan functioneren.

Het voorgaande maakt duidelijk dat privacy om uiteenlopende redenen belangrijk wordt gevonden gerelateerd aan autonomie, geheimhouding, waardigheid, integriteit, controle over sociale relaties, voorkomen van misbruik, intimiteit, eigendom, controle over informatiedeling, vrijheid, anonimiteit, zelfontplooiing en democratie. In deze aspecten kan een zekere hiërarchie worden onderkend zoals ook in de behoeftepiramide van Maslow. Maslow (1943) ontwikkelde een theorie voor de graduele ontwikkeling van motivatie bij individuen. Motivatie op een bepaald niveau wordt pas actueel zodra de behoeften van alle onderliggende

⁶ <http://www.infowars.com/hes-wearing-a-diaper-tsa-agent-humiliates-cancer-victim/>

niveaus zijn bevredigd. Zo zal iemand pas behoefte hebben aan sociale relaties als de primaire behoeften (voedsel, kleding, onderdak, hygiëne) en de bestaanszekerheid behoeften (veiligheid, bescherming) zijn ingevuld. Alhoewel de theorie van Maslow wereldwijde faam heeft verkregen, is weinig wetenschappelijk onderzoek bekend wat deze theorie ondersteunt. Gekeken naar privacy lijkt dit een behoefte op het niveau van bestaanszekerheid te zijn. De werking van privacy is nadrukkelijk ook op de andere niveaus terug te vinden (figuur 5) alwaar het de condities schept voor de bevrediging van de daar geldende behoeften.



Figuur 5. Behoeftepiramide (Maslow, 1943)

Privacy in het algemeen biedt individuen een ‘veilige haven’ waarin zij vrij zijn van indringing in de persoonlijke levenssfeer door anderen. Deze omstandigheden stelt ze in staat om invulling te geven aan een eigen levenswijze en de daarvoor benodigde condities te controleren (Nissenbaum, 1998).

2.3 Belangenorganisaties

Rondom de behartiging van privacy belangen van individuen, springen de hierna genoemde organisaties het meest in het oog.

2.3.1 College bescherming persoonsgegevens (CBP)

“Iedereen moet erop kunnen rekenen dat met de persoonsgegevens die hij - al dan niet bewust - afgeeft aan overheden en bedrijven, zorgvuldig wordt omgegaan” (CBP, 2014). Het CBP is een Nederlands orgaan dat ressorteert onder het ministerie van veiligheid en justitie en toeziet op de naleving van de Wet bescherming persoonsgegevens (Wbp). De motivatie voor het oprichten van het CBP voert terug naar 28 januari 1981, de dag waarop het ‘Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens’ door de leden van de Raad van Europa (RvE) werd ondertekend. De aanleiding hiervoor was het toenemende, grensoverschrijdende verkeer van persoonsgegevens en als gevolg daarvan de behoefte om de fundamentele rechten, vrijheden en eerbiediging van de persoonlijke levenssfeer van natuurlijke personen te beschermen. De RvE, die mede door Nederland in 1949 werd opgericht, ziet met haar 47 leden toe op de bescherming van de mensenrechten en dient als zodanig niet verward te worden met de Europese Unie. In lijn met het genoemde verdrag, bracht het Europees Parlement en de Raad van de Europese Unie op 23 november 1995 een richtlijn uit (nr. 95/46/EG) voor de bescherming van persoonsgegevens en regulering van het verkeer van die gegevens. Dit leidde ertoe dat op 6 juli 2000, de Wbp in werking trad waarbij in artikel 51 de instelling

van het CBP wordt verordend als toezichthoudend instituut op de verwerking van persoonsgegevens overeenkomstig diezelfde wet. De formele taken van het CBP worden in bijlage 3 toegelicht.

Zoals uit haar jaarverslagen blijkt, is het CBP in 2012 en 2013 regelmatig betrokken geweest in dossiers waarbij er sprake was van privacyschendingen. Zo werd een werkgever ten aanzien van ziekmeldingen gewezen op onrechtmatig handelen door te vragen naar de aard en oorzaak van de ziekte. Een andere interventie betrof de beëindiging van het verzamelen van kijkgedrag gegevens ten behoeve van gepersonaliseerde advertenties op smart tv's. Naast deze voorbeelden beschrijven beide jaarverslagen vele andere privacy casussen in de gezondheidszorg, rondom arbeidsrelaties, internet en Telecom, handel en diensten, overheid, politie en justitie. De verankering van privacy in wetten is voor het CBP leidend bij de uitvoering van haar werkzaamheden. Het CBP ziet privacy dan ook als een grondrecht. Daar waar er niet zorgvuldig met persoonsgegevens wordt omgegaan en die als commodity worden verhandeld, dreigt de mogelijkheid om onbespied te kunnen leven te verdwijnen. "Daarom moet bij het benaderen van privacy als economische waarde, de bescherming ervan goed in ogenschouw worden genomen"⁷.

2.3.2 DDMA

De "DDMA (Dutch Dialogue Marketing Association) is de branchevereniging voor adverteerders en dienstverleners die in hun dagelijkse werkzaamheden de dialoog aangaan met hun (potentiële) klanten via data driven marketing"⁸. De DDMA ondersteunt en adviseert haar leden rondom privacy kwesties en behartigt hun belangen bij privacy dossiers in Den Haag en Brussel. De DDMA streeft naar zelfregulering van de branche. Bedrijven die zijn aangesloten bij de DDMA kunnen het Privacy Waarborg keurmerk voeren waarmee zij: (1) zekerheid hebben dat hun marketing voldoet aan de geldende privacy regels; (2) dit zichtbaar kunnen uitdragen; (3) verzekerd zijn van gratis juridisch advies bij privacy vraagstukken; en (4) recht hebben op kosteloze afhandeling van geschillen tussen consumenten en bedrijven. De DDMA pretendeert zichzelf extra strenge regels te hebben opgelegd die verder gaan dan de wettelijke verplichtingen onder meer om daarmee antwoord te geven op onbehagen in de samenleving. "De groeiende hoeveelheid data die organisaties en overheid van de burger verzamelen, leidt tot maatschappelijk onbehagen. Burgers zien door de bomen het bos niet meer en hebben het gevoel de controle over hun eigen gegevens te verliezen. Voor marketeers is het belangrijk open en duidelijk te zijn over welke gegevens worden verzameld en hoe gegevens worden gebruikt"⁹.

2.3.3 Nederlandse Vereniging voor Personeelsbeleid

Rondom de werving en selectie ter vervulling van vacatures bestaat in Nederland de NVP-sollicitatiecode. Deze code bevat basisregels die ondernemingen naar het oordeel van de Nederlandse Vereniging voor Personeelsbeleid (NVP) in acht behoren te nemen waarbij sollicitanten recht hebben op: (1) een eerlijke kans op aanstelling; (2) deugdelijke informatie en doelbinding; (3) privacy; (4) een vertrouwelijke behandeling van je persoonlijke gegevens; (5) een doelmatige sollicitatieprocedure; en (6) toegang tot een geschillenregeling.¹⁰ Met het onderschrijven van deze code geven ondernemingen uiting aan hun intenties om de privacy belangen van sollicitanten te beschermen.

2.3.4 Artikel 29-werkgroep

'De Artikel 29-werkgroep ('Working Party 29', kortweg WP29) is een onafhankelijk, raadgevend orgaan dat bestaat uit vertegenwoordigers van de nationale privacy toezichthouders in de Europese Unie' (CBP, 2012). In die hoedanigheid houdt het zich bezig met de bescherming van persoonsgegevens en levert de werkgroep een

⁷ <http://ddma.nl/privacy/privacy-waard-cbp-consumentenbond-vvd-ddma-debat/>

⁸ <https://ddma.nl/wat-doet-ddma/>

⁹ <http://ddma.nl/vereniging-ddma/visie/>

¹⁰ <http://www.nvp-plaza.nl/site/nl/kennis.phtml?p=sollicitatiecode>

bijdrage aan de ontwikkeling van Europese normen en gemeenschappelijke interpretaties rondom de bescherming van persoonsgegevens. De wijze waarop de werkgroep zich uitlaat over privacy kwesties, is door het formuleren van zogenaamde opinies. Zo werden in 2013 opinies aangenomen over doelbinding en 'slimme' grenzen (CBP, 2014). De doelbinding opinie houdt in dat persoonsgegevens die voor een bepaald doel zijn verzameld, niet opeens voor een geheel ander doel mogen worden gebruikt. De tweede opinie is een kritische reactie op voorstellen van de Europese Commissie voor het aanleggen van een omvangrijke database met daarin de aankomst- en vertrekgegevens van niet-EU-burgers die voor een kort verblijf tot het Schengengebied zijn toegelaten.

2.3.5 Global Privacy Enforcement Network

Dit informele netwerk gaat uit van de OECD ('Organisation for Economic Co-operation and Development') en richt zich op het bevorderen van grensoverschrijdende samenwerking inzake privacywetgeving. In 2007 is dit initiatief gestart vooral vanwege de toename van de internationale data stromen en de daarbij optredende risico's voor individuen.

2.4 Conclusie

In dit hoofdstuk is gezocht naar een beschrijving van het concept privacy (deelvraag 1). Ten aanzien van privacy blijken er geen scherpe scheidslijnen getrokken te kunnen worden waarlangs dit concept gedefinieerd kan worden. Privacy is een multidimensionaal begrip waaraan vanuit diverse perspectieven verschillende interpretaties gegeven kunnen worden. Voor overheden betekent dit dat privacywetgeving expliciet geformuleerd dient te worden; een verbod op privacyschendingen alleen is niet voldoende en zal vergezeld moeten gaan met een specificering van welke handelingen als privacyschending worden gezien. Hetzelfde is van toepassing op andere wetgeving rondom privacy rechten en plichten. Daar waar dat niet of onvoldoende gebeurt, ontstaat speelruimte voor de betrokkenen om de eigen belangen te verdedigen. Door burgers kan deze speelruimte worden gebruikt voor onrechtmatige praktijken zoals het achter de voordeur onderdrukken van vrouwen, het plegen van fraude en andere veiligheidsbedreigende handelingen. Ondernemingen kunnen de speelruimte gebruiken om met zogenaamde 'privacy invasive' strategieën de voor hun relevante informatie te verkrijgen. Dat privacy een diffuus begrip is waaraan uiteenlopende interpretaties gegeven kunnen worden, betekent dat reacties van stakeholders op privacy gerelateerde voornemens moeilijk te voorspellen zijn. Daarnaast lijken er geen algemeen geaccepteerde criteria te bestaan op basis waarvan een rationele keuze vóór of tegen privacy kan worden gemaakt. Wat de één als een privacyschending ziet, is voor de ander geen probleem. Ondernemingen dienen zich bewust te zijn van deze (soms) tegenstrijdige interpretaties en emoties teneinde risico's op imago schade te verkleinen en affaires zoals bij ING¹¹ te voorkomen.

¹¹ Zie hoofdstuk 1

3 WAT STAAT ER OP HET SPEL

In dit hoofdstuk zal vanuit verschillende perspectieven worden ingegaan op de trade-off's die rondom het concept privacy onderkend kunnen worden. Vervolgens zal worden nagegaan hoe vertegenwoordigers van de oude en nieuwe economie in hun business modellen rekening houden met de tegenstellingen rondom deze trade-off's.

3.1 Privacy trade-off's

Een trade-off betekent in het algemeen het bestaan van tegengestelde belangen waarbij de winst voor de één het verlies voor de ander betekent (Tulder R. v., 2011). In dat geval wordt er een 'zero-sum' uitkomst gerealiseerd maar ook een 'negative-sum' uitkomst is mogelijk. Mede vanwege het ontbreken van een universele definitie van privacy, hebben belanghebbenden ruimte om trade-off's vanuit eigen zienswijzen te beoordelen en te waarderen. Vanuit een juridisch perspectief bestaat verschil van mening of privacy als een recht beschermd dient te worden (Goold, 2009). Vanuit een sociaal perspectief kan de vraag worden gesteld welke belangen zwaarder dienen te wegen, die van het individu of die van het collectief? De beoordeling van de trade-off vanuit een economisch perspectief is een kosten-batenanalyse waarbij alle betrokken de voordelen afwegen tegen de kosten. Ook kan worden gedacht aan een ethisch perspectief waarbij normen en waarden vanuit verschillende culturen en religies de keuze voor meer of minder privacy beïnvloeden. Daarnaast spelen persoonlijke opvattingen een rol bij het maken van keuzes en het afwegen van belangen. Ten aanzien van privacy zijn het altijd belangen van individuen die worden afgewogen tegen andere belangen van hetzij diezelfde individuen of belangen van de overheid, markt of maatschappij. Voor elk van deze partijen kunnen verschillende trade-off's worden onderkend hetzij vanuit een institutionele verantwoordelijkheid of overwegingen van sociaal-maatschappelijke of economische aard.

3.1.1 Rol van de overheid

De bedreiging van privacy door overheden vindt plaats op drie verschillende manieren (Harper, 2004). De eerste bedreiging komt voort uit de uitdijende databases met persoonsgegevens waarop willekeurige observaties mogelijk zijn. De tweede bedreiging is het systematisch verzamelen, analyseren en delen van gegevens van burgers voor administratieve doeleinden. De derde bedreiging betreft een gerichte anti-privacy wet- en regelgeving ter voorkoming dat de toegang tot individuen wordt afgesloten. Voorbeelden hiervan zijn het verbieden van dataencryptie in de privésfeer en het voorschrijven van tracking functionaliteit in mobiele apparaten zodat deze gelokaliseerd kunnen worden. Door deze ondermijning verkrijgt de overheid informatie over personen zonder hun nadrukkelijke toestemming. Dat zij dat niet zonder reden doet, wordt duidelijk uit de volgende trade-off's.

Privacy versus veiligheid

Veiligheid valt onder de verantwoordelijkheid van de overheid. Dit betreft bescherming tegen krachten die de staat van buitenaf bedreigen maar ook binnenlandse bedreigingen die de persoonlijke levenssfeer van burgers raken, vallen hieronder. Veiligheid richt zich tegen alles wat ontwrichtend kan zijn en wordt dermate belangrijk gevonden dat desnoods niet-normale middelen gebruikt mogen worden als het wordt bedreigd (Muller, Kummeling, & Bron, 2007). Veiligheid is daarmee een breed begrip "dat betrekking heeft op de adequate bescherming tegen onrechtmatige of disproportionele inbreuken op lijf, eerbaarheid en goed" (Muller, Kummeling, & Bron, 2007). Veiligheid ofwel veilig zijn, impliceert het vrij zijn van risico's en gevaren (Lieshout, Friedewald, Wright, & Gutwirth, 2013). De trade-off tussen privacy en veiligheid wordt doorgaans geassocieerd met het balanceren tussen de bescherming van de privacy rechten van burgers en de bestrijding van terreur, criminaliteit, fraude en illegaliteit. De aanslag van 11 september (2001) en de bomaanslagen in Madrid (2004) en London (2005), waren bijvoorbeeld voor politici in de VS, UK en EU, aanleiding om rondom veiligheid extra maatregelen te nemen zoals cameratoezicht, langere bewaarplicht van digitale gegevens en het aftappen van spraak- en dataverkeer. Daar waar van politici wordt verwacht dat zij zorgdragen voor een veilige samenleving,

wordt tegelijkertijd van hen verwacht dat ze fundamentele rechten beschermen waaronder het recht op privacy. Dit lijkt onverenigbaar met elkaar hetgeen mogelijk wordt veroorzaakt doordat beide concepten - privacy en veiligheid - onvoldoende concreet worden geïnterpreteerd en ze in deze trade-off alleen in verband worden gebracht met technologieën die veiligheid stimuleren maar privacy ondermijnen (Lieshout, Friedewald, Wright, & Gutwirth, 2013). Veiligheid is eveneens gerelateerd aan de bestrijding van terreur en misdaad; naarmate de overheid meer en meer indringt in de levens van individuen, zal zij effectiever zijn in de bestrijding hiervan. Zo stond burgemeester Opstelten van Rotterdam in 2005 toe dat er preventief werd gefouilleerd, cameratoezicht werd toegepast en informatie werd uitgewisseld, teneinde de 700 meest overlastgevende personen in de stad aan te pakken (Muller, Kummeling, & Bron, 2007).

Privacy versus fraudebestrijding

In deze trade-off richt de overheid zich op het verkrijgen van gegevens ten behoeve van het detecteren van fraude. Bij fraude worden zaken bewust anders voorgesteld dan ze in werkelijkheid zijn teneinde daarmee eigen voordelen te realiseren. Fraude komt in veel vormen voor waaronder belastingfraude, uitkeringsfraude, diplomafraude, plagiaat en bouwfraude. Ter voorkoming van fraude zal de overheid proberen om zoveel mogelijk relevante informatie te verzamelen op basis waarvan fraude of vermoedens daarvan kunnen worden vastgesteld. Ook het delen van deze informatie met derden kan voorkomen zoals bleek uit de aanpak van het scheefwonen waarover in 2012 een wetsvoorstel werd aangenomen. In dit voorstel werd geregeld dat huurders met een te hoog inkomen, een extra huurverhoging van maximaal vijf procent zou worden opgelegd. Vooruitlopend hierop bleek de belastingdienst al inkomensgegevens te hebben verstrekt aan verhuurders zonder daarvoor toestemming te hebben gevraagd of gekregen van de huurders in kwestie. De zaak werd juridisch aangevochten met als resultaat dat de belastingdienst stopte met het verstrekken van deze gegevens (CBP, 2012).

Privacy versus kapitaal

De vraag in deze trade-off is in hoeverre privacy belangen van burgers opgeofferd kunnen worden ten behoeve van marktstimulering en kapitaalvermeerdering. In de visie van Fuchs (2012) wordt privacy in een kapitalistische samenleving voortdurend door de overheid en bedrijven ondermijnd ten behoeve van kapitaalvermeerdering. Fuchs ziet privacy als een antagonistische waarde die enerzijds is gericht op de bescherming van bezit maar anderzijds door voortdurende observatie wordt bedreigd. Enerzijds is er dus de druk vanuit de markt om privacy minimaal te reguleren maar anderzijds vraagt de burger om maximale bescherming. Daar waar de overheid niet in staat is om vanwege conflicterende belangen regulerend op te treden, ontstaat een institutioneel gat waarvan door anderen gebruik kan worden gemaakt. Een argument voor het zwaarder laten wegen van economische belangen is dat economische groei in het algemeen ook de persoonlijke welvaart bevordert. Dit betekent dat er concessies aan privacy moeten worden gedaan zodra dit de economische groei frustreert (Kemp & Moore, 2007).

3.1.2 Sociaal-maatschappelijke belangen

Vanuit een sociaal-maatschappelijk perspectief kunnen verschillende rechten, normen, fundamentele waarden, sociale verplichtingen en verantwoordelijkheden worden onderkend waarvan de belangen kunnen conflicteren met de privacy belangen van individuen.

Mensenrecht versus commodity

De verleidingen voor ondernemingen om persoonsgegevens te verwerken zijn groot: informatie betekent zowel geld als macht (Prins, 2006). Een visie op privacy is dat het als een persoonlijk bezit wordt gezien. Aanhangers van deze gedachte kennen persoonsgegevens commerciële waarde toe en om die reden moet individuen het recht op privacy als persoonlijk bezit worden toegekend. Vanuit een economisch perspectief kan privacy als een 'social cost' worden gezien waarbij de actie van een partij een negatieve externaliteit creëert voor een andere partij. Anders gesteld: als een onderneming iets doet heeft dat een negatieve impact op iemand anders. De technologische voortuitgang waardoor ondernemingen relatief goedkoop aan

persoonsgegevens kunnen komen en de hoge kosten voor individuen om zich te beschermen tegen het verzamelen van deze gegevens door ondernemingen, zorgen ervoor dat informatie lichtvaardig wordt ontsloten (Prins, 2006). Voor mensen die persoonsgegevens als bezit zien, is bescherming van dit recht daarom noodzakelijk. Andere voordelen van het behandelen van privacy als persoonlijk bezit zijn volgens Prins (2006): (1) de (immateriële) kosten van informatieverzameling zullen verschuiven naar de ondernemingen en niet meer op burgers drukken; en (2) ondernemingen zullen meer respect tonen voor de menselijke waardigheid. Een andere visie op privacy is dat dit als een onvervreemdbaar mensenrecht wordt gezien. Deze gedachte plaatst privacy op gelijke hoogte met andere waarden als vrijheid, gelijkheid, democratie en respect. Privacy heeft zo gezien geen commerciële waarde maar is onderdeel van het morele waardensysteem. In deze visie kan van burgers niet worden verwacht dat zij in staat zijn om juiste beslissingen te nemen omtrent het opgeven van privacy in ruil voor bepaalde voordelen.

Privacy versus vrijheid

Een zienswijze op vrijheid kan zijn dat je kunt doen en laten wat je wilt. In deze interpretatie bestaan er geen beperkingen waardoor dit doen of laten wordt beïnvloed. Een dergelijke perceptie van vrijheid is onvoorstelbaar en zou leiden tot chaos en anarchie. In die zin bestaat absolute vrijheid niet en gelden er geschreven en ongeschreven wetten en regels waaraan burgers in een maatschappij zich dienen te houden. In deze wetten worden wel bepaalde vrijheden geregeld bijvoorbeeld de vrijheid van meningsuiting, vrijheid van godsdienst, vrijheid van onderwijs, persvrijheid en keuzevrijheid. Met betrekking tot vrijheid kan onderscheid worden gemaakt in negatieve en positieve vrijheid. Negatieve vrijheid is de mate waarin je vrij bent van invloeden van anderen terwijl bij positieve vrijheid een dergelijke invloed ontbreekt. Negatieve vrijheid in abstracte bewoordingen is: “the 'pure negative' concept of freedom according to which I am unfree to perform some action, A, if someone interferes with my performance of A or if someone has the disposition to interfere with my performance of A if I were to attempt to perform A” (Bruin, 2010). Zo wordt iemands negatieve vrijheid beperkt als hij onderweg naar huis, wordt opgehouden door een politieblokkade. Ook de mate waarin persoonlijke informatie publiekelijk beschikbaar is, of als het ontbreekt aan inzicht wie welke informatie heeft, kan dat de negatieve vrijheid beperken. Een voorbeeld hiervan is de bankier die illegaal toegang kreeg tot de medische gegevens van zijn klanten en hen die aan kanker leden, dwong om hun lening af te betalen (Bruin, 2010). De trade-off tussen privacy en vrijheid is de voortdurende afweging tussen het ontsluiten van persoonsgegevens en de mogelijke consequenties daarvan op de negatieve vrijheid. Des te strikter de privacy wordt beschermd, des te kleiner zal de kans op een beperking van de negatieve vrijheid zijn. Anderzijds geldt ook dat met het beperken van fundamentele vrijheden, de privacy wordt beperkt. In ‘1984’ (Orwell, 1949) wordt dit werkelijkheid en bestaat vrijheid niet, evenmin als privacy en worden burgers tot zelfs in de eigen huiskamer geobserveerd.

Privacy versus gelijke behandeling

Het recht op privacy biedt de mogelijkheid te volharden in praktijken die ongewenst of zelfs verboden zijn. Verschillende feministische wetenschappers bekritiseren privacy bijvoorbeeld omdat het bepaalde misstanden in de privésfeer in stand houdt zoals onderdrukking, misbruik en geweld. Achter de muur van privacy blijven de machtsrelaties onzichtbaar die de ongelijkheid tussen man en vrouw laten voortduren (Kemp & Moore, 2007).

Privacy versus sociale verantwoordelijkheid

Mensen kunnen lijden aan verschijnselen die ze zelf niet onder controle hebben zoals alcohol-, drugs- en gokverslaving. Ook kan er sprake zijn van een buitensporig uitgavenpatroon, zelfverwaarlozing of andere schadelijke zaken waardoor een ‘normaal’ leven niet mogelijk is. De vraag in deze trade-off is in hoeverre ongevraagde inmenging in het leven van deze mensen toegestaan is teneinde ze uit hun misère te helpen.

Privacy versus opvoeding

In het leven van kinderen spelen zich veel zaken af die verborgen zijn voor hun ouders. De vraag in deze trade-off is in hoeverre ouders zich toegang tot deze verborgen zaken verschaffen waardoor zij de opvoedingstaak

adequaat kunnen vervullen. Zo kunnen activiteiten op ‘social network sites’ leiden tot schadelijke contacten zonder dat een kind zich dit realiseert. Of, voortdurend inzicht in de schoolprestaties kan nodig zijn om controle te houden over de voortgang van een studie.

Privacy versus eenzaamheid

Daar waar privacy vanuit verschillende perspectieven kan worden bekeken zoals een juridisch, sociaal-maatschappelijk, economisch en ethisch perspectief, geldt dat in mindere mate voor eenzaamheid. Het spreken over het ‘recht op eenzaamheid’ of een ‘kosten-batenanalyse van eenzaamheid’ ligt niet voor de hand. Veel eerder is eenzaamheid een emotie die zich in individuen manifesteert als gevolg van het niet betrokken zijn in waardevolle sociale relaties (Franklin, 2009). Ten aanzien van deze sociale relaties is er sinds jaren 60 uit de vorige eeuw een verandering waar te nemen waarbij de aard van de relatie eerder is gebaseerd op plezier en voordeel voor het individu dan op liefde, afhankelijkheid en betrokkenheid voor elkaar (Franklin, 2009). Sociale relaties lijken dus oppervlakkiger te worden en het aantal eenpersoonshuishoudens is hiervoor indicatief evenals het gegeven dat het aantal huisdieren in functie van gezelschap toeneemt. Een trade-off tussen privacy en eenzaamheid impliceert dat er een samenhang tussen beide concepten is die zich volgens een vast patroon manifesteert. Zo lijkt het logisch om te veronderstellen dat naarmate meer privacy wordt opgeëist, dit de kans op eenzaamheid doet toenemen. Het opgeven van privacy zou logischerwijs leiden tot minder eenzaamheid omdat het de toegang tot het individu vergemakkelijkt. Uit onderzoek blijkt echter dat niet de kwantiteit, maar veelmeer de kwaliteit van relaties bepalend is of gevoelens van eenzaamheid optreden (Franklin, 2009). Zo kunnen individuen zich in een relatie met bloedverwanten of een partner toch eenzaam voelen terwijl anderen een gelukkig solitair leven kunnen leiden. Een ander bezwaar betreft het verschijnsel dat als ‘social network’ relaties dominant worden, dit samenhangt met meer eenzaamheid (Coget, Yamauchie, & Suman, 2002). Anders gesteld: ondanks dat individuen meer persoonsgegevens online beschikbaar stellen en daarmee hun privacy verminderen, leidt dit niet tot minder maar tot meer eenzaamheid. Een verklaring hiervoor is dat ‘social network’ relaties in een netwerksamenleving weliswaar snel en efficiënt tot stand komen, maar in het algemeen niet leiden tot hechte banden.

Privacy versus gezondheid

Een voorbeeld van deze trade-off is de verstrekking van zoveel mogelijk relevante medische gegevens zoals achtergrond, leefgewoontes en erfelijkheid, teneinde de juiste behandeling te kunnen adviseren. Daarnaast biedt informatie over het ziekteverloop mogelijkheden voor het zoeken naar en verbeteren van behandelmogelijkheden.

Controle versus gemak

In deze trade-off wordt de mate waarin individuen controle hebben over de eigen persoonsgegevens, afgewogen tegen meer of minder gemak. Een voorbeeld is de noodzakelijke toestemming voor het gebruik van internet cookies. Alhoewel dit gebruikers meer controle geeft, zullen velen het hinderlijk vinden dat bij website bezoeken akkoord voor het toepassen van cookies moet worden gegeven.

Privacy versus empowerment

De Arabische lente van 2011 inclusief de ‘Facebook revolutie’, toont volgens sommigen aan hoe ‘social networks’ politieke veranderingen kunnen bewerkstelligen (Swire, 2012). De ‘Facebook revolutie’ is daarbij de metafoor voor de verdrijving van de Egyptische president Mubarak waarbij burgers via Facebook werden gemobiliseerd onder meer met verwijzingen naar protestacties en adviezen voor het verwijderen van traangas.¹² In maart 2014 blokkeerde de Turkse president Erdogan de websites van Twitter en Youtube¹³; via deze sites zouden geluidsbanden zijn gelekt met daarop gesprekken van regeringsfunctionarissen maar ook van Erdogan zelf. Een derde voorbeeld waarin ‘social network sites’ (SNS’s) een politiek doel dienden, was de

¹² <http://www.heritage.org/events/2011/02/facebook-revolution>

¹³ <http://www.nrc.nl/nieuws/2014/03/28/erdogan-blokkeert-twitter-en-youtube-in-turkije-wat-zit-erachter/>

campagne van Obama voor de presidentsverkiezing in 2008. Met hulp van Facebook's medeoprichter Chris Hughes, werd volop gebruik gemaakt van de 'nieuwe media' voor het mobiliseren van supporters en binnenhalen van donaties (Swire, 2012). De voorbeelden tonen aan dat SNS's een katalyserend effect kunnen hebben op politieke en maatschappelijke ontwikkelingen en tendensen. Een 'posting' op een website heeft blijkbaar de potentie om veranderingen af te dwingen en geeft individuen een zekere vorm van macht die voorheen voor hen onbereikbaar was. De keerzijde is wel dat je je identiteit daarbij prijsgeeft en wordt blootgesteld aan mogelijke risico's. Volgens Swire (2012) gaat het daarbij ten diepste om het volgende spanningsveld: "A basic tension exists between information sharing, which can promote the freedom of association, and limits on information sharing, notably for privacy protection".

3.1.3 Economische belangen

Evenals de overheid wil ook de markt beschikken over relevante informatie over personen zodat zij optimaal kan functioneren. Inzicht in de demografische samenstelling stelt bedrijven in staat om de behoefte aan producten en diensten in te schatten. Anderzijds biedt inzicht in iemands gedrag en voorkeuren, bedrijven de mogelijkheid om hun presentatie daarop af te stemmen.

Privaat versus publiek

Rondom privacy zijn twee verschillende markten te onderscheiden te weten de markt voor persoonsgegevens en de markt voor privacy. De eerste richt zich op het verhandelen van persoonsgegevens en de laatste op producten en diensten voor het beschermen van persoonsgegevens. Alhoewel beide markten aan elkaar zijn gerelateerd, betreft het toch verschillende markten. Persoonsgegevens die worden verhandeld worden: (1) in het publieke domein gebracht; (2) gelden als ruilmiddel in transacties; en (3) kunnen leiden tot negatieve externaliteiten voor individuen. De markt voor privacy beoogt juist dat persoonsgegevens privé blijven en dientengevolge kunnen deze gegevens geen ruilmiddel zijn.

Privacy versus efficiëntie

Privacy kan resulteren in informatie asymmetrie. Van informatie asymmetrie is sprake als in een economische transactie de ene partij meer of betere informatie heeft dan de tegenpartij waardoor er een onbalans in de machtsverhoudingen optreedt (PRESCIENT, 2011). Zo zouden banken op basis van medische gegevens risicoleningen kunnen identificeren en klanten dwingen de financiële positie te verbeteren. Het eventueel ontsluiten van informatie over de gezondheid, leefgewoonten, normen en waarden van (kandidaat) werknemers, stelt bedrijven in staat om mogelijke bedrijfsrisico's vast te stellen en deze mee te wegen in beslissingen rondom promotie, demotie, aanname, compensatie en opleiding. Vaak worden er twee vormen van informatie asymmetrie onderscheiden te weten 'adverse selection' en 'moral hazard'. Een bekend voorbeeld van 'adverse selection' is een particulier die zijn auto wil verkopen op de tweedehands automarkt. De verkoper weet wat de kwaliteit van de auto is op basis van het gebruik en onderhoud. Aan de hand daarvan zal de verkoper een reële prijs willen hebben echter de koper heeft deze informatie niet en veronderstelt een slechtere kwaliteit. Op die manier ontstaat een suboptimale transactie waarbij een prijs wordt gevonden die tussen de vraag- en biedprijs in ligt. Dit betekent dat er teveel wordt betaald bij een slechte kwaliteit maar te weinig als er sprake is van een goede kwaliteit. 'Moral hazard' is het verschijnsel dat optreedt als mensen niet verantwoordelijk worden gehouden voor hun beslissingen en handelen. In het besef dat er een vangnet is voor mogelijke risico's, wordt er geen verantwoordelijkheid genomen om zelf die risico's af te dekken. Naarmate individuen meer persoonsgegevens ontsluiten, zijn zij minder in staat om te weten welke partijen hun gegevens gebruiken. Deze onzekerheid creëert een negatieve externaliteit voor het individu en verzwakt diens machtspositie.

Privacy versus transactiekosten

Voor het uitvoeren van de activiteiten waarmee ondernemingen hun waardepropositie realiseren, zijn mensen en middelen nodig. Ten aanzien van de organisatie van mensen kunnen er privacy belangen worden onderscheiden gerelateerd aan de toegang tot informatie over medewerkers en sollicitanten. De argumenten van

voorstanders van het beschermen van deze belangen worden gekenmerkt door onwelwillendheid ten aanzien van onderzoek naar de subjectiviteit van (potentiële) medewerkers (Nye, 2002). Volgens hen is de 'commerciële' relatie tussen werkgevers en werknemers geen excuus voor een ongelimiteerde toegang tot de persoonlijke levenssfeer. Dit betekent dat alleen feitelijke gegevens zoals opleiding, werkervaring, resultaten van competentietesten en rollenspellen, referenties en interviews legitieme middelen zijn voor het verkrijgen van inzicht in de profielen van (kandidaat) medewerkers. Informatie over levensstijl, genetische kenmerken, levensovertuigingen en aanleg voor ziekten, dienen hiervan uitgesloten te worden. De argumentatie hiervoor is gebaseerd op een ethisch waardesysteem waarbij informationele privacy individuen in staat stelt om: (1) een eigen identiteit te ontwikkelen; (2) autonoom te zijn in gedragingen; en (3) onderdeel te zijn van bepaalde sociale groepen in de maatschappij (Nye, 2002). Het recht op privacy kan de transactiekosten (de kosten die ontstaan om de benodigde resources voor het productieproces te verkrijgen) rondom de organisatie van personeel beïnvloeden bijvoorbeeld als (kandidaat) werknemers zich in hun presentatie alleen laten leiden door eigen belangen. Deze belangentegenstelling kan ook worden verondersteld in andere relaties tussen deelnemers aan het economische proces zoals bedoeld in de 'agency theory'. Deze theorie gaat uit van het idee dat in de relatie opdrachtgever en opdrachtnemer, de opdrachtnemer meer gericht is op de eigen belangen dan op die van de opdrachtgever. In bedrijven leidt dit ertoe dat er controlemechanismen worden toegepast om dergelijk gedrag te voorkomen.

Privacy versus personalisatie

Het verzamelen en gebruiken van gegevens biedt e-commerce bedrijven de mogelijkheid om gepersonaliseerde reclame uitingen en aanbiedingen te doen. Anderzijds zijn consumenten bezorgd over hun privacy en zien zij misbruik van persoonsgegevens als een reëel risico (Lee & Ahn, 2011). Voorbeelden van dergelijke risico's zijn ongewenste mails, het ongeoorloofd verspreiden van persoonsgegevens, creditcard fraude en mogelijk zelfs identiteitsdiefstal. Ondanks deze barrière die consumenten voorzichtig maakt om betrokken te worden in e-commerce activiteiten (Pavlou, 2011), is het delen van informatie noodzakelijk voor het functioneren van de e-commerce markt. De wenselijkheid van consumenten om in e-commerce activiteiten betrokken te zijn en de mogelijke privacy risico's daarvan, zijn daarbij de afwegingen die in deze trade-off worden meegenomen.

Privacy versus economisch voordeel

Ten aanzien van de grondhouding bij individuen voor het delen van informatie in een economische context, kan onderscheid worden gemaakt naar de 'privacy onbezorgden', 'privacy pragmatici' en 'privacy fundamentalisten' (Lee & Ahn, 2011). De 'onbezorgden' stellen welwillend persoonlijke informatie ter beschikking in ruil voor economische voordelen, de 'pragmatici' delen informatie eveneens in ruil voor economische voordelen echter alleen zolang ze beschermd worden door een actief privacy beleid. De 'fundamentalisten' zullen nooit persoonlijke informatie delen en dientengevolge ook niet profiteren van bepaalde voordelen. Een fenomeen dat zich in een economische context voordoet is de 'privacy paradox'. Hiervan is sprake als een individu zich enerzijds bezorgd toont over de eigen privacy maar anderzijds hier tegenovergesteld naar handelt, bijvoorbeeld door toch de eigen persoonsgegevens met anderen te delen. De intenties van individuen omtrent het ontsluiten van persoonlijke gegevens stemt dus niet overeen met hun gedragingen (Norberg, Horne, & Horne, 2007). Een uitleg die hier aan gegeven kan worden is dat privacy niet absoluut is maar een construct waaraan economische waarde kan worden toegekend. In verband hiermee doet zich een andere fenomeen voor namelijk de 'privacy calculus' waarbij consumenten bepaalde informatie ontsluiten omwille van bepaalde voordelen. Consumenten zien privacy in dat geval als een commodity dat kan worden opgeofferd in ruil voor bepaalde voordelen van financiële, economische of sociale aard (Pavlou, 2011).

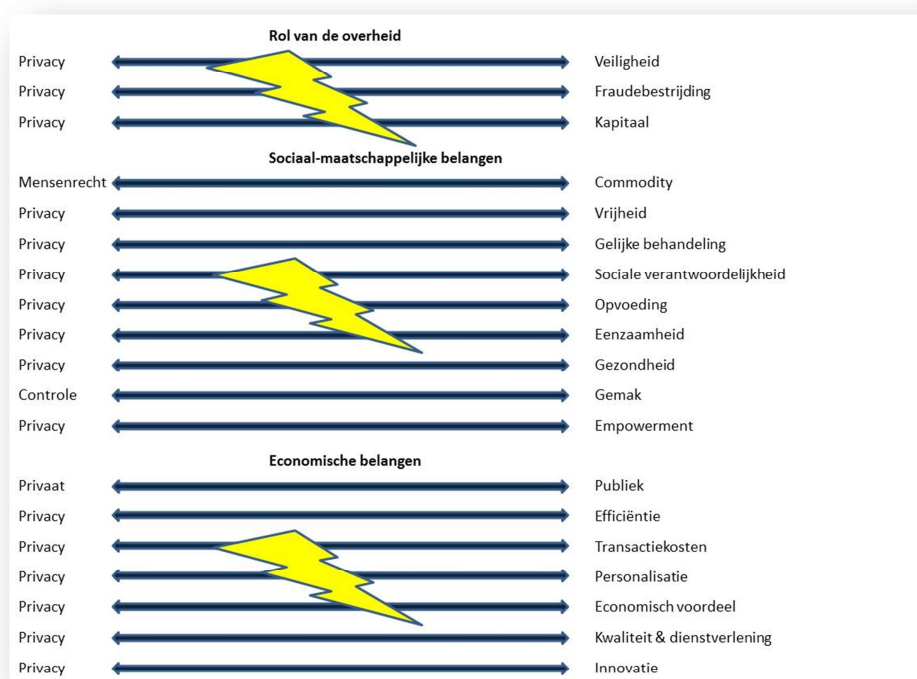
Privacy versus kwaliteit en dienstverlening

Technologische innovaties stellen bedrijven in staat om meer informatie te verzamelen over de leefwijze van huishoudens. Een voorbeeld hiervan is de 'slimme energiemeter' die informatie verstuurt over het lokale verbruik en zelfopwekking van energie. Op die manier is direct inzichtelijk hoeveel energie er ergens nodig is en

kan een betere kwaliteit worden gerealiseerd. Inzicht in gedragingen van klanten biedt bedrijven de mogelijkheid om hun dienstverlening daarop aan te passen en uit te breiden. Zo kunnen energieleveranciers significante afwijkingen in het energieverbruik detecteren en de betreffende huishoudens daarvan op de hoogte stellen. Een andere mogelijkheid is dat een bank klanten adviseert over goedkopere alternatieven bijvoorbeeld voor verzekeringen en internet- en telefoon diensten. In 2012 verzamelde de gemeente Utrecht warmtescans van 60.000 woningen.¹⁴ Deze scans laten zien hoeveel warmte een huis uitstraalt en tonen tegelijkertijd aan of een huis wel of niet goed is geïsoleerd. Alhoewel in dit voorbeeld de voordelen voor burgers evident zijn, ging de discussie over het schenden van de privacy omdat er geen anonimisering was toegepast en de scans herleidbaar waren naar individuen.

Privacy versus innovatie

In deze trade-off wordt privacy afgewogen tegen de belangen van wetenschappelijke, technische en medische vooruitgang. Sommigen beweren bijvoorbeeld dat grootschalige toegang tot medische gegevens noodzakelijk is om een nieuwe generatie medicijnen te ontwikkelen met minder bijwerkingen (NRC Handelsblad, 15-2-2014). Dit is aannemelijk maar tevens biedt dit mogelijkheid om diezelfde gegevens voor commerciële doeleinden aan te wenden en te verkopen aan andere belanghebbenden. Eerder¹⁵ kwamen al andere technologische innovaties aan de orde zoals 'wearables' en 'big data'. Juist rondom technologie als facilitator van de netwerksamenleving, lijkt de trade-off privacy versus innovatie nadrukkelijk een rol te spelen.



Figuur 6. Overzicht trade-off's

3.2 Reacties op de trade-off's

Hoe manifesteren de disputen rondom de privacy trade-off's zich in de business modellen van de oude en nieuwe economie? Gekeken naar Facebook als vertegenwoordiger van de nieuwe economie, lijkt privacy

¹⁴ <http://www.oneworld.nl/privacy-versus-duurzaamheid>

¹⁵ Zie hoofdstuk 2

ondergeschikt te zijn aan andere 'hogere' doelen zoals 'empowerment', het verbinden van mensen en het zoveel mogelijk delen van informatie:

Our [Facebook] guiding compass is our mission: to give people the power to share and make the world more open and connected (Facebook, 2013).

People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.¹⁶ (Mark Zuckerberg)

In haar waardepropositie focust Facebook zich op gebruikers, marketeers en ontwikkelaars. Ten aanzien van de gebruikers wordt waarde gecreëerd door 'engaging products' te ontwikkelen waardoor mensen contacten kunnen onderhouden, kunnen leren en ontdekken, zichzelf kunnen profileren en overal en altijd online kunnen zijn. Het toenemend aantal gebruikers resulteert in positieve netwerk effecten en maakt Facebook meer en meer interessant voor marketeers. In december 2013 was het gemiddelde aantal actieve gebruikers per dag 757 miljoen tegen 618 miljoen het jaar daarvoor. Door het profileren van persoonskenmerken en sociale context, kan er doelgericht worden geadverteerd hetgeen voor Facebook de grootste bron van inkomsten is. Daarnaast biedt Facebook marketeers toegang tot 'engagement' gegevens en worden er hulpmiddelen geboden voor het opzetten en monitoren van reclame campagnes. Een derde groep waarop Facebook zich richt zijn ontwikkelaars; tegen betaling kunnen zij gebruik maken van ontwikkeltools om vanuit eigen applicaties integraties met Facebook tot stand te brengen.

Persoonsgegevens lijken voor Facebook een publiek goed te zijn waarbij het haar vrij staat om die ten behoeve van doelgerichte advertenties te verhandelen. De compensatie voor de producenten van deze gegevens (ofwel de Facebook gebruikers), bestaat uit toegang tot het Facebook platform. Facebook is echter een beursgenoteerd bedrijf waarbij aandeelhouders rendement op hun investering eisen. In hoeverre en hoelang deze verschillende belangen met elkaar verenigd kunnen worden, is een nog onbeantwoorde vraag. Voorstelbaar is dat Facebook een vergoeding zal vragen voor het gebruik van haar platform. Een andere wijziging in het business model kan zijn dat de visie 'privacy bestaat niet' tot in het extreme wordt doorgevoerd en er betaald moet worden om persoonsgegevens voor anderen af te schermen. Het eenzijdig wijzigen van spelregels zal zeer waarschijnlijk leiden tot negatieve netwerk effecten met een waardedaling van de onderneming tot gevolg. Negatieve netwerk effecten kunnen eveneens ontstaan als gebruikers de waarde van hun persoonsgegevens meer gaan inzien, of als er alternatieven komen waarmee hun privacy beter wordt beschermd. Inmiddels lijkt Facebook zich hier van bewust blijkens haar constatering dat er veranderingen in het sentiment van gebruikers gerelateerd aan privacy zijn waar te nemen (Facebook, 2013).

Daar waar het business model van Facebook is gebaseerd op de verkoop van gratis verkregen persoonsgegevens, is dat van WhatsApp gebaseerd op 'subscription'. Gebruikers van WhatsApp betalen jaarlijks een vergoeding om de berichtendienst te kunnen gebruiken. In februari 2014 werd bekend dat WhatsApp door Facebook zou worden overgenomen. De overname leidde tot beroering onder de WhatsApp gebruikers en deden velen overstappen op alternatieven waaronder de Russische concurrent 'Telegram'. Te midden van deze commotie reageerde Jan Koum, CEO van WhatsApp, als volgt:

Above all else, I want to make sure you understand how deeply I value the principle of private communication. For me, this is very personal. [...] The fact that we couldn't speak freely without the fear that our communications would be monitored by KGB is in part why we moved to the United States when I was a teenager. Respect for your privacy is coded into our DNA, and we built WhatsApp around the goal of knowing as little about you as possible: You don't have to give us your name and we don't ask for your email address. We don't know your birthday. We don't know your home address. [...] None of that data has ever been collected and stored by

¹⁶ <http://www.theguardian.com/technology/2010/jan/11/facebook-privacy>

WhatsApp, and we really have no plans to change that. If partnering with Facebook meant that we had to change our values, we wouldn't have done it.¹⁷

Opmerkelijk in deze uitspraak is de doelstelling om zo weinig mogelijk over klanten te willen weten. Dit staat haaks op de ambities van Facebook waarbij daarvoor juist geen grenzen lijken te zijn, ofwel Facebook wil alles van haar gebruikers weten. Duidt dit op inconsistenties in de visie van Mark Zuckerberg op privacy, of sorteert hij voor op ontwikkelingen die zullen leiden tot een nieuwe visie op privacy? Vooralsnog lijkt privacy voor Facebook niet relevant te zijn of zelfs niet te bestaan en wordt er ingezet op andere doelen.

Het business model van Google is eveneens gebaseerd op de verkoop van gratis verkregen persoonsgegevens. Google wil 'alle' informatie ter wereld organiseren en universeel toegankelijk en bruikbaar maken¹⁸. De wijze waarop Google deze missie tracht te realiseren, roept veel weerstand op zoals blijkt uit de verschillende privacy rechtszaken waarin zij de afgelopen jaren was verwikkeld (Rubinstein & Good, 2012). Voor Google lijken er geen grenzen te bestaan ten aanzien van de gegevens waartoe zij toegang wil hebben; voor individuen betekent dit dat moet worden afgezien om dingen te doen als daardoor vertrouwelijke informatie naar buiten komt, aldus Eric Schmidt, voormalig CEO van Google, getuige zijn volgende uitspraak: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"¹⁹. In deze uitspraak kan de trade-off privacy versus vrijheid worden herkend waarbij in dit geval de negatieve vrijheid wordt beperkt door een risico op ongewenste ontsluiting van intieme gegevens.

Bij Facebook en Google hebben gebruikers geen controle over de exploitatie van hun persoonlijke gegevens. In reactie hierop zijn er inmiddels initiatieven gestart waarbij zogenaamde 'infomediators' consumenten een digitaal domein bieden waarin zij de eigen persoonsgegevens kunnen beheeren. Deze gegevens worden opgeslagen in een digitale kluis en zijn alleen toegankelijk voor bedrijven waaraan expliciet toestemming is gegeven. Het Nederlandse bedrijf Qiy is een pionier op dit terrein en werkt momenteel aan een platform waarop deze diensten aangeboden kunnen worden. Op de vraag wat hun verdienmodel is, werd de volgende reactie gegeven:

Het verdienmodel van de Qiy Foundation is er op gebaseerd dat partijen die via Qiy een verbinding willen met hun klanten een bedrag betalen voor de aansluiting op de Qiy infrastructuur. Dat doen ze graag omdat ze daarmee de kans hebben een veilige en vertrouwde relatie op te bouwen met hun klant.

Gekeken naar enkele vertegenwoordigers van de oude economie, lijken zij zich ook bewust te zijn van de economische waarde van persoonsgegevens. Daar waar de nieuwe economie deze waarde echter ongestraft kan verzilveren, is dat bij de oude economie niet het geval zoals bleek uit het voornemen van ING om (weliswaar alleen na toestemming van de klant) persoonsgegevens aan te wenden voor advertentiedoeleinden. De maatschappelijke discussie die volgde, leidde uiteindelijk tot excuses van Nick Jue, directievoorzitter ING Nederland, voor de gang van zaken als ook tot het in de ijskast zetten van de plannen.²⁰ Tegelijkertijd met de excuses poogde hij tevens de zorgen van klanten inzake hun privacy als volgt weg te nemen:

Ik kan het niet duidelijker stellen: Uw individuele klant- en transactiegegevens worden door ING niet met derden gedeeld of verkocht. [...] Laat ik nogmaals benadrukken: de ING deelt uw klantgegevens niet met derden, laat staan dat wij die zouden verkopen. Voor ING heeft bescherming van de persoonsgegevens van onze klanten de hoogste prioriteit. Want wij realiseren ons dat uw privacy een groot goed is. [...] Wij zullen in gesprek met klanten, toezichthouders, privacy-organisaties en consumentenorganisaties bepalen of en hoe we verder gaan. [...] Onze dienstverlening draait om vertrouwen en het dienen van uw belang.

¹⁷ <http://blog.whatsapp.com/index.php/2014/03/setting-the-record-straight/>

¹⁸ http://www.google.com/intl/nl_nl/about/company/

¹⁹ <https://www.youtube.com/watch?v=A6e7wFDHzew>

²⁰ http://www.ing.nl/nieuws/nieuws_en_persberichten/2014/03/ing_en_het_gebruik_van_klant_brief.aspx

Maatschappelijke onrust ontstond eveneens in 2013 na berichten dat de nieuwe bonuskaart van Albert Heijn zo lek als een mandje zou zijn. Het leidde zelfs tot Kamervragen²¹ en tot speculaties over het doorverkopen van ‘ongezonde’ aankopen aan zorgverzekeraars (Oltshoorn, 2013). De vraag is in hoeverre er een relatie is tussen deze ‘sterke merken’ en de intensiteit van de maatschappelijke verontwaardiging? Voor nieuwkomers zoals Facebook lijkt een dergelijke verontwaardiging er niet te zijn terwijl hun houding overduidelijk anti-privacy is. Of is juist deze duidelijkheid en daarmee de wetenschap dat je gegevens worden verkocht, voor mensen een reden om bewust wel of geen Facebook account te nemen? Bedrijven als ING en Albert Heijn zijn diep geworteld in de Nederlandse samenleving. Voor de gewone burger staat Albert Heijn voor ‘het op de kleintjes passen’ en wordt ING geassocieerd met de degelijke spaarbank waarvan de wortels terugvoeren naar eerdere banken zoals de Rijkspostspaarbank, Nederlandsche Middenstandsbank, Postcheque- en Girodienst en Postbank. De diepe worteling veronderstelt dat klanten de relatie met deze bedrijven als een ongeschreven contract beschouwen. Voorstelbaar is dat een eenzijdige wijziging hiervan als onrechtvaardig wordt ervaren en leidt tot het ter discussie stellen van hun waardepropositie. Zo bezien lijkt de wet van de remmende voorsprong van toepassing te zijn op de oude economie bedrijven. Immers, de goede relatie met hun klanten lijkt eerder belemmerend dan stimulerend te werken terwijl de nieuwe economie bedrijven daar geen last van lijken te hebben.

De privacy versus dienstverlening trade-off blijkt ook bij de Rabobank een rol te spelen. In een reactie op een aanbeveling voor een integraal klantenkennissysteem reageerde Dr. P.W. Moerland, voorzitter raad van bestuur Rabobank, in een brief aan de Monitoring Commissie Code Banken in 2012 als volgt:

Rabobank is voor de lange termijn een betrouwbare financiële partner voor de klant door de zorg af te stemmen op de aard van de klant, de dienstverlening en het product. [...] Daarvoor moet je als bank veel weten van je individuele klant en het totaal aan klantgroepen. Prof Verhoef pleit dan ook voor een integraal klantenkennissysteem. Hoewel wij de aanbeveling onderschrijven, is de uitwerking niet eenvoudig. Ook vanuit de optiek van bescherming van de privacy van de klant, bestaan er in ieder geval grenzen aan het volledig toegankelijk maken van klantinformatie.²²

De uitspraak suggereert dat de privacy belangen van klanten voor de Rabobank zwaarder wegen dan een verbeterde waardepropositie. Eenzelfde houding kan worden herkend in de zogenaamde ‘Golden Rules’²³ van KPN:

1. Alles wat ik doe met klantdata zou privacy kunnen raken;
2. Geanonimiseerde data zijn geen persoonsgegevens en kunnen vrijelijk gebruikt worden;
3. Verzamel nooit meer data dan nodig is en sla het ook niet langer op;
4. Gebruik traffic en content data voor marketing of analytics, alleen met expliciete toestemming van de klant;
5. Toestemming van de klant is alleen geldig als: (1) deze is gebaseerd op detail informatie; (2) deze expliciet is gegeven; en (3) deze vooraf is gegeven.

In de ‘Golden Rules’ wordt nadrukkelijk gesproken over ‘een noodzakelijke toestemming vooraf’ alvorens persoonsgegevens voor marketingdoeleinden gebruikt mogen worden. Opmerkelijk is daarom het privacy statement²⁴ waarin wordt gesproken over ‘bezwaar maken’ hetgeen impliceert dat marketing uitingen pas worden gestopt nadat bezwaar is ingediend. Toch lijkt KPN privacy belangrijk te vinden hetgeen kan worden afgeleid uit: (1) de introductie van de ‘Blackphone’, een telefoon met encryptie waarmee afluisteren en aftappen wordt voorkomen; en (2) het volgende statement waarin de privacy versus innovatie trade-off kan worden herkend:

²¹ <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/10/22/antwoorden-kamervragen-over-privacyschendingen-door-middel-van-de-bonuskaart-van-albert-heijn.html>

²² <http://www.commissiecodebanken.nl/scrivo/asset.php?id=980863>

²³ <http://ddma.nl/privacy/privacy-waard-cbp-consumentenbond-vvd-ddma-debat/>

²⁴ <http://www.kpn.com/algemeen/missie-en-privacy-statement/onze-missie.htm>

Voortdurende technologische ontwikkelingen zijn van invloed op privacy en veiligheid. De ambitie van KPN is om hierbij het belang en de wensen van de klant voorop te blijven stellen. Daar waar klanten een eigen verantwoordelijkheid hebben, helpen wij hen met producten, diensten en voorlichting.²⁵

Het statement sluit aan bij de zogenaamde 'privacy by design' (PbD) principes zoals opgesteld door de Canadese professor Ann Cavoukian²⁶. Ook het telecom bedrijf UPC past deze principes toe teneinde de bescherming van de persoonlijke levenssfeer van klanten te kunnen waarborgen.²⁷ Ondernemingen die PbD toepassen committeren zich aan:

- Voorkomen in plaats van genezen; er dient geanticipeerd te worden op 'privacy invasive events' waarbij in het ontwerp voorzieningen worden getroffen die deze 'events' afweren.
- Privacy is de standaard instelling; in het ontwerp dient de standaard werking van de functionaliteit gebaseerd te zijn op 'geen privacy consequenties' voor individuen. Daar waar de werking wel privacy consequenties heeft, dient: (1) duidelijkheid te zijn over de doelen waarvoor persoonsgegevens worden verzameld; (2) voldaan te worden aan wet- en regelgeving; (3) alleen die informatie verzameld te worden die nodig is voor de correcte werking van de functionaliteit; en (4) het gebruik, bewaren en ontsluiten van gegevens verenigbaar te zijn met de beoogde doelen (doelbinding).
- Privacy is ingebed in functionaliteit; dit betreft het integreren van privacy in architectuur, IT systemen en ondernemingsactiviteiten.
- Geen verlies van functionaliteit; in het ontwerp dient maximaal gestreefd te worden naar het behartigen van de belangen van alle stakeholders waarbij valse dichotomieën worden voorkomen.
- Beveiliging van informatie in de hele levenscyclus; in het ontwerp dient voorzien te worden in maatregelen voor het beschermen van privacy gedurende de hele levenscyclus.
- Zichtbaarheid en transparantie richting belanghebbenden; dit beoogt het inzicht geven aan individuen over de wijze waarop persoonsgegevens worden beheerd en welke verantwoordelijkheden daarbij zijn geformaliseerd.
- De belangen van het individu staan centraal; respect voor de privacy van individuen dient het uitgangspunt te zijn. Daar waar privacy belangen worden geraakt, dienen in het ontwerp voorzieningen opgenomen te worden waarmee individuen hun privacy belangen optimaal kunnen controleren.

Ten aanzien van de privacy versus efficiëntie trade-off, blijken ondernemingen maatregelen te treffen om risico's als gevolg van onvolledige informatie te minimaliseren. Een voorbeeld hiervan is de stichting Preventel, een samenwerkingsverband van telecommunicatie aanbieders die de registratie voert van personen en bedrijven die bij één of meerdere deelnemers een openstaande vordering hebben.²⁸ Een registratie bij Preventel betekent dat je met naam en toenaam als wanbetaler bekend staat én dat deze informatie beschikbaar is voor andere Telecom aanbieders. Een ander voorbeeld betreft het gebruik van zogenaamde 'zwarte lijsten' bedoeld voor de registratie van wanbetalers en fraudeurs.

3.3 Conclusie

Welke belangen staan op het spel en in hoeverre houden vertegenwoordigers van de oude en nieuwe economie in hun business model rekening met tegenstellingen rondom de genoemde trade-off's (deelvraag 2)? Gekeken naar bijvoorbeeld de privacy versus veiligheid trade-off, is het de vraag of een pro-privacy houding betekent dat je daarmee automatisch tegen veiligheid bent en sociaal-maatschappelijke en economische belangen minder belangrijk vindt? Of vinden we met elkaar dat de dreigingen inmiddels zo groot zijn geworden

²⁵ <http://www.kpn.com/algemeen/missie-en-privacy-statement/onze-missie.htm>

²⁶ www.privacybydesign.ca

²⁷ <http://www.upc.nl/pdf/over-upc-maatschappelijk-overzicht-2012.pdf>

²⁸ <http://www.preventel.nl/>

dat we ons geen privacy meer kunnen permitteren? Of is dit angst die door sommigen wordt aangewakkerd om daarmee legitimiteit voor hun keuzes en handelwijze te krijgen en anderen in diskrediet te brengen? Met name bij trade-off's waarin privacy wordt afgewogen tegen andere fundamentele grondbeginselen waarop de maatschappij en democratie is gebouwd, lijkt nuancering noodzakelijk en zijn er ook andere aspecten en belangen die een keuze voor meer of minder privacy beïnvloeden. Zo zal het (deels) opgeven van privacy waarschijnlijk minder problematisch worden gevonden als daarmee het voorkomen van aanslagen wordt beoogd, dan wanneer dit zou worden gevraagd bijvoorbeeld om vast te stellen of je wel gezond leeft. Bij elke trade-off zou de vraag gesteld moeten worden of er minder bezwarende alternatieven voorhanden zijn waarmee toch hetzelfde doel gerealiseerd kan worden (subsidiariteitsbeginsel). Daar waar dat niet mogelijk is, biedt mogelijk het proportionaliteitsbeginsel een uitweg waarbij de inbreuk op de privacy niet verder gaat dan noodzakelijk voor het beoogde doel. Echter, dan nog blijven bezwaren van privacy fundamentalisten voorstelbaar, zeker bij hen die privacy als een noodzakelijke voorwaarde voor vrijheid zien. Het gevolg kan zijn dat er impasses ontstaan waarbij vervolgens van de overheid wordt verwacht om deze te doorbreken. Ofwel, ten aanzien van de voornoemde trade-off's dient de overheid dan te besluiten wiens belangen zij laat prevaleren boven die van anderen. Welke argumenten worden daarvoor aangevoerd en wie bepaalt daarbij de legitimiteit en objectiviteit van dergelijke beslissingen? Teneinde deze vragen te kunnen beantwoorden, zijn 'out-of-the-box' oplossingen nodig die vooralsnog duiden op een nieuwe betekenisgeving aan privacy.

In het algemeen is het aannemelijk om te veronderstellen dat persoonsgegevens per definitie waardevol zijn voor ondernemingen omdat dit ze in staat stelt om daar slimme dingen mee te doen zoals 'personalized advertizing', verbreding van dienstverlening en het verhogen van de kwaliteit. Op die wijze kunnen bedrijven hun waardepropositie verbeteren rondom de producten en diensten die ze al jarenlang verkopen. Voor internetbedrijven zoals Facebook, Twitter en Google geldt echter dat zij hun bestaansrecht ontleen aan de toegang tot gratis persoonsgegevens. Dit stelde Facebook in 2013 in staat om 89% van de omzet met advertentie-inkomsten te realiseren, in 2012 was dat 84%. Het business model en de afhankelijkheid van de toegang tot persoonsgegevens, lijken dus bepalend te zijn voor de wijze waarop ondernemingen met privacy en persoonsgegevens omgaan. Kijkend naar banken, dan lijken er weinig andere commerciële instellingen te zijn die inzicht hebben in de volledige financiële huishouding van consumenten en daaruit allerlei leefgewoonten kunnen afleiden. Dit biedt banken tal van mogelijkheden waarvan ING er onlangs één probeerde te verzilveren. Dat dit mislukte heeft mogelijk te maken met de gepercipieerde functie van banken, en is het in de huidige maatschappelijk discourse wellicht 'not done' dat banken persoonsgegevens ook voor andere doeleinden gebruiken.

Voor wat betreft de trade-off's kan worden geconcludeerd dat ondernemingen te maken hebben met belangentegenstellingen rondom privacy. Verrassenderwijs zijn dat niet alleen economisch geladen trade-off's maar ook trade-off's waar fundamentele rechten ter discussie gesteld lijken te worden. Ten aanzien van de nieuwe economie bedrijven lijken er geen intenties te bestaan om deze disputen op te lossen en moeten we maar wennen aan wat Scott McNealy, voormalig CEO van Sun, in 1999 al zei: "You have zero privacy, get over it". De oude economie bedrijven lijken zich te realiseren dat het schenden van privacy hun imago kan schaden; derhalve zijn ze voorzigtiger rondom het maken van keuzes bij trade-off's of pretenderen ze de belangen van de klant voorop te stellen. De vraag die voor ondernemingen steeds relevanter lijkt te worden is: wat is onze houding richting privacy op dit moment en welke ambities zouden we hieromtrent willen (intrinsiek) en moeten (extrinsiek) hebben? Daar waar deze van elkaar afwijken, dient nagedacht te worden over een transitietraject waarlangs de ambities kunnen worden gerealiseerd. Wat zijn in dat geval de consequenties van een keuze voor meer of minder privacy, bijvoorbeeld op het business model en de concurrentiepositie? In het hypothetische geval dat Facebook zou besluiten om de visie op privacy van WhatsApp te volgen, lijkt dat te betekenen dat hun business model onhoudbaar is. Immers, daar waar je pretendeert zo weinig mogelijk te willen weten van je gebruikers, zal de effectiviteit van gepersonaliseerde advertenties waarschijnlijk afnemen. In het omgekeerde geval dat WhatsApp besluit het business model van Facebook toe te passen, betekent dat

waarschijnlijk dat WhatsApp minder actief richting privacy zal worden. Een actieve houding vandaag geeft zo gezien geen garanties voor de toekomst.

Uit het voorgaande wordt duidelijk dat privacy ook voor ondernemingen een complex vraagstuk kan zijn of worden. In het maatschappelijk debat lijkt de oude economie geassocieerd te worden met pro-privacy terwijl privacy voor de nieuwe economie van ondergeschikt belang lijkt te zijn. Gaandeweg het debat is een herijking van het privacy concept voorstelbaar waarbij er nieuwe spelregels ontstaan en het bijvoorbeeld wel wordt geaccepteerd dat banken persoonsgegevens gebruiken voor op maat gesneden advies, of dat voor persoonsgegevens een prijs betaald dient te worden. In dat proces zal van ondernemingen worden gevraagd om keuzes te maken en waar nodig bij te stellen onder meer ten aanzien van de hiervoor genoemde trade-off's.

4 METHODOLOGIE

4.1 Onderzoeksaanpak

De onderzoeksaanpak in dit onderzoek is tweeledig. Middels een ‘subjectief descriptieve’ aanpak is gezocht naar het antwoord op het eerste gedeelte van de onderzoeksvraag namelijk: “Hoe manifesteren de verschillende visies op privacy zich in de business modellen van de oude en nieuwe economie?”. Een ‘exploratieve’ aanpak is gebruikt voor de beantwoording van het tweede gedeelte te weten: “Welke verschuivingen in deze visies kunnen worden verwacht in de strijd tussen vertegenwoordigers van beide economieën?”. Volgens De Groot (1964) kenmerkt descriptief onderzoek zich door het volgens een expliciet aangegeven systematiek registreren van ‘datgene wat zich voordoet’. Daarbinnen kan objectief en subjectief descriptief onderzoek worden onderscheiden waarbij “naar gelang de beschrijving, de registratie, c.q. de categorisering, telling, berekeningen geheel volgens objectieve instructies of, in meerdere of in mindere mate, volgens subjectieve waarnemings- en beoordelingsprocessen verlopen” (Groot, 1964). Daar waar voor het eerste deel van de onderzoeksvraag een ‘subjectief descriptieve’ onderzoeksaanpak is gekozen, is dat voor ‘datgene wat zich in de toekomst zal voordoen’ niet mogelijk. Derhalve is daarvoor een explorerende onderzoeksaanpak toegepast. Swanborn (2004) stelt dat een dergelijke aanpak logisch is als weinig over het onderzoeksobject bekend is. Volgens de Groot (1964) beoogt de onderzoeker met exploratief onderzoek vooral het vormen en selecteren van hypothesen en in mindere mate het verkennen en registreren van verschijnselen rondom het te onderzoeken fenomeen. In dit onderzoek is bij de exploratie gebruik gemaakt van de transitie management theorie zoals beschreven in paragraaf 4.5.

De voorafgaande hoofdstukken waarin de deelvragen 1 en 2 zijn behandeld, zijn tot stand gekomen op basis van literatuuronderzoek, deskresearch en media analyse. De beantwoording van deelvraag 3 is gedaan door het toetsen van een privacy taxonomie (categorisering) bij elf ondernemingen waarbij gebruik is gemaakt van deskresearch, interviews en feedbackverzoeken op de taxonomie. De deskresearch heeft zich gericht op het analyseren van jaarverslagen, ‘privacy statements’, ‘privacy policies’, ‘business principles’, ‘codes of conduct’, gedragscodes en overige relevante bronnen. De interviews zijn gehouden met ING, Philips en de Qiy Foundation. Na afronding van de interviews en de deskresearch, is aan de Rabobank, KPN, UPC, Albert Heijn en G4S gevraagd om de onderzoeksresultaten te reviewen en de ontbrekende duidingen aan te vullen. Alleen de Rabobank en Albert Heijn hebben hierop een reactie gegeven.

4.2 Privacy taxonomie

De in dit onderzoek opgestelde privacy taxonomie duidt de houding van ondernemingen richting privacy. De taxonomie is opgesteld op basis van: (1) inzichten van Tilburg et al. (2012) ten aanzien van de management disciplines die bij ondernemingen onderkend kunnen worden; en (2) een ontwikkelingsmodel van Tulder R. v. (2010) met een groeipad voor ondernemingen ten aanzien van hun houding richting issues en thema’s. Met betrekking tot de management disciplines is gezocht naar indicatoren (tabel 1) waarvoor logischerwijs een relatie met privacy verondersteld kan worden rondom: (1) strategisch en algemeen management; (2) inkoopbeleid en ketenmanagement; (3) personeelsbeleid; (4) financieel management; (5) communicatie en publieke zaken; (6) marketing en verkoop; (7) innovatie; en (8) operations.

Indicator	Omschrijving	Subindicatoren
Grondhouding	Classificeert de houding richting privacy op basis van intrinsieke opvattingen, overtuigingen, normen, waarden en eigen visies op thema’s en issues zoals privacy.	Visie, Belang, Zeggenschap, Markt voor persoonsgegevens, Markt voor privacy, Mensenrecht
Compliance	Classificeert de houding richting privacy op basis van aspecten gerelateerd aan compliance.	Wettelijke regels, Privacy policy, Cookies, Keurmerk en/of gedragscode, Doelbinding, Belangenorganisaties

Indicator	Omschrijving	Subindicatoren
Communicatie & Informatiedeling	Classificeert de houding richting privacy op basis van aspecten gerelateerd aan public relations en het delen van informatie met derde partijen.	Zichtbaarheid, Informatiedeling, Zwarte lijsten, Openbaarheid
Marketing	Classificeert de houding richting privacy vanuit het marketing en verkoop perspectief.	Marketing strategie, Customer intelligence, Kwaliteit en dienstverlening, Economische voordelen
HRM	Classificeert de houding richting privacy op vanuit de management discipline HRM.	Cameratoezicht, Screening, Verzuim, Levenssfeer, Gedragscode, Personeelsbeleid
Innovatie & technologie	Classificeert de houding richting privacy op basis van aan technologie en innovatie gerelateerde aspecten.	Technologie, Preventie, Privacy instellingen, Functionaliteit, Beveiliging
Society & instituties	Classificeert de houding van ondernemingen richting privacy vanuit hun visie op de samenleving en de gepercipieerde rol van de overheid en instituties.	Veiligheid, Marktwerving, Onderzoeksbelangen, Samenleving

Tabel 1. Privacy indicatoren

Bijlage 4 bevat de taxonomie waarin de voornoemde (sub)indicatoren zijn geoperationaliseerd gerelateerd aan de fasering en redenatie van het ontwikkelingsmodel. Bijlage 5 bevat een nadere beschrijving van de genoemde subindicatoren. Ten aanzien van het ontwikkelingsmodel wordt de werking hiervan in de volgende paragraaf toegelicht.

4.3 Ontwikkelingsmodel

Met betrekking tot duurzaam ondernemen wordt door Tilburg et al. (2012) een ontwikkelingsmodel beschreven met een groeipad om vanuit een inactieve opstelling te komen tot een proactieve houding. In deze ontwikkeling worden vier afzonderlijke businesscases onderkend te weten: (1) de klassieke businesscase met financiële winst als primair oogmerk; (2) de defensieve business gericht op het voorkomen van verliezen en reputatieschade; (3) de strategische businesscase ten behoeve van de concurrentiepositie en overlevingsstrategie; en (4) de maatschappelijke of 'new economy' businesscase. Alhoewel de auteurs het model specifiek voor duurzaam ondernemen beschrijven, kan het ook op andere onderwerpen, issues en vraagstukken zoals privacy worden toegepast. De functie van het ontwikkelingsmodel is om ondernemingen inzicht te geven in hun positie ten opzichte van een bepaald thema of issue. Ook biedt het bedrijven een handvat om te reflecteren op hun gedrag ten aanzien van hetzelfde issue.

4.3.1 Gedragsdimensies

De indeling van het model is gebaseerd op twee gedragsdimensies namelijk een grondhouding en maatschappelijke responsiviteit.

Grondhouding

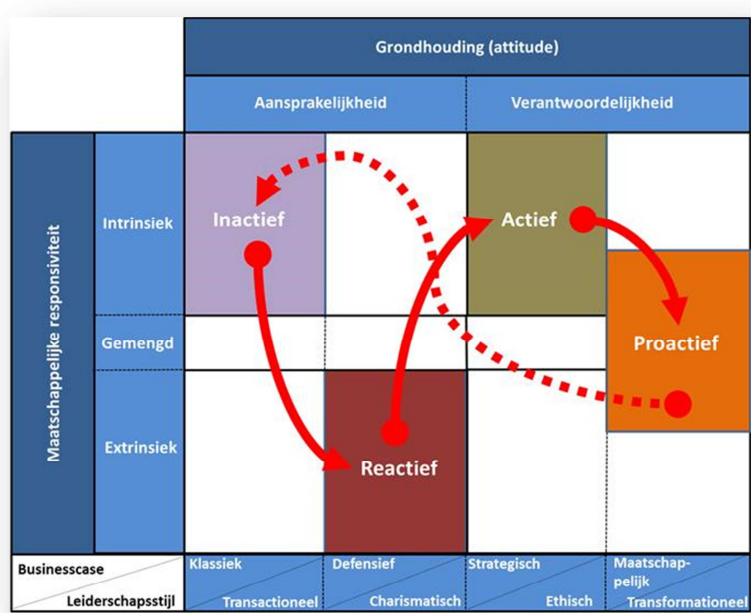
De grondhouding wordt op de horizontale as weergegeven en is bedoeld om de attitude jegens maatschappelijke uitdagingen als motivatie voor bepaald gedrag te duiden. In basis worden hiervoor twee uitersten onderkend namelijk aansprakelijkheid en verantwoordelijkheid. Aansprakelijkheid is primair gericht op het voorkomen van schade door wetten en voorschriften plichtmatig na te leven. Verantwoordelijkheden worden bij andere stakeholders neergelegd en het zijn voornamelijk externe invloeden zoals wet- en regelgeving, die organisaties aanzetten tot handelen. Dit handelen zal zich tot het hoogst noodzakelijke beperken totdat wordt voldaan aan de gestelde eisen. De grondhouding verantwoordelijkheid betekent dat organisaties in hun handelwijze wel een eigen verantwoordelijkheid ervaren en zich primair niet laten leiden door wat hen door anderen wordt opgelegd.

Maatschappelijke responsiviteit

De maatschappelijke responsiviteit wordt op de verticale as weergegeven en is bedoeld om de oriëntatie op interne of externe stakeholders als motivatie voor bepaald gedrag te duiden. De twee uitersten die daarbij worden onderkend zijn een intrinsieke en extrinsieke oriëntatie. De intrinsieke oriëntatie betekent dat gedrag vooral wordt bepaald op basis van de eigen beeldvorming en waarbij de mening van externe stakeholders geen rol speelt. Een extrinsieke oriëntatie vindt externe stakeholders wel belangrijk en zal daarbij ook luisteren naar partijen die geen directe binding met de organisatie hebben maar wel een rol spelen in het debat zoals belangengroepen.

4.3.2 Fasering

Op basis van de genoemde dimensies, kunnen vier fases worden onderkend waarin organisaties zich kunnen bevinden ten aanzien van een thema of issue. Het betreft de inactieve, reactieve, actieve en proactieve fase zoals weergegeven in figuur 7.



Figuur 7. Ontwikkelingsmodel (Tulder R. v., 2010)

De pijlen in het model markeren het groeipad dat ondernemingen hoogstwaarschijnlijk zullen bewandelen. Naast de grondhouding en maatschappelijke responsiviteit, wordt elke fase ook getypeerd door een bepaald type businesscase en een leiderschapsstijl wat voor die fase het meest geschikt wordt geacht.

Inactieve fase

Een onderneming, business unit, afdeling of zelfs persoon in de inactieve fase ziet geen reden om zich te conformeren aan een issue tenzij de overheid dit dwingend oplegt of er directe voordelen te behalen zijn. Voor issues ter zake is de onderneming van mening dat regulering waar nodig door de overheid moet worden gedaan, omdat zij vanuit haar institutionele rol daarin het meest effectief zal zijn. Tot actie zal pas worden overgegaan als de onderneming aansprakelijk wordt gesteld voor de consequenties van hun handelen, of als de economische nadelen van de status quo de organisatie teveel belast dan wel als de economische voordelen van verandering de status quo overtreffen. In het algemeen zal er geen visie bestaan over het issue en wordt er een klassieke businesscase gehanteerd dat is gericht op de totstandkoming van transacties en kostenbesparingen. Hierbij past de transactionele leiderschapsstijl dat is gericht op maximalisatie van efficiëntie.

Reactieve fase

Ondernemingen in de reactieve fase erkennen het belang van externe stakeholders en zullen daar in hun handelwijze ook rekening mee houden. De businesscase is defensief van aard waarin kostenvoordelen, interactie met de markt en bescherming van de eigen reputatie een rol spelen. De ambities van een onderneming ten aanzien van een issue, zijn afgestemd op die van de concurrenten waarbij de koploperpositie aan anderen wordt overgelaten. Reageren op signalen van belanghebbenden zoals klanten, leveranciers, aandeelhouders en maatschappelijke organisaties, typeert de aard van het handelen van organisaties in deze fase. Dit plaatst de organisatie en haar mensen onder hoge druk en charismatisch leiderschap is in dergelijke situaties een voor de hand liggende stijl van leidinggeven.

Actieve fase

In de actieve fase is het 'eigen verantwoordelijkheid' waardoor ondernemingen zich laten leiden. Niet de eisen die anderen stellen of de plichten die anderen opleggen, maar een intrinsieke motivatie is de drijfveer voor bepaalde handelwijzen en keuzes. Als zodanig heeft dit een moreel en ethisch aspect waarbij dingen 'goed of fout' dan wel 'gewenst of ongewenst' zijn. Ten aanzien van de interactie met andere stakeholders is er een open communicatie gebaseerd op wederzijds respect en stelt de organisatie zich receptief op ten aanzien van gedachten en ideeën die door anderen worden aangereikt. Bedrijven in deze fase doen actief verslag van de stand van zaken en ook worden er initiatieven ondernomen voor het realiseren van innovaties. De businesscase is strategisch en gericht op het innemen van een unieke, lange termijn concurrentiepositie rondom een thema. Qua stijl van leidinggeven vraagt dit om visionair en ethisch leiderschap.

Passive		Active	
Inactive	Reactive	Active: go-it-alone	Pro-active: partnership
Definition of CSR			
"Corporate Self Responsibility"	"Corporate Social Responsiveness"	"Corporate Social Responsibility"	"Corporate Societal Responsibility"
Main characteristics			
Legal compliance and utilitarian motives: profit maximalisation	Moral (negative) duty compliance: short term profit and market capitalization	Choice for responsibility and virtue: long term profit	Choice for interactive responsibility: midterm and sustainable profit
Indifference	Compliance/reputation	Integrity	Discourse ethics
Efficiency	Limit inefficiency	Equity/Ethics	Effectiveness
Inside-In	Outside-in	Inside-out	In-outside-in/out
"Doing things right"	"Don't do things wrong"	"Doing the right things"	"Doing the right things right"
"Doing well"	"Doing well and doing good"	"Doing good"	"Doing well by doing good"
Resource based view	Shareholder view	Capabilities view	Stakeholder view
Marketing and demand approach		Marketing and production: supply and demand	

Figuur 8. Ontwikkelingsmodel karakteristieken (Tulder & Zwart, 2006)

Proactieve fase

In deze fase is de verwevenheid van de strategie en het thema het grootst waarbij beiden in optima forma nauwelijks van elkaar te onderscheiden zijn. De onderneming heeft oog voor alle ontwikkelingen rondom het thema; ook daar waar de onderneming daar niet door wordt beïnvloed. Er ontstaan nieuwe verdienmodellen en er is ruimte voor samenwerking met externe stakeholders. Kenmerkend voor deze fase is dat het thema in alle bedrijfsdisciplines van de organisatie een plaats heeft gekregen. Ondernemingen in deze fase zijn vernieuwend en binnen hun sector of branche zijn zij de spelbepalers. De businesscase in deze fase heeft een maatschappelijke argumentatie waarbij 'verbindend' of transformatieel leiderschap het meest geschikt lijkt om de overgang van de actieve naar de proactieve fase te leiden.

Figuur 8 toont de karakteristieken zoals deze per fase uit het ontwikkelingsmodel onderkend kunnen worden.

4.3.3 Transitie en kantelpunten

De fasering in het ontwikkelingsmodel veronderstelt een groeipad waarbij in deze transitie drie impulsen onderscheiden kunnen worden te weten activering, interne 'alignment' en externe 'alignment'. Activering treedt op als externe stakeholders dringend verzoeken om bepaalde veranderingen door te voeren. De organisatie verlaat daardoor de inactieve fase en richt zich op het veiligstellen van de reputatie waarbij alle betrokkenen door interne alignment op één lijn komen. De overgang van de reactieve naar de actieve fase zal plaatsvinden als de attitude ten opzichte van maatschappelijk thema's omslaat van aansprakelijkheid in verantwoordelijkheid. Dit legt de basis voor een transitie naar een proactieve houding waarbij door samenwerking met externen het thema van organisatie naar systeemniveau kan worden getild.

4.4 Onderzoekspopulatie

De onderzoekspopulatie bestaat uit vertegenwoordigers van de oude economie, nieuwe economie en enkele telecommunicatie bedrijven (tabel 2). Daar waar vertegenwoordigers van de nieuwe economie hun bestaan danken aan de opkomst van het informatietijdperk en het internet, is dat bij vertegenwoordigers van de oude economie niet het geval. Voor de Telecom bedrijven geldt dat er aanknopingspunten zijn voor zowel de oude als nieuwe economie; derhalve is in dit onderzoek gekozen om deze ondernemingen als aparte groep te behandelen. Gekeken naar de rol van het verdienmodel, zijn de volgende typeringen gebruikt ten aanzien van de wijze waarop de onderzochte ondernemingen hun inkomsten realiseren.

- Online adverteren; betreft de verkoop van geprofileerde persoonsgegevens en advertentieruimtes aan marketeers.
- Licenties & abonnementen; licenties betreft de éénmalige verkoop van bepaalde gebruiksrechten veelal in combinatie met terugkerende inkomsten waarbij periodiek een percentage over de geïndiceerde licentiebedragen in rekening wordt gebracht. Abonnementen betreft de levering van producten of diensten gedurende een afgesproken periode volgens een vooraf afgesproken betaalschema.
- Goederenverkoop; betreft eenmalige transacties voor de levering van goederen of diensten.
- Contracten; inkomsten worden gerealiseerd door het nakomen van de verplichtingen die contractueel zijn overeengekomen.
- Geldproducten; betreft eenmalige en terugkerende inkomsten uit de verkoop van geld gerelateerde producten waaronder hypotheekleningen, derivaten, verzekeringen en beleggingsproducten.

Sector	Onderneming	Visie / Missie	Sinds	Economie	Verdien-model
eBusiness		Our mission is to give people the power to share and make the world more open and connected.	2004	Nieuw	Online adverteren
		De missie van Google is alle informatie ter wereld te organiseren en universeel toegankelijk en bruikbaar te maken.	1998	Nieuw	Online adverteren
		De visie van de Qiy Foundation is dat de positie van mensen in digitale wereld zo veel als mogelijk gelijk zou moeten zijn aan de positie van mensen in de fysieke wereld. Belangrijke principes zijn menselijke waarden en normen en acteren conform de menselijke maat. De missie van de Qiy Foundation is om mensen controle te geven over hun gegevens en ze te helpen daar slimme dingen mee te doen. Gegevens die men zelf veroorzaakt en gegevens die van hen beschikbaar zijn bij derden.	2005	Nieuw	Licenties & abon.
		Building a cool product used globally by everybody.	2009	Nieuw	Licenties & abon.

Sector	Onderneming	Visie / Missie	Sinds	Economie	Verdien-model
Telecom		We geloven in een samenleving waarin communicatietechnologie het leven verrijkt. Het is onze missie om veilige, betrouwbare en toekomstbestendige netwerken en diensten te bieden waardoor mensen, bedrijven en organisaties altijd en overal met elkaar verbonden kunnen zijn.	1852	Telecom	Licenties & abon.
		De digitale wereld neemt een enorme vlucht. Dit kan overweldigend zijn. In een wereld vol mogelijkheden is het goed als iemand de weg wijst. UPC wil dat iedereen mee kan doen, ook zonder technologische kennis. UPC geeft toegang tot een wereld vol informatie en entertainment. Simpel, op maat en 24 uur per dag. N.B. UPC is in eigendom van Liberty Global.	1995	Telecom	Licenties & abon.
Elektronica		Missie: Het leven van mensen verbeteren met zinvolle innovaties. Visie: Philips streeft ernaar middels innovaties de wereld om ons heen gezonder en duurzamer te maken. Ons doel is om in 2025 de levens van drie miljard mensen te hebben verbeterd. Wij bieden de beste werkomgeving voor mensen die onze passie delen en samen bieden we onze klanten en aandeelhouders ongekennde meerwaarde.	1891	Oud	Goederen-verkoop
Retail		'Het alledaagse betaalbaar, het bijzondere bereikbaar', dat is de missie van Albert Heijn. Het is eigenlijk precies wat de oprichter van ons bedrijf voor ogen had. Op strooibiljetjes liet hij de volgende tekst drukken: 'Prima Kwaliteit, Groote Omzet, Kleine Winst. Arm en Rijk kunnen bij mij hun inkopen doen.' Naast bijzondere producten en acties, zijn we óók een betaalbare winkel voor de alledaagse boodschappen. Dat onderstrepen we met onze missie.	1887	Oud	Goederen-verkoop
Beveiliging		Our vision is to be recognised as the global leader in providing secure outsourcing solutions, to help customers to achieve their own strategic goals and to deliver sustainable growth for G4S and long-term value for shareholders.	1901	Oud	Contracten
Banken		ING is van mening dat duurzame vooruitgang wordt gestimuleerd door mensen met de verbeeldingskracht en het doorzettingsvermogen om hun eigen toekomst en de toekomst van hun naasten te verbeteren. Wij stellen mensen en organisaties in staat om hun eigen ideeën over een betere toekomst te realiseren – hoe bescheiden of groots ook. Onze doelstelling is daarom: mensen in staat stellen om zowel privé als zakelijk steeds voorop te blijven lopen.	1881	Oud	Geld-producten

Sector	Onderneming	Visie / Missie	Sinds	Economie	Verdien-model
		De Rabobank Groep heeft als doel het dienen van de economische belangen van onze leden en klanten. De manier waarop we deze ambitie willen realiseren, is samengevat in vier kernwaarden: respect, integriteit, professionaliteit en duurzaamheid. Het zijn als het ware de randvoorwaarden voor ons handelen. De kernwaarden zijn opgenomen in de Gedragscode die door alle medewerkers wordt onderschreven.	1898	Oud	Geld-producten

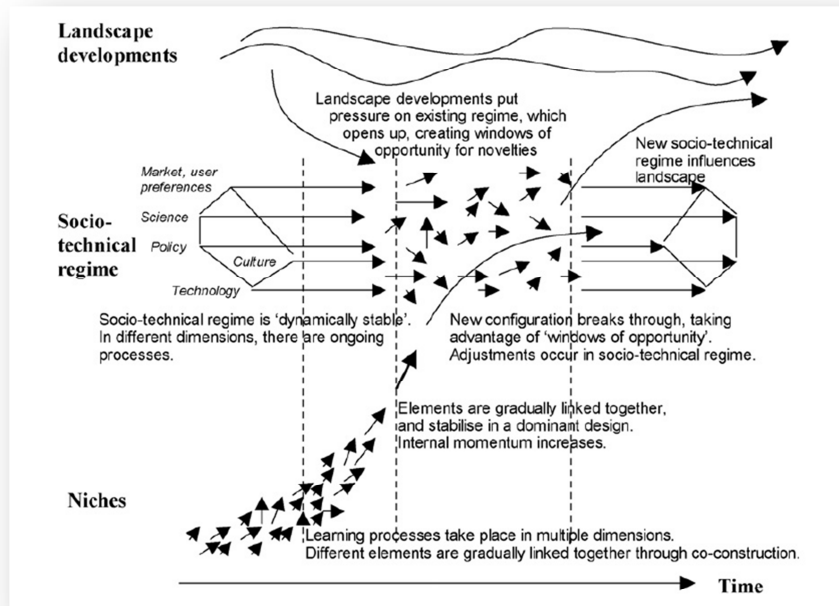
Tabel 2. Onderzoekspopulatie

4.5 Transitie management theorie

Bij de exploratie naar de verwachte verschuivingen in de visies op privacy, wordt zoals aangegeven gebruik gemaakt van de transitie management (TM) theorie²⁹. Volgens deze theorie zijn de huidige duurzaamheidsproblemen (water, energie, milieu, e.a.) zo ingrijpend dat deze alleen kunnen worden opgelost door fundamentele, systemische wijzigingen rondom technologie, economie, ecologie, instituties en ondernemingen (Loorbach & Wijsman, 2013). De doelstelling van TM is “to create a societal movement through new coalitions, partnerships and networks around arenas that allow for building up continuous pressure on the political and market arena to safeguard the long-term orientation and goals of the transition process” (Loorbach & Rotmans, 2010). De ‘societal movement’ ofwel de ‘transitie’ kan daarbij worden opgevat als “a fundamental change in the structures, cultures and practices of a societal system, profoundly altering the way it functions” (Haan & Rotmans, 2011). Transitie management beoogt dus het realiseren van fundamentele veranderingen in de inrichting en organisatie van de maatschappij en ondernemingen (figuur 9). Een praktijkvoorbeeld in Nederland is de transitie van traditionele bitumen dakbedekkingen naar duurzame dakbedekkingen gecombineerd met extra functies zoals wateropslag, energieopwekking en CO₂ reductie (Loorbach & Rotmans, 2010). Het voorbeeld illustreert een paradigma shift resulterend in nieuwe business modellen met een focus op duurzaamheid.

Het realiseren van systemische wijzigingen gebeurt door ‘reconstellation’, ‘empowerment’ of ‘adaptation’ (Haan & Rotmans, 2011). ‘Reconstellation’ betekent ten aanzien van privacy dat dit als mensenrecht ter discussie wordt gesteld en er - onder invloed van buitenaf - dwingend plaats wordt gemaakt voor een nieuw paradigma met een fundamenteel andere kijk op privacy. Mogelijke processen waarin deze transitievorm tot stand komt zijn: (1) hervormingswetgeving; (2) nieuwe infrastructuren; en (3) regionale heroriëntatie (Haan & Rotmans, 2011). In het geval van ‘empowerment’ komt een paradigma shift tot stand doordat een niche of meerdere niches met andere visies op privacy zich van binnenuit ontwikkelen tot het nieuwe regime. Mogelijke processen waarin deze transitievorm tot stand komt zijn: (1) zoeken naar erkenning bijvoorbeeld door het ontwikkelen van standaarden en certificering van producten en diensten; (2) vorming van vakbonden, kartels, lobby’s en belangenorganisaties; en (3) professionalisering bijvoorbeeld door specialisering, educatie, R&D en ervaring (Haan & Rotmans, 2011). ‘Adaptation’ betekent dat het regime andere visies op privacy adopteert. Hierdoor kan het de dominante positie behouden en wordt er ingespeeld op de actuele behoeften. Mogelijke processen waarin deze transitievorm tot stand komt zijn: (1) herpositionering, bijvoorbeeld een oliemaatschappij die overstapt op groene energiebronnen; (2) reorganiseren, bijvoorbeeld het samenvoegen of splitsen van bedrijfsonderdelen; en (3) innovatie, bijvoorbeeld het toepassen van een nieuwe technologie (Haan & Rotmans, 2011).

²⁹ Zie hoofdstuk 6



Figuur 9. Multi-level perspectief op systeem innovaties (Geels, 2004)

De waarschijnlijkheid dat een transitie zich manifesteert hangt af van de mate waarin een sociaal-maatschappelijk systeem gecompromitteerd raakt. In dat geval vervult het systeem niet meer de functie die het geacht wordt te vervullen. Mogelijke aanjagers hiervoor zijn volgens de Haan en Rotmans (2011) 'tensions', 'stress' en 'pressure'. Van 'tensions' is sprake als de functie van het systeem in relatie tot de omgeving onder druk staat. Typische signalen hiervoor zijn een vijandig politiek klimaat, uitputting van resources en invloed van de publieke opinie. Stress is het verschijnsel als een regime interne inconsistenties vertoont waardoor het de functie niet meer kan vervullen. Signalen hiervoor zijn afwijkingen tussen de pretenties en praktijken van een systeem. 'Pressure' treedt op als niches levensvatbare concurrenten worden voor het regime of aspecten daarvan zelfs irrelevant maken. Een voorbeeld hiervan is de introductie van de CD/DVD waardoor grammofoonplaten overbodig werden (Haan & Rotmans, 2011).

5 ONDERZOEKSRESULTATEN

Welke visies op privacy kunnen in de huidige discourse bij vertegenwoordigers van de oude en nieuwe economie worden waargenomen (deelvraag 3)? Voor de beantwoording van deze vraag worden hierna de aangetroffen houdingen op de diverse indicatoren geanalyseerd en geïnterpreteerd.

5.1 Overzicht onderzoeksresultaten

De aangetroffen houdingen op de verschillende subindicatoren worden in tabel 3 getoond.

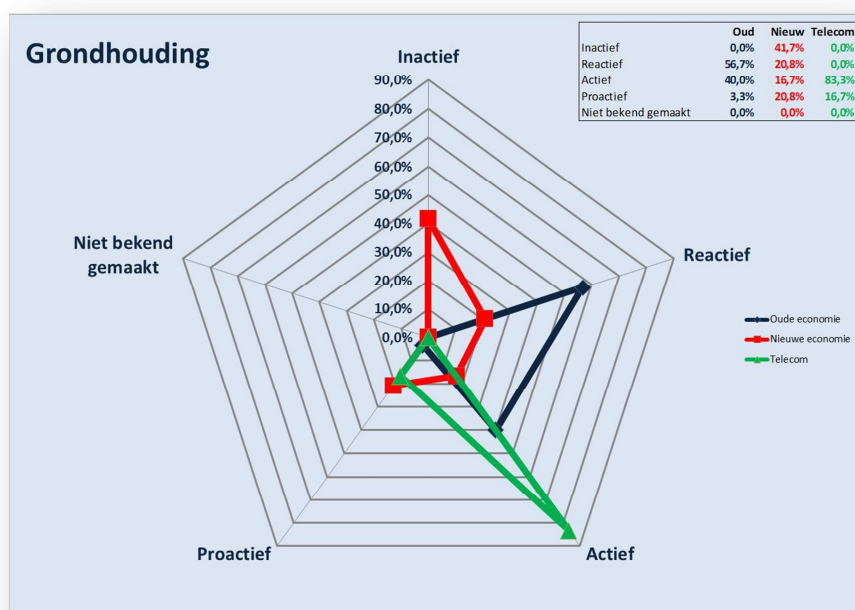
Indicator	Subindicator	Facebook	Google	Qiy Foundation	WhatsApp	KPN	UPC	Philips	Albert Heijn	G4S	ING	Rabobank
Grondhouding	Visie	Inactief	Inactief	Proactief	Actief	Proactief	Actief	Actief	Actief	Reactief	Proactief	Actief
	Belang	Reactief	Reactief	Proactief	Reactief	Actief	Actief	Reactief	Reactief	Reactief	Actief	Actief
	Zeggenschap	Inactief	Inactief	Proactief	Reactief	Actief	Actief	Reactief	Reactief	Reactief	Reactief	Reactief
	Markt voor pers.geg	Inactief	Inactief	Proactief	Reactief	Actief	Actief	Reactief	Reactief	Reactief	Reactief	Actief
	Markt voor privacy	Inactief	Inactief	Proactief	Actief	Actief	Proactief	Reactief	Reactief	Reactief	Reactief	Actief
	Mensenrecht	Inactief	Inactief	Actief	Actief	Actief	Actief	Actief	Actief	Actief	Actief	Actief
Compliance	Wettelijke regels	Reactief	Reactief	Actief	Reactief	Actief	Actief	Actief	Reactief	Reactief	Actief	Reactief
	Privacy policy	Reactief	Reactief	Proactief	Actief	Actief	Actief	Proactief	Actief	Reactief	Actief	Reactief
	Cookies	Reactief	Inactief	Proactief	Inactief	Reactief	Actief	Actief	Reactief	Reactief	Reactief	Reactief
	Keurmerk/gedragscode	Inactief	Inactief	Proactief	NBG	Actief	Actief	Reactief	Reactief	NBG	Proactief	Actief
	Doelbinding	Inactief	Inactief	Actief	Inactief	Actief	Actief	Actief	Actief	Reactief	Reactief	Actief
	Belangenorganisaties	Inactief	Inactief	Actief	Reactief	Actief	Actief	Actief	Reactief	Reactief	Reactief	Reactief
Communicatie & informatiedeling	Zichtbaarheid	Reactief	Reactief	Proactief	Reactief	Actief	Actief	Reactief	Reactief	Reactief	Actief	Reactief
	Informatiedeling	Inactief	Inactief	Proactief	Inactief	Reactief	Reactief	Actief	Actief	Actief	Actief	Actief
	Zwarte lijsten	NBG	NBG	Proactief	NBG	Reactief	Reactief	Reactief	Reactief	Reactief	Reactief	Actief
	Openbaarheid	Reactief	Reactief	Proactief	Reactief	Reactief	Reactief	Reactief	Reactief	Reactief	Reactief	Reactief
Marketing	Marketing strategie	Inactief	Inactief	Proactief	Reactief	Reactief	Reactief	Reactief	Reactief	Reactief	Reactief	Reactief
	Customer intelligence	Inactief	Inactief	Actief	Reactief	Actief	Reactief	Actief	Reactief	Reactief	Reactief	Actief
	Kwaliteit en dienstverl.	Inactief	Inactief	Actief	Inactief	Reactief	Reactief	Actief	Reactief	Reactief	Reactief	Reactief
	Economische voordelen	Reactief	Reactief	Actief	Actief	Actief	Actief	Actief	Reactief	Reactief	Reactief	Reactief
HRM	Cameratoezicht	NBG	NBG	Actief	NBG	NBG	NBG	Actief	NBG	NBG	Reactief	Reactief
	Screening	NBG	NBG	Actief	NBG	NBG	NBG	Reactief	NBG	Reactief	Actief	Actief
	Verzuim	NBG	NBG	Proactief	NBG	NBG	NBG	Proactief	NBG	NBG	Actief	Actief
	Levensfeer	NBG	NBG	Proactief	NBG	NBG	NBG	Reactief	NBG	NBG	Actief	Reactief
	Gedragscode	NBG	NBG	Proactief	NBG	Actief	NBG	Reactief	NBG	NBG	Actief	Actief
	Personeelsbeleid	NBG	NBG	Proactief	NBG	Actief	Actief	NBG	Inactief	NBG	Actief	Reactief
Innovatie & technologie	Technologie	Inactief	Reactief	Proactief	Actief	Actief	Actief	Reactief	Reactief	Reactief	Proactief	Reactief
	Preventie	Reactief	Inactief	Proactief	Reactief	Actief	Actief	Reactief	NBG	NBG	Actief	Actief
	Privacy instellingen	Inactief	Inactief	Proactief	Reactief	Actief	Actief	Proactief	NBG	NBG	Actief	Inactief
	Functionaliteit	Reactief	Reactief	Proactief	Actief	Actief	Actief	Actief	NBG	NBG	Reactief	Actief
	Beveiliging	Actief	Reactief	Actief	Reactief	Actief	Actief	Actief	Actief	Actief	Actief	Actief
Society & instituties	Veiligheid	NBG	Reactief	Proactief	Actief	Proactief	Actief	Reactief	NBG	Actief	Reactief	Actief
	Marktwerving	Inactief	Inactief	Proactief	Actief	Actief	Actief	Reactief	Reactief	Reactief	Reactief	Actief
	Onderzoeksbelangen	NBG	Actief	Proactief	NBG	Actief	Actief	Actief	NBG	NBG	Actief	Actief
	Samenleving	Inactief	Inactief	Actief	Actief	Actief	Actief	Reactief	Actief	Reactief	Actief	Actief
Scores per attitude	Niet bekend gemaakt	9	7	0	9	4	5	1	10	10	0	0
	Inactief	16	17	0	4	0	0	0	1	0	0	1
	Reactief	9	10	0	12	6	6	17	17	21	15	14
	Actief	1	1	11	10	23	23	14	7	4	17	20
	Proactief	0	0	24	0	2	1	3	0	0	3	0

Tabel 3. Detail resultaten

5.2 Analyse onderzoeksresultaten

5.2.1 Grondhouding

Gekeken naar de grondhouding (figuur 10) valt op dat de drie groepen weinig coherentie vertonen. De oude economie is overwegend reactief-actief, de nieuwe economie is enigszins diffuus maar overwegend inactief en Telecom is nadrukkelijk actief. Hoe ondernemingen tegen privacy aankijken, lijkt derhalve samen te hangen met welke economie wordt vertegenwoordigd.



Figuur 10. Grondhouding richting privacy

Oude economie

De oude economie ziet privacy als een fundamenteel mensenrecht. Dit uit zich onder meer door het onderschrijven van artikel 12 van de 'Universele Verklaring van de Rechten van de Mens'³⁰ waarin inmenging in iemands persoonlijke levenssfeer wordt afgewezen.

[Philips] With due regard to the Universal Declaration of Human Rights, which states that all parties in society, including corporate persons, have a duty to respect and safeguard human rights, and within the framework of the legitimate role of business, Philips supports and respects human rights and strives to ensure that its activities do not make it an accessory to infringements of human rights. [...] The privacy of personally identifiable information about customers, employees, business partners and other individuals will be protected.³¹

[Rabobank] De Rabobank Groep respecteert de rechten van de mens. Zij wil niet betrokken zijn bij omstandigheden die de waardigheid van de mens aantasten.³²

[G4S] is committed to fulfilling its responsibilities on human rights around the world by applying the United Nations Guiding Principles on Business and Human Rights (2011).³³

³⁰ <http://www.un.org/en/documents/udhr/index.shtml#a12>

³¹ http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/GeneralBusinessPrinciples.pdf

³² https://www.rabobank.com/nl/images/Gedragcode_Rabobank_Groep.pdf

De redenen waarom de oude economie privacy belangrijk vindt, zijn divers zoals: (1) conformeren aan wet- en regelgeving; (2) behartigen van klantbelangen; (3) integriteit; en (4) voorkomen van reputatieschade.

[ING] Het gebruik van Big Data kent vele mogelijkheden, maar zoals voor veel zaken geldt: niet alles wat mogelijk is, is wenselijk. Voor ING staat bescherming van de persoonsgegevens van haar klanten altijd voorop. Want we realiseren ons dat privacy een groot goed is. ING zal nooit individueel herleidbare klantdata doorgeven aan derden en klanten kunnen erop vertrouwen dat ING uitsluitend gebruik maakt van hun persoonsgegevens wanneer dat ook is toegestaan. We zullen hierin altijd compliant handelen, in overeenstemming met de wetgeving en onze business principles.³⁴

[Rabobank] Voor de Rabobank Groep staat het belang van de klant – uw belang – te allen tijde centraal. Dat betekent dat wij financiële diensten, -producten én oplossingen bieden, die voor u waardevol zijn en aansluiten bij uw situatie. Gebaseerd op integriteit en wederzijds respect.³⁵

[G4S] Integriteit is de kern van onze dienstverlening. Klanten vertrouwen hun veiligheid aan ons toe en dat vertrouwen mogen we nooit beschamen. Klanten kunnen erop vertrouwen dat wij altijd de juiste dingen doen. Maar integriteit is meer. Het is ook respect hebben voor anderen, voor andermans mening, gedrag, gevoelens en eigendommen. G4S heeft een open cultuur. Dat betekent dat we elkaar kunnen aanspreken op gedrag, kritiek durven geven en kritiek kunnen ontvangen.³⁶

[Ahold] Disclosure of confidential information to unintended third parties may negatively impact Ahold's corporate reputation and competitive position or result in litigation or regulatory action. This could have a material adverse effect on Ahold's financial position. (Ahold, 2013)

De oude economie (met name de banken) zegt veel waarde te hechten aan het klantbelang in de betekenis van respect voor privacy. De keerzijde hiervan is dat de potentiële waarde van persoonsgegevens niet of slechts deels benut kan worden voor 'slimme dingen'.

Nieuwe economie

De enigszins diffuse houding bij de nieuwe economie wordt verklaard door de sterk uiteenlopende visies op privacy bij de individuele vertegenwoordigers. Daar waar Facebook en Google inactief zijn, is WhatsApp reactief en Qiy proactief. Dit impliceert dat: (1) vertegenwoordigers van de nieuwe economie niet per se anti-privacy zijn; en (2) privacy relevant is voor de business modellen van de nieuwe economie hetzij door het te negeren, hetzij door het te omarmen. Facebook vindt privacy belangrijk voor zover dit betrekking heeft op het onderling delen van persoonsgegevens onder gebruikers; over het aanwenden van persoonsgegevens voor commerciële doeleinden, hebben Facebook gebruikers echter geen zeggenschap (Fuchs, 2011).

[Facebook] Protecting user privacy is an important part of our product development process. Our objective is to give users choice over what they share and with whom they share it. This effort is fundamental to our business and focuses on control, transparency, and accountability. (Facebook, 2013)

[Facebook]-advertenties zijn ontworpen om adverteerders te helpen gebruikers advertenties te laten zien die interessant en relevant voor ze zijn. [...] Bedrijven betalen Facebook om advertenties te laten zien aan personen die mogelijk interesse hebben in hun boodschap.³⁷

³³ http://www.g4s.com/~media/Files/Corporate%20Files/Group%20Policies/g4s_business_ethics_policy.ashx

³⁴ http://www.ing.nl/nieuws/nieuws_en_persberichten/2014/03/ing_en_het_gebruik_van_klantdata.aspx

³⁵ https://www.rabobank.nl/particulieren/servicemenu/privacy/privacy_statement/

³⁶ <http://www.g4s.nl/nl-NL/over%20G4S/Kernwaarden/>

³⁷ <https://www.facebook.com/about/ads/#personal>

De Qiy Foundation geeft gebruikers wel controle over het delen van informatie met andere commerciële partijen. Zij biedt gebruikers een platform voor het verhandelen van hun gegevens: “Dit vanuit het principe het individu te faciliteren met een gewaarborgde digitale identiteit in combinatie met een eigen omgeving”³⁸.

[Qiy] De Qiy Foundation heeft al vijf jaar geleden een visie ontwikkeld op een wereld waarin het individu écht centraal staat. En daarmee weer de regie kan nemen over zijn of haar informatie en daar bovendien slimme en handige combinaties mee kan maken.³⁹

Google realiseert zich dat technologie de privacy kan bedreigen; in haar overwegingen lijken echter vooral de eigen belangen een rol te spelen en niet die van de gebruikers. In deze houding zijn de aspecten gerelateerd aan een inactieve-reactieve opstelling herkenbaar zoals het voorkomen van reputatieschade, nadruk op winsttoegmerk en efficiëntie.

[Google] Privacy concerns relating to our technology could damage our reputation and deter current and potential users from using our products and services. (Google Inc., 2012)

Telecom

De relevantie van privacy voor Telecom is hoog. Zowel KPN als UPC zien het als hun verantwoordelijkheid en plicht om de persoonlijke gegevens te beschermen. Beide ondernemingen lijken intrinsiek gemotiveerd te zijn om de privacy belangen van klanten te behartigen hetgeen duidt op een actieve houding.

[KPN] Klanten kunnen erop rekenen dat bij KPN privacy en veiligheid prioriteit hebben. Het bewaken van de vertrouwelijkheid van communicatie is al meer dan een eeuw het fundament van onze onderneming.⁴⁰

[UPC] Omdat de bescherming van uw persoonlijke informatie één van de belangrijkste kernwaarden van ons bedrijf is, hanteren wij een brede uitleg van het begrip ‘persoonlijke informatie’.⁴¹ Garanderen van de privacy en de veiligheid blijft het belangrijkste.⁴²

Het belang dat Telecom aan privacy hecht wordt ook duidelijk uit de al genoemde ‘Golden rules’ van KPN en de lancering van de ‘Blackphone’. UPC blijkt daarnaast te participeren in diverse beleidsmakende privacy-gremia waaronder het ECP (Electronic Commerce Platform Nederland), Nederland ICT en VNO-NCW.⁴³

³⁸ <https://www.pvib.nl/download/?id=17680837&download=1>

³⁹ <https://www.pvib.nl/download/?id=17680837&download=1>

⁴⁰ <http://www.kpn.com/algemeen/missie-en-privacy-statement/onze-missie.htm>

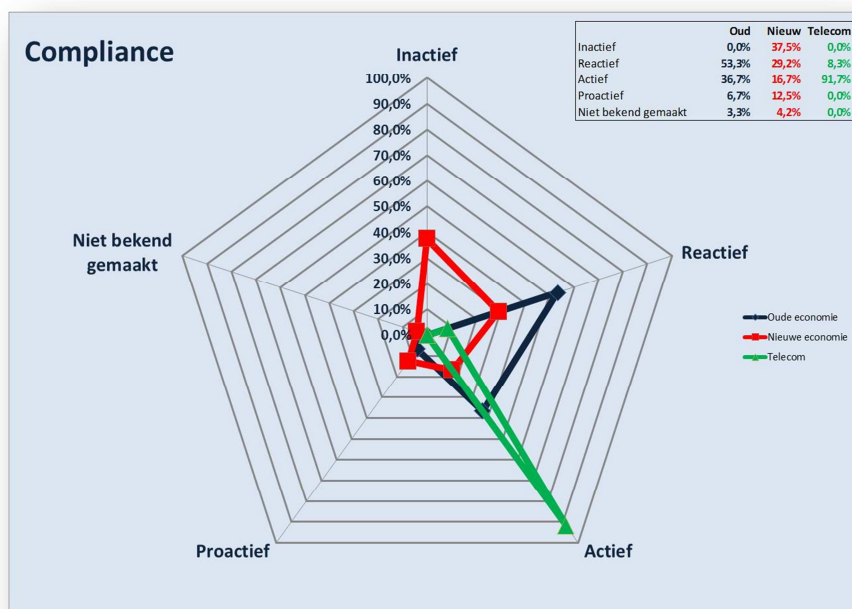
⁴¹ <http://www.upc.nl/pdf/upc-privacy-policy.pdf>

⁴² <http://www.upc.nl/pdf/over-upc-maatschappelijk-overzicht-2012.pdf>

⁴³ <http://www.upc.nl/pdf/over-upc-maatschappelijk-overzicht-2012.pdf>

5.2.2 Compliance

Gekeken naar compliance (figuur 11) valt op dat de drie groepen weinig coherent zijn. De oude economie is overwegend reactief-actief, de nieuwe economie is enigszins diffuus maar overwegend inactief en Telecom is nadrukkelijk actief. De mate waarin ondernemingen privacy compliant willen zijn, lijkt samen te hangen met welke economie wordt vertegenwoordigd.



Figuur 11. Compliance attitude

Oude economie

Een deel van de oude economie committeert zich in algemene bewoordingen aan de geldende wet- en regelgeving.

[Ahold] At Ahold, an essential part of responsible retailing is behaving according to our values. One of Ahold's values is "Doing what's right," which means that the Company and all its employees are responsible for acting with honesty, integrity, and respect for others. We strive to comply with applicable laws and regulations everywhere we do business. (Ahold, 2013)

[G4S] will comply fully with all relevant national and international laws and will act in accordance with local guidelines and regulations, including those which are industry specific, governing our operations."⁴⁴

De banken geven expliciet aan de wetgeving rondom de bescherming van persoonsgegevens te respecteren. Daarnaast hanteren zij de 'Gedragscode Verwerking Persoonsgegevens Financiële Instellingen'.

[Rabobank] De Rabobank Groep is gebonden aan de Wet bescherming persoonsgegevens. Zij onderschrijft de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen, die is opgesteld door de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars. Deze gedragscode is een uitwerking van de wettelijke bescherming van de omgang met persoonsgegevens van klanten.⁴⁵

⁴⁴ http://www.g4s.com/~media/Files/Corporate%20Files/Group%20Policies/g4s_business_ethics_policy.ashx

⁴⁵ https://www.rabobank.nl/particulieren/servicemenu/privacy/privacy_statement/

[ING] De Nederlandse banken die aangesloten zijn bij de Nederlandse Vereniging van Banken, hebben afspraken gemaakt over hoe zij omgaan met uw gegevens. Deze regels zijn vastgelegd in de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen. Deze Gedragscode is een uitwerking van de Wet bescherming persoonsgegevens (Wbp), speciaal voor de financiële sector.⁴⁶

De gedragscode voorziet eveneens in regels rondom doelbinding. Met het onderschrijven van de 'guidelines' van de OECD⁴⁷ (met name de artikelen 9 en 10 uit deel 2), belooft ook Philips persoonlijke gegevens niet voor andere doelen te gebruiken dan waarvoor deze zijn verkregen.⁴⁸ Philips vindt het daarnaast belangrijk om belanghebbenden te informeren over hoe persoonlijke gegevens worden gebruikt.

[Philips] hecht veel waarde aan het beschermen van de privacy van de persoonlijke herkenbare gegevens die u aan ons verstrekt. Wij zijn tevens van mening dat het van belang is u te informeren over de manier waarop wij uw persoonlijke gegevens gebruiken, en u daarnaast keuzes te bieden over hoe de gegevens worden gebruikt. Wij raden u dus aan om deze Privacy Policy zorgvuldig door te lezen.⁴⁹

ING is terughoudend in het participeren in belangenorganisaties vanwege: (1) de tegengestelde belangen van de diverse stakeholders zoals de FIOD, belastingdienst, consumentenbond en de Nederlandse Bank; (2) verplichtende wet- en regelgeving waardoor er geen ruimte voor 'onderhandeling' is; en (3) de 'slechte' reputatie van de sector.⁵⁰

Rondom het gebruik van cookies lijkt de oude economie zich te houden aan de daarvoor geldende regels.

Met betrekking tot G4S is het opmerkelijk dat het woord privacy nauwelijks voorkomt in het jaarverslag van 2013, nog in de 'business ethics policy', nog in het 'social responsibility commitment'. Vanwege de aard van de bedrijfsactiviteiten (beveiliging) is het echter aannemelijk om een privacy belang te veronderstellen.

Nieuwe economie

Een deel van de nieuwe economie ziet compliance als een bedreiging vanwege de potentiële hoge kosten die daaraan verbonden zijn. In hun pogingen te voldoen aan wetgeving, lijken deze ondernemingen daarnaast risico te lopen vanwege afwijkende interpretaties van wet- en regelgeving dan door henzelf begrepen en geoperationaliseerd.

[Google] The costs of compliance with these laws and regulations are high and are likely to increase in the future and any failure on our part to comply with these laws may subject us to significant liabilities and other penalties. [...] It is possible that these laws may be interpreted and applied in a manner that is inconsistent with our data practices. (Google Inc., 2012)

[Facebook] Our efforts to comply with these laws and regulations could be costly and result in diversion of management time and effort and may still not guarantee compliance. (Facebook, 2013)

In haar jaarverslag van 2013 lijkt Facebook te beseffen dat er in haar privacy beleid ruimte voor verbetering is.

[Facebook] We agreed to enhance various data protection and privacy practices to ensure compliance with the law and adherence to industry best practices. (Facebook, 2013)

⁴⁶ <http://www.ing.nl/de-ing/privacy-statement/bezoek-aan-ing-websites/index.aspx>

⁴⁷ http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/GBPDirectives2011.pdf

⁴⁸ <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>

⁴⁹ <http://www.philips.nl/privacypolicy>

⁵⁰ Interview 15-5-2014

Rondom compliance lijkt Qiy een actieve-proactieve houding aan te nemen getuige haar expliciete comittingering aan de WBP en hoogst mogelijke security en privacy certificering. Evenals bij de grondhouding indicator, is de houding hier significant anders dan die van Google en Facebook.

[Qiy] BV voldoet geheel aan de verplichtingen die uit hoofde van de Wet Bescherming Persoonsgegevens op haar rusten: Qiy BV verzamelt en verwerkt alleen die persoonsgegevens die strikt noodzakelijk zijn om diensten aan jou te kunnen verlenen.⁵¹

[Qiy] Qiy is privacy gecertificeerd op het hoogste niveau op het gebied van security en privacy met het keurmerk Privacy-Audit-Proof van Nivra/Norea.⁵²

Ten aanzien van cookies kiest Qiy ervoor om deze niet te gebruiken. Volgens Qiy bestaat hiervoor geen technische noodzaak hetgeen opmerkelijk is omdat andere ondernemingen zoals ING dit wel suggereren.⁵³

Telecom

Het belang van privacy komt bij KPN en UPC tot uiting in het hanteren van een keurmerk en de participatie in belangenorganisaties.

[UPC] Door ons lidmaatschap committeren wij ons aan de afspraken over integere commerciële communicatie die DDMA voor de dialoogmarketingsector heeft opgesteld.⁵⁴

[UPC] Zo nemen medewerkers vanuit het UPC online team zitting in een aantal werkgroepen van de Dutch Dialogue Marketing Association (DDMA) en het Interactive Advertising Bureau (IAB). Daarbij wordt veel gesproken over privacy en er wordt ook daadwerkelijk beleid gemaakt voor de gehele sector.⁵⁵

[KPN] Op het gebied van privacy en veiligheid werken we nauw samen met andere partijen. Met ons brede diensten- en productenportfolio voor alle onderdelen van de maatschappij laten we bovendien zien dat veiligheid en privacy voor KPN de hoogste prioriteit heeft en altijd zal houden.⁵⁶

Evenals de banken geeft KPN expliciet aan zich te houden aan geldende privacy wet- en regelgeving: “We abide by all relevant privacy laws. In case of violations, we immediately take necessary actions” (KPN, 2013). Ten aanzien van het gebruik van cookies, springt de gebruikersvriendelijkheid van de UPC website in het oog. Sinds 1 januari 2013 wordt er een duidelijke cookie opt-in gehanteerd waarbij bezoekers van de website een keuze kunnen maken welke cookies zij willen accepteren.⁵⁷

⁵¹ <https://www.qiy.nl/nl/privacy/>

⁵² <https://www.pvib.nl/download/?id=17680837&download=1>

⁵³ <http://www.ing.nl/de-ing/privacy-statement/bezoek-aan-ing-websites/index.aspx>

⁵⁴ <http://ddma.nl/ddma-nieuws/leden-aan-het-woord-jeroen-millenaar-van-upc/>

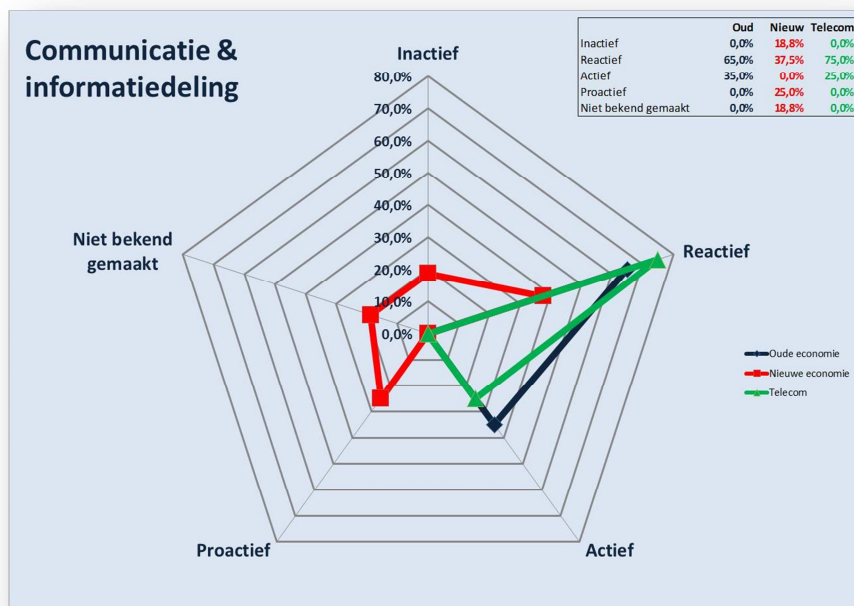
⁵⁵ <http://www.upc.nl/pdf/over-upc-maatschappelijk-overzicht-2012.pdf>

⁵⁶ <http://corporate.kpn.com/voor-nederland/privacy-security.htm>

⁵⁷ <http://www.upc.nl/pdf/over-upc-maatschappelijk-overzicht-2012.pdf>

5.2.3 Communicatie en informatiedeling

Gekeken naar communicatie en informatiedeling (figuur 12) valt op dat de reactieve houding van de oude economie vrijwel gelijk is aan de houding van Telecom. De nieuwe economie is diffuus maar neigt naar reactief. Voor diverse ondernemingen geldt dat vanwege hun notering aan een aandelenbeurs en de daaruit voortvloeiende verplichtingen, openheid moet worden gegeven over de beloning en compensatie van bestuurders. Derhalve konden er hieromtrent weinig onderscheidende aanwijzingen worden gevonden.



Figuur 12. Communicatie & informatiedeling attitude

Oude economie

De oude economie blijkt persoonsgegevens te delen met andere bedrijfsonderdelen maar ook met derde partijen. Een reden is dat deze derde partijen een aandeel hebben in de keten; teneinde hun taak daarin te kunnen vervullen, lijkt toegang tot deze gegevens noodzakelijk te zijn.

[ING] De ING opereert wereldwijd en wisselt in het kader van haar dienstverlening persoonsgegevens uit binnen de ondernemingen die onder de ING vallen, met bewerkers en andere partijen.⁵⁸

Daar waar ING elders aangeeft persoonsgegevens niet met derden te delen⁵⁹, dient de nuance aangebracht te worden dat daarmee alleen derden worden bedoeld die geen overeenkomst met ING hebben. G4S stelt dat persoonlijke informatie niet met derden wordt gedeeld.⁶⁰

Hoe de oude economie met persoonlijke gegevens omgaat, is in privacy statements of privacy policies vastgelegd. De drijfveren lijken sterk gerelateerd te zijn aan het voldoen aan wet- en regelgeving zoals bijvoorbeeld bleek bij ING ten aanzien van het gebruik van zwarte lijsten ter voorkoming van fraude en

⁵⁸ <http://www.ing.nl/de-ing/privacy-statement/omgang-met-uw-persoonsgegevens/index.aspx>

⁵⁹ http://www.ing.nl/nieuws/nieuws_en_persberichten/2014/03/ing_en_het_gebruik_van_klantdata.aspx

⁶⁰ <http://www.g4s.nl/nl-NL/Site%20Tools/Privacy/>

wanbetalingen. ING stelt dit te doen binnen de geldende wettelijke kaders en voorziet daarbij in een klachten- en bezwaarprocedure.⁶¹

Nieuwe economie

In vergelijking met de oude economie en Telecom, typeert het delen van persoonsgegevens met derden de houding van de nieuwe economie. Dit wordt verklaard doordat Facebook en Google hun bestaansrecht daaraan ontleen. WhatsApp blijkt ook gegevens met derden te delen voor zover dit ten goede komt aan haar dienstverlening.

[WhatsApp] We may share your Personally Identifiable Information with third party service providers to the extent that it is reasonably necessary to perform, improve or maintain the WhatsApp Service.⁶²

Telecom

KPN en UPC dragen hun visie op privacy zichtbaar uit in jaarverslagen en maatschappelijke overzichten. Beide ondernemingen richten zich op bewustwording en gedragsveranderingen bij stakeholders. Ook wordt de dialoog aangegaan waarbij wordt gezocht naar mogelijkheden om te profiteren van de voordelen van 'big data' zonder daarbij de klantbelangen te ondermijnen.

[KPN] Privacy and security are an integral part of our business. To embed privacy and security even better in our organization, we continued our program to increase employee awareness of privacy and security and to stimulate and monitor the required behavior according to our internal policies. [...] There is a balance to be found and KPN attempts to play a key role in this debate: how to reach the benefits of this 'big data' without jeopardizing the privacy of our customers? (KPN, 2013)

[UPC] Privacy is geen statisch begrip. Bewustwording, educatie en dialoog zijn daarom ook belangrijke instrumenten in privacybeleid. UPC is tegen die achtergrond ook richting stakeholders actief.⁶³

Rondom het delen van persoonlijke informatie met derden zegt UPC: "Wij kunnen ook persoonlijke informatie delen met krediettoetsingsinstellingen of incassobureaus."⁶⁴ KPN blijkt te participeren in Preventel⁶⁵, een stichting binnen de telecom sector die zich bezighoudt met de registratie van wanbetalers. Via deze stichting worden persoonsgegevens gedeeld met andere ondernemingen die eveneens bij Preventel zijn aangesloten.

⁶¹ Interview 15-5-2014

⁶² <http://www.whatsapp.com/legal/#Privacy>

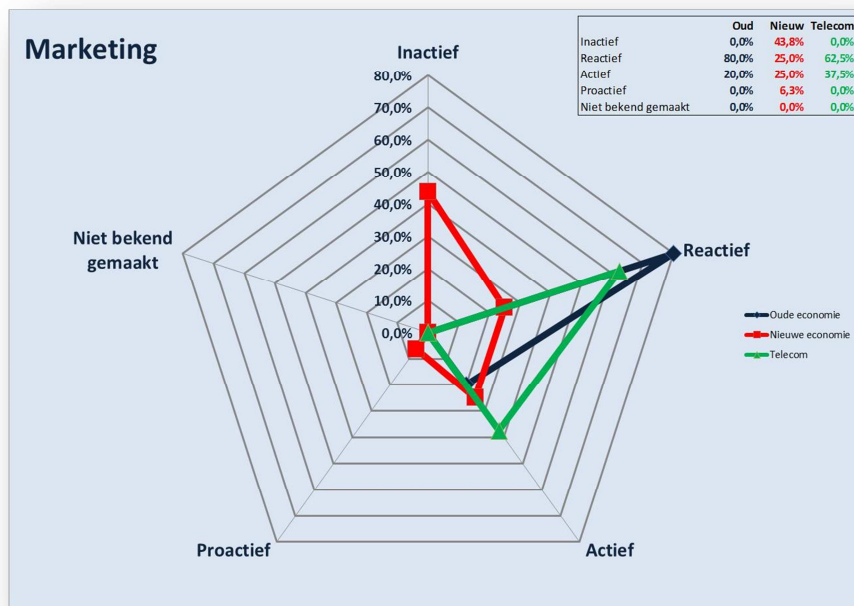
⁶³ <http://www.upc.nl/pdf/over-upc-maatschappelijk-overzicht-2012.pdf>

⁶⁴ <http://www.upc.nl/pdf/upc-privacy-policy.pdf>

⁶⁵ Zie hoofdstuk 3

5.2.4 Marketing

Gekeken naar marketing (figuur 13) valt op dat de houding van de nieuwe economie overwegend inactief is. De houdingen van de oude economie en Telecom vertonen grote overeenkomsten en stellen zich ten aanzien van marketing reactief op.



Figuur 13. Marketing attitude

Oude economie

De oude economie verzamelt persoonsgegevens ten behoeve van marketing doeleinden en customer intelligence activiteiten. De privacy beschermende maatregelen die daarbij worden genomen zijn anonimisering, opt-in en opt-out.

[Philips] To the extent required by applicable law, when Processing Personal Data for the purpose of making direct marketing communications, Philips will either: (i) obtain the prior affirmative consent ("opt-in") of the targeted individual; or (ii) offer the individual the opportunity to choose not to receive such communications ("opt-out").⁶⁶

[ING] Om marketingactiviteiten uit te kunnen voeren verwerken wij persoonsgegevens van onze klanten, zoals uw adresgegevens, e-mailadres en uw bezoek aan onze webpagina's. Op basis van gegevens uit interne, externe bronnen en uw bezoek aan onze webpagina's, zoals Mijn ING, doet de ING u passende en gerichte commerciële aanbiedingen, bijvoorbeeld via post, telefoon of internet. [...] We weten van welke ING producten u gebruik maakt en ook kunnen we zien wie bijvoorbeeld studiefinanciering ontvangt. Op basis van deze gegevens kunnen we u aanbiedingen doen die aansluiten bij uw persoonlijke situatie en interesses.⁶⁷

[Rabobank] Voor de KoopstromenMonitor *[analyseert bestedingen van consumenten]* vormen echter de gemeten geanonimiseerde pintransacties van Rabobank-klanten de basis. Miljoenen pintransacties liggen aan het model ten grondslag. Daarbij is de privacy gegarandeerd omdat individuele klantgegevens onder geen enkele voorwaarde herkenbaar of herleidbaar zijn.⁶⁸

⁶⁶ http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/PhilipsPrivacyRulesCSBData.pdf

⁶⁷ <http://www.ing.nl/de-ing/privacy-statement/gebruik-van-uw-persoonsgegevens/index.aspx>

⁶⁸ https://www.rabobank.com/nl/press/search/2013/20130510_Rabobank_Inspelen_op_veranderend_koopgedrag_bepalend_voor_succes_detailhandel.html

ING blijkt persoonsgegevens bij derden in te kopen waardoor zij specifieke aanbiedingen kan doen zoals een spaarrekening bij een geboorte, een studentenrekening aan 17-jarigen en ‘aantrekkelijke’ rentes in periodes waarin mensen hun vakantiegeld krijgen.⁶⁹ Een deel uit het voornoemde citaat van ING was mede aanleiding voor de ophef in maart 2014⁷⁰; tijdens het interview met ING wordt benadrukt dat persoonsgegevens nooit zonder toestemming met anderen gedeeld zullen worden. De Rabobank gebruikt persoonsgegevens teneinde klanten zo goed mogelijk te kunnen adviseren. De houding van Albert Heijn is vergelijkbaar en is eveneens gericht op het verbeteren van de dienstverlening.

[Rabobank] De door u verstrekte persoonsgegevens gebruikt de Rabobank Groep om u zo goed mogelijk te kunnen adviseren over haar producten en diensten. Uw persoonsgegevens zijn beschikbaar voor alle onderdelen van de Rabobank Groep, zodat steeds een zo afgewogen en evenwichtig mogelijk advies of dienst geleverd kan worden.⁷¹

[Albert Heijn] Wij zijn dan ook voortdurend op zoek naar manieren om onze dienstverlening waar nodig te verbeteren en deze zoveel mogelijk af te stemmen op je persoonlijke wensen en behoeften. Albert Heijn gaat daarbij zorgvuldig om met je gegevens en zorgt ervoor dat elke verwerking van je gegevens voldoet aan de toepasselijke wet- en regelgeving.⁷²

Philips en ING verwerken persoonsgegevens ten behoeve van betere producten en diensten alleen na toestemming of geanonimiseerd.

[Philips] Wij willen u beter leren kennen zodat we u beter van dienst kunnen zijn. De keuze of u van deze service gebruik wilt maken, is echter geheel aan uzelf.⁷³

[ING] Wij gebruiken persoonsgegevens van klanten geanonimiseerd voor bijvoorbeeld interne analyses en productontwikkeling. Hierdoor kunnen wij onze producten en diensten voor onze klanten verbeteren.⁷⁴

Een mogelijk effect van privacy kan informatie asymmetrie zijn⁷⁵ waardoor er een onbalans in de machtsverhoudingen ontstaat. De ‘Gedragscodex Verwerking Persoonsgegevens Financiële Instellingen’ bevat aanwijzingen voor de verwerking van bijzondere persoonsgegevens. Banken en verzekeraars mogen bijvoorbeeld onder voorwaarden medische en strafrechtelijke gegevens verwerken voor het beoordelen en accepteren van potentiële klanten als ook om uitvoering te geven aan bestaande overeenkomsten met klanten.

Nieuwe economie

De inactieve houding van de nieuwe economie wordt gekenmerkt door het negeren of ontkennen van privacy belangen. Voor Facebook gebruikers betekent dit dat alle informatie die zij delen, kan worden gebruikt voor marketing doeleinden.

[Facebook] We enable marketers to engage with more than 1.2 billion monthly active users (MAUs) on Facebook or subsets of our users based on information they have chosen to share with us such as their age, location, gender, or interests. (Facebook, 2013)

WhatsApp kiest voor een advertentievrij product maar lijkt niet te kunnen garanderen dat dit altijd zo zal blijven. Daarnaast behoudt WhatsApp zich het recht voor om in voorkomende gevallen marketing

⁶⁹ Interview 15-5-2014

⁷⁰ Zie hoofdstuk 1

⁷¹ https://www.rabobank.nl/particulieren/servicemenu/privacy/privacy_statement/

⁷² <http://www.ah.nl/privacy>

⁷³ <http://www.philips.nl/privacypolicy>

⁷⁴ <http://www.ing.nl/de-ing/privacy-statement/gebruik-van-uw-persoonsgegevens/index.aspx>

⁷⁵ Zie hoofdstuk 2

boodschappen te versturen. In dat geval krijgen gebruikers wel de mogelijkheid om hier middels een opt-in (actief) of opt-out (reactief) van af te zien.

[WhatsApp] We are not fans of advertising. WhatsApp is currently ad-free and we hope to keep it that way forever. We have no intention to introduce advertisement into the product, but if we ever do, will update this section. [...] We do not use your mobile phone number or other Personally Identifiable Information to send commercial or marketing messages without your consent or except as part of a specific program or feature for which you will have the ability to opt-in or opt-out.⁷⁶

Google ziet 'customer intelligence' als een onderscheidende factor in haar waardepropositie richting haar 'betalende' klanten.

[Google] Marketing is responsible for generating advertiser revenue through marketing campaigns to small businesses, as well as providing thought leadership to chief marketing officers through industry insight, research, and analysis. (Google Inc., 2012)

By Qiy hebben gebruikers volledige controle over het gebruik van hun gegevens voor marketing activiteiten.

[Qiy] Middels Qiy ontstaat een zeer relevante vorm van 'permission based marketing'. [...] Met Qiy zit de consument aan het stuur. Qiy verandert daarmee het begrip Customer Relationship Management daadwerkelijk in Customer Managed Relations.⁷⁷

[Qiy] Er gaat nooit informatie uit jouw Qiy zonder dat je hiervoor toestemming geeft en er komt geen informatie in zonder jouw toestemming.⁷⁸

Het verbeteren van de dienstverlening wordt door vertegenwoordigers van de nieuwe economie als argument aangevoerd voor het verzamelen van gebruiks- en persoonlijke gegevens.

[Google] We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.⁷⁹

[WhatsApp] In order to provide the WhatsApp Service, WhatsApp will periodically access your address book or contact list on your mobile phone to locate the mobile phone numbers of other WhatsApp users ("in-network" numbers), or otherwise categorize other mobile phone numbers as "out-network" numbers, which are stored as one-way irreversibly hashed values.⁸⁰

De toegang tot de adresboeken die WhatsApp zich permitteert beoordeelde het CBP in 2013 als onrechtmatig.⁸¹ Begin 2014 dreigde het CBP zelfs met een dwangsom omdat nog steeds niet werd voldaan aan de Nederlandse wetgeving.

Telecom

De houding van Telecom ten aanzien van marketing is overwegend reactief. Telecom verzamelt klantgegevens voor de levering van diensten. Het voldoen aan wet- en regelgeving lijkt daarbij een belangrijke voorwaarde te zijn.

⁷⁶ <http://www.whatsapp.com/legal/#Privacy>

⁷⁷ <https://www.pvib.nl/download/?id=17680837&download=1>

⁷⁸ <https://www.qiy.nl/nl/privacy/>

⁷⁹ <http://www.google.com/intl/en/policies/privacy/>

⁸⁰ <http://www.whatsapp.com/legal/#Privacy>

⁸¹ http://www.cbpreweb.nl/Pages/pb_20130128-whatsapp.aspx

[KPN] Wij respecteren alle relevante wetgeving voor het beschermen van de privacy van onze klanten. Dit houdt in dat we niet meeluisteren en -kijken in de communicatie van onze klanten. We gebruiken de gegevens van onze klanten, voor zover we ze nodig hebben, uitsluitend voor de levering van de diensten en de uitvoering van de overeenkomst met onze klanten.⁸²

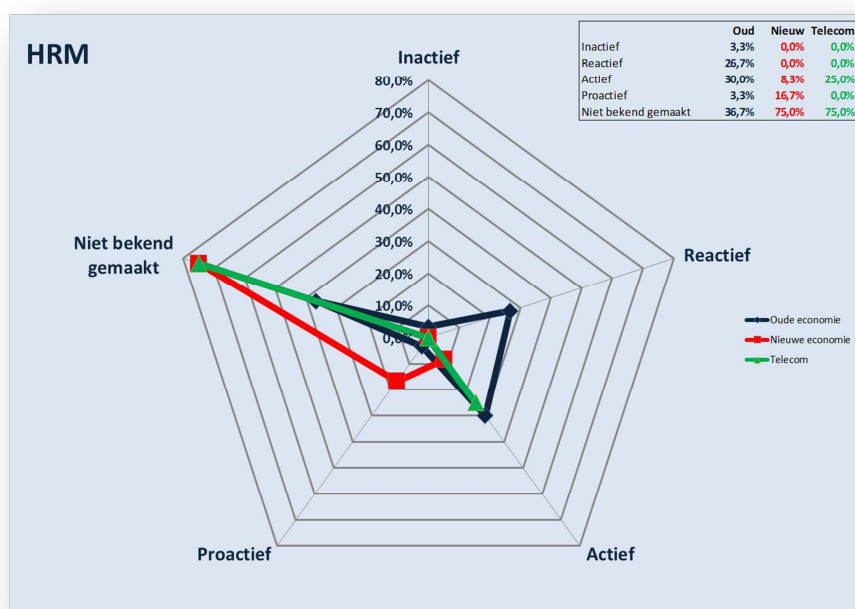
[UPC] Wij zijn steeds op zoek naar manieren om onze diensten en producten te verbeteren en ze zoveel mogelijk af te stemmen op uw persoonlijke behoeften. Daarom kunnen wij, met uw toestemming voor zover vereist, persoonlijke informatie verzamelen voor de volgende doelen [...].⁸³

⁸² <http://corporate.kpn.com/voor-nederland/privacy-security.htm>

⁸³ <http://www.upc.nl/pdf/upc-privacy-policy.pdf>

5.2.5 Personeelsbeleid (HRM)

Het vaststellen van de houding richting privacy vanuit het HRM perspectief (figuur 14), is vanwege onvoldoende openbare informatie niet mogelijk gebleken. De meeste aanwijzingen konden worden gevonden bij vertegenwoordigers van de oude economie; de daar aangetroffen houding lijkt overwegend reactief-actief te zijn.



Figuur 14. HRM attitude

Oude economie

De 'Gedragscode Verwerking Persoonsgegevens Financiële Instellingen'⁸⁴ vermeldt dat banken cameratoezicht mogen gebruiken voor beveiligingsdoeleinden maar ook om eventuele strafbare feiten vast te stellen.

ING stelt geen gevoelige informatie van sollicitanten te verzamelen of bij derden in te winnen tenzij daarvoor expliciet toestemming is gegeven door de persoon in kwestie.

[ING] does not collect or process any sensitive applicant data, such as data that reveals your race or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. If, owing to certain circumstances, ING does collect sensitive applicant data, the applicant's explicit prior written consent will be asked. [...] ING is committed to protecting the privacy of external and internal applicants.⁸⁵

[ING] Het inwinnen van informatie over een sollicitant bij derden vindt uitsluitend plaats, nadat de sollicitant schriftelijk toestemming heeft gegeven.⁸⁶

Het beveiligingsbedrijf G4S past screening toe en voert aan dit vanwege de aard van haar bedrijfsactiviteiten te moeten doen. Daarnaast benadrukt G4S dat medewerkers kunnen rekenen op een rechtvaardige behandeling, waardigheid en respect.

⁸⁴ http://www.cbppweb.nl/downloads_gedragcodes/gedr_financiele_instellingen.pdf

⁸⁵ <http://www.ing.jobs/Netherlands/Privacy-statement.htm>

⁸⁶ <http://www.ing.jobs/Nederland/Waarom-ING/Sollicitatiecode.htm>

[G4S] In order to protect the interests of its employees and customers, and because of the nature of its business, G4S will apply rigorous pre-employment screening and selection techniques. [...] To achieve a working environment in which team spirit and commitment to the goals and values of G4S are maintained, the Company will ensure that individual employees are treated fairly and with dignity and respect.⁸⁷

De NVP-sollicitatiecode wordt door de Rabobank⁸⁸ onderschreven.

Philips zegt rekening te houden met de privacy belangen van haar medewerkers; er blijken zelfs 'privacy rules' te bestaan met richtlijnen voor de verwerking van medewerker gegevens.

[Philips] While exercising its rights and duties as an employer, Philips shall take into account the privacy interests of its employees whenever processing their personal data, and do so only in accordance with Philips Privacy Rules for Employee Data.⁸⁹

Nieuwe economie

Met uitzondering van het bedrijf Qiy, zijn er ten aanzien van HRM geen aanwijzingen gevonden waarmee de houding van de vertegenwoordigers van de nieuwe economie geduid kon worden.

Telecom

De NVP-sollicitatiecode wordt door KPN⁹⁰ onderschreven. UPC respecteert het recht op privacy als ook geldende wetgeving rondom het gebruik van persoonsgegevens.

[UPC] We respecteren een ieders recht op privacy met betrekking tot hun persoonsgegevens. En we houden ons aan alle geldende wetgeving voor het gebruik van persoonsgegevens.⁹¹

⁸⁷ http://www.g4s.com/~media/Files/Corporate%20Files/Group%20Policies/g4s_business_ethics_policy.ashx

⁸⁸ https://www.rabobank.nl/images/privacynl_29536384.pdf

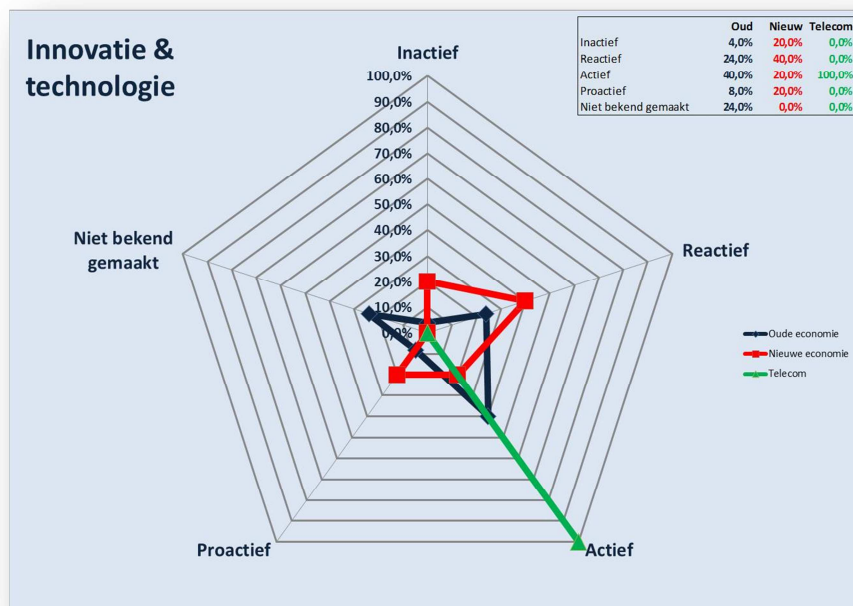
⁸⁹ http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/GBPDirectives2011.pdf

⁹⁰ <https://vacatures.werkenbijkpn.com/privacy-disclaimer.html>

⁹¹ <http://www.upc.nl/over-upc/het-bedrijf/onze-gedragscode/>

5.2.6 Innovatie en technologie

Gekeken naar innovatie en technologie (figuur 15) valt op dat Telecom een nadrukkelijke actieve houding aanneemt. De oude economie lijkt actief te zijn maar vanwege de score op 'niet bekend gemaakt' is een reactief-actieve houding aannemelijker. De nieuwe economie is overwegend reactief.



Figuur 15. Innovatie en technologie attitude

Oude economie

De trade-off privacy versus technologische vooruitgang is voor ING herkenbaar. Tijdens het interview wordt aangegeven dat altijd gezocht zal worden naar een 'positive-sum' oplossing waarmee de belangen van alle stakeholders worden gediend. ING denkt dat technologische vooruitgang niet tegengehouden kan worden; inmiddels zijn er geen beperkingen meer om iemand 7 dagen per week, 24 uur per dag te volgen. Privacy lijkt daarmee een 'fictie' te zijn en mensen zouden zich hiervan meer bewust moeten zijn. De Rabobank ziet kansen rondom technologische vooruitgang maar verbindt daar geen duidelijke privacy consequenties aan. De houding lijkt daarmee vooralsnog reactief.

[Rabobank] Nieuwe technologie en technologische ontwikkelingen bieden nieuwe mogelijkheden voor interactie met de klant. Dit kan helpen bij efficiencyverbetering door de dienstverlening beter en goedkoper te maken. Veranderingen gaan steeds sneller en daarop zal moeten worden ingespeeld. (Rabobank Groep, 2013)

Het beveiligen van informatie wordt door de oude economie belangrijk gevonden. Vrijwel alle ondernemingen blijken maatregelen te treffen ter voorkoming van indringing in hun systemen.

[Philips] Wij erkennen onze verantwoordelijkheid om de gegevens die u ons toevertrouwt te beveiligen. Philips gebruikt verschillende veilige technieken om uw gegevens te beschermen, waaronder veilige servers, firewalls, en versleuteling van financiële gegevens.⁹²

⁹² <http://www.philips.nl/privacypolicy>

[Albert Heijn] Zo beveiligen wij onze systemen en applicaties volgens de geldende standaarden voor informatiebeveiliging, zoals Control Objectives for Information 27 and related Technology (CobIT) en de Standard of Good Practice for Information Security (ISF, 2011).⁹³

[ING] Uw persoonsgegevens zijn bij de ING in goede handen. De ING zorgt ervoor dat uw gegevens goed beveiligd zijn. Veilig internetbankieren heeft daarbij bijzondere aandacht. Internetcriminelen worden immers steeds slimmer. Een speciaal team van de ING houdt zich continu bezig met de veiligheid van internetbankieren.⁹⁴

Nieuwe economie

Facebook ziet technologie als de katalysator voor het realiseren van haar missie namelijk het verbinden van mensen. Google ambieert een toonaangevende rol rondom technologie en stelt wet- en regelgeving daarbij te respecteren.

[Facebook] We build technology to enable faster, easier and richer communication" (Facebook, 2013).

[Google] Our ambition is to be at the leading edge of technology, including the development of tools that help users manage their personal information in a simple, accessible manner without detracting from a valuable user experience. We comply with privacy laws, and additionally work internally and with regulators and industry partners to develop and implement strong privacy standards.⁹⁵

Qiy committeert zich aan de 'Privacy by Design' (PbD) principes. Dit impliceert dat maximale privacy het uitgangspunt is in hun producten, diensten en organisatie.

[Qiy] Een andere belangrijke kernwaarde van Qiy is dat de infrastructuur en zelfs de hele organisatie is ingericht op basis van 'privacy by design' principes.⁹⁶

Voor Google is een korte 'time-to-market' belangrijk; in combinatie met hun missie lijkt privacy daaraan ondergeschikt te zijn.

[Google] Our product development philosophy is to launch innovative products early and often, and then iterate rapidly to make those products even better. (Google Inc., 2012)

Evenals de oude economie, spreekt ook de nieuwe economie zich nadrukkelijk uit over beveiliging. De redenen hiervoor zijn divers zoals het voldoen aan wet- en regelgeving, de bescherming van data en het voorkomen van reputatieschade.

[Facebook] As part of the audit process, we agreed to enhance various data protection and privacy practices to ensure compliance with the law and adherence to industry best practices. [...] We invest in technology, processes, and people as part of our commitment to safeguarding our users' information. (Facebook, 2013)

[Google] We expect to continue to expend significant resources to protect against security breaches. [...] Any systems failure or compromise of our security that results in the release of our users' data could seriously limit the adoption of our products and services, as well as harm our reputation and brand and, therefore, our business. (Google Inc., 2012)

[Qiy] is veilig. Data wordt opgeslagen op de eigen servers van Qiy binnen gecertificeerde datacenters in Nederland. Bovendien wordt al je informatie versleuteld opgeslagen.⁹⁷

⁹³ <http://www.ah.nl/privacy>

⁹⁴ <http://www.ing.nl/de-ing/privacy-statement/omgang-met-uw-persoonsgegevens/index.aspx>

⁹⁵ <http://www.google.com/intl/en/policies/technologies/>

⁹⁶ <https://www.pvib.nl/download/?id=17680837&download=1>

⁹⁷ <https://www.qiy.nl/nl/privacy/>

[WhatsApp] uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information.⁹⁸

Telecom

KPN onderkent de toenemende afhankelijkheid van technologie maar stelt de belangen van de klant voorop.

[KPN] Voortdurende technologische ontwikkelingen zijn van invloed op privacy en veiligheid. De ambitie van KPN is om hierbij het belang en de wensen van de klant voorop te blijven stellen.⁹⁹

[KPN] De wereld drijft op internet. De maatschappij, het bedrijfsleven en privélevens zijn in toenemende mate afhankelijk van het wereldwijde web. Steeds meer vertrouwelijke informatie wordt via internet verstuurd. De samenleving wil en mag er op vertrouwen dat ICT-dienstverleners dit dataverkeer veilig en zorgvuldig verwerken.¹⁰⁰

UPC past 'Privacy by Design' toe in hun innovatieproces waarmee het streven naar maximale privacy wordt onderstreept.

[UPC] Tijdens de ontwikkeling van IT-processen en producten, wordt 'privacy by design' toegepast om de bescherming van de persoonlijke levenssfeer van klanten te waarborgen.¹⁰¹

Ook Telecom spreekt zich expliciet uit over de beveiliging van hun systemen.

[KPN] Klanten verwachten van ons dat we hun privacy waarborgen en hun persoonsgegevens beschermen. Als grootste telecom- en ICT-provider van Nederland zijn we ons bewust van onze grote verantwoordelijkheid op dit gebied. Het is onze plicht om onze netwerken veilig te houden en de data en privacy van onze klanten te beschermen. Dit is de ruggengraat van onze dienstverlening. (KPN, 2013)

[UPC] Wij werken er hard aan om uw privacy te beschermen en hebben hiervoor belangrijke stappen ondernomen. Wij hebben formeel personen aangesteld die verantwoordelijk zijn voor de veiligheid van ons netwerk, de ondersteunende infrastructuur en onze informatiesystemen. Wij hebben oplossingen geïmplementeerd om persoonlijke informatie te beschermen.¹⁰²

⁹⁸ <http://www.whatsapp.com/legal/#Privacy>

⁹⁹ <http://www.kpn.com/algemeen/missie-en-privacy-statement/onzemissie.htm>

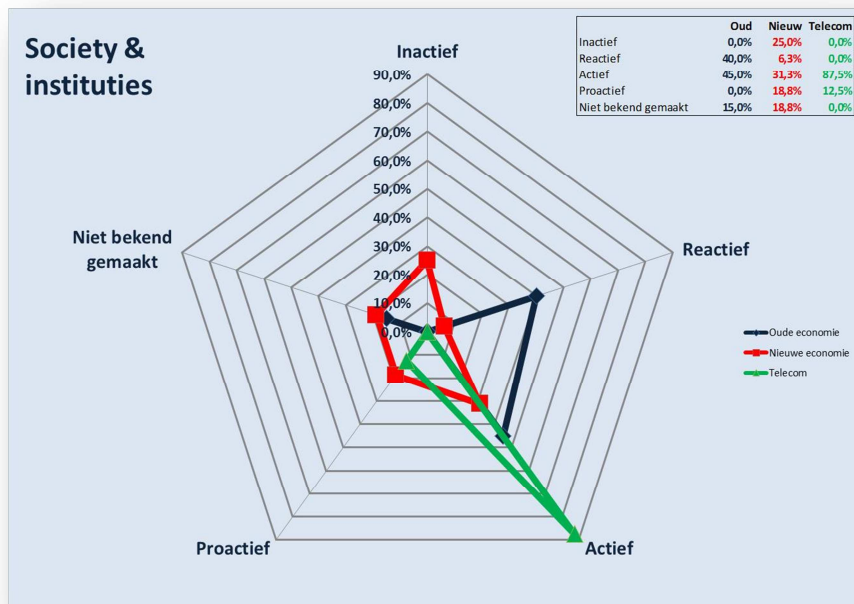
¹⁰⁰ <http://corporate.kpn.com/voor-nederland/privacy-security.htm>

¹⁰¹ <http://www.upc.nl/pdf/over-upc-maatschappelijk-overzicht-2012.pdf>

¹⁰² <http://www.upc.nl/pdf/upc-privacy-policy.pdf>

5.2.7 Society en instituties

Gekeken naar society en instituties (figuur 16) valt op dat de oude economie hier een reactieve-actieve houding aanneemt. De houding van de nieuwe economie is diffuus terwijl Telecom duidelijk actief is.



Figuur 16. Society en instituties attitude

Oude economie

Met name de banken laten zich expliciet uit over privacy als mensenrecht; in de afweging met andere fundamentele rechten, zullen trade-off's per geval beoordeeld worden.

Philips pretendeert verantwoordelijkheid te willen nemen voor een florerende samenleving. In combinatie met andere verwijzingen naar mensenrechten, lijkt Philips voorstander van een 'veilige haven' waar individuen zich vrij weten van invloeden van anderen.

[Philips] wishes to be a responsible partner in society, acting with integrity towards its shareholders, customers, employees, suppliers and business partners, competitors, governments and their agencies, and others who can be affected by its activities.¹⁰³

Nieuwe economie

Ten behoeve van meer veiligheid is afluisteren volgens Google tot op zekere hoogte toegestaan mits dit plaatsvindt binnen de kaders zoals die met elkaar zijn vastgesteld. Ook lijkt Google voorstander te zijn van het delen van medische gegevens voor research doeleinden.

[Larry Page/Google] he said, is open to the argument that national security requires the NSA and other agencies need to do some level of electronic eavesdropping — but determining the limits of that eavesdropping needs to happen in public if it's going to have the public's blessing.¹⁰⁴

¹⁰³ http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/GeneralBusinessPrinciples.pdf

¹⁰⁴ <http://www.forbes.com/sites/jeffbercovici/2014/03/19/at-ted-googles-larry-page-says-nsa-spying-threatens-democracy/>

[Larry Page/Google] Wouldn't it be amazing if everyone's medical records were available anonymously to research doctors?¹⁰⁵

Google zet in op een open internet; dit sluit aan op haar missie om alle informatie te organiseren en toegankelijk te maken.

[Google] We zetten ons ook in voor een open internet en zijn daarom betrokken bij verschillende projecten die het ontwikkelaars gemakkelijker moeten maken bij te dragen aan het online ecosysteem en internet verder te ontwikkelen.¹⁰⁶

WhatsApp hecht veel waarde aan vrijheid van meningsuiting. Gezien de context waarin de volgende uitspraak is gedaan¹⁰⁷, lijkt dit zelfs meer waarde dan veiligheid te hebben.

[WhatsApp] Our focus remains on delivering the promise of WhatsApp far and wide, so that people around the world have the freedom to speak their mind without fear.¹⁰⁸

Telecom

De privacy belangen van klanten lijken voor KPN belangrijker te zijn dan de kwaliteit van haar dienstverlening. Daarnaast zoekt KPN naar een middenweg waarbij wordt geprofiteerd van technologische vooruitgang zonder dat daarbij wordt ingeboet aan veiligheid en privacy.

[KPN] We doen er alles aan om te voorkomen dat onze dienstverlening ten koste gaat van het milieu. Of ten koste van onze klanten, die onze diensten moeten kunnen gebruiken in de volle overtuiging dat hun privacy gewaarborgd is. (KPN, 2013)

[KPN] We geloven in een samenleving waarin communicatietechnologie het leven verrijkt. Het maakt het alledaagse leven aangenamer en kan echt het verschil maken. Dit brengt een grote verantwoordelijkheid met zich mee: de dienstverlening moet van hoge kwaliteit zijn en veiligheid en privacy moeten worden beschermd. (KPN, 2013)

¹⁰⁵ <http://www.theverge.com/2014/3/19/5526844/larry-page-talks-privacy-medical-records-and-machines-mastering-8-bit-games>

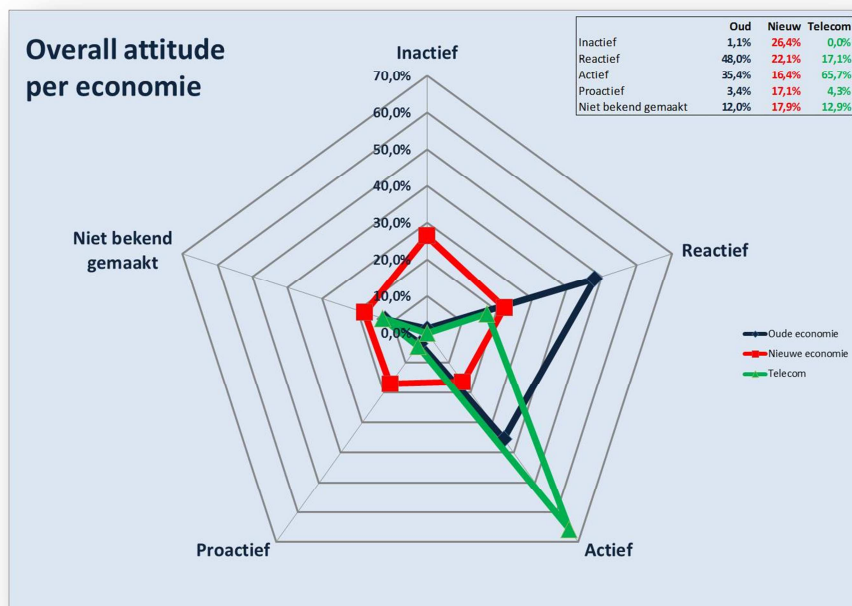
¹⁰⁶ <https://www.google.nl/about/company/products/>

¹⁰⁷ Zie hoofdstuk 3

¹⁰⁸ <http://blog.whatsapp.com/529/Setting-the-record-straight>

5.2.8 Attitude per economie

In de voorgaande paragrafen is in detail gekeken naar de houding van de onderzochte ondernemingen op de verschillende indicatoren. In deze paragraaf zal op geaggregeerd niveau worden gekeken naar de overall attitude per economie (figuur 17).



Figuur 17. Overall attitude per economie

Uit de figuur valt op te maken dat de houding van de oude economie 'reactief-actief' is. Typerend voor de oude economie is dat zij zich conformeert aan geldende wet- en regelgeving. Daarnaast wordt privacy als een fundamenteel mensenrecht gezien. Gekeken naar de onderlinge samenhang van de verschillende indicatoren (tabel 4), lijken de ambities ten aanzien van privacy verder te gaan dan feitelijk wordt waargemaakt. Daar waar er bij de grondhouding en compliance aanwijzingen waren voor een actieve houding, lijken de commerciële belangen zwaarder te wegen waardoor een reactieve houding wordt uitgelokt. Illustratief hiervoor zijn de afwijkende visies op privacy bij de afdelingen 'compliance' en 'marketing' waarnaar in het interview met Philips werd verwezen.

Indicator	Oud	Nieuw	Telecom
Grondhouding	Reactief-actief	Inactief	Actief
Compliance	Reactief-actief	Inactief-reactief	Actief
Communicatie & informatiedeling	Reactief	Reactief	Reactief
Marketing	Reactief	Inactief	Reactief
HRM	Reactief-actief	Niet bekend gemaakt	Niet bekend gemaakt
Innovatie & technologie	Actief	Reactief	Actief
Society & instituties	Reactief-actief	Actief	Actief
Overall attitude	Reactief-actief	Inactief-reactief	Actief

Tabel 4. Attitudes per indicator

De houding van de nieuwe economie is overwegend inactief-reactief. Opmerkelijk in deze populatie zijn de zeer uiteenlopende visies van enerzijds Google en Facebook versus Qiy. De houding van WhatsApp lijkt zich tussen beide extremen te bevinden. Gekeken naar de onderlinge samenhang van de verschillende indicatoren lijkt de nieuwe economie consistent te zijn in haar denken inclusief de genoemde extremen. De actieve houding bij society & instituties wordt veroorzaakt doordat Qiy uitgesproken (pro)actief is en de 'niet bekend gemaakt' score bij Facebook.

Telecom blijkt het meest actief te zijn richting privacy en is in haar uitingen ook het meest uitgesproken waarbij er veelal een directe verwijzing naar privacy wordt gelegd. Dit komt onder meer tot uiting in de 'Golden rules' en de committering aan de 'Privacy by Design' principes. Desondanks lijken ook de ambities van Telecom verder te reiken dan in de praktijk wordt waargemaakt gegeven de hogere scores op grondhouding en compliance in vergelijking met communicatie & informatiedeling en marketing. Evenals de nieuwe economie, lijkt Telecom consistent te zijn in haar denken gezien de redelijk vergelijkbare houdingen op de afzonderlijke indicatoren.

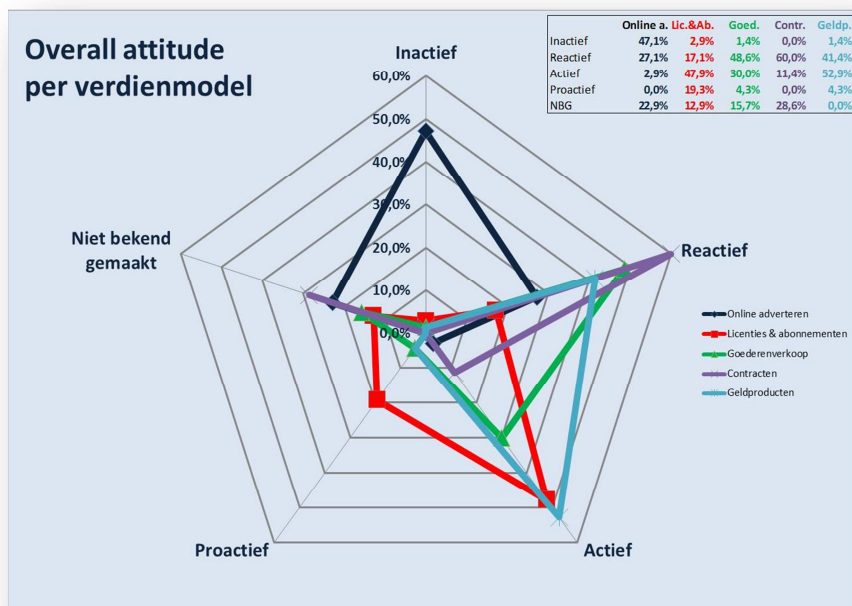
Gekeken naar de ranking (tabel 5) van de onderzochte ondernemingen, valt op dat de lijst wordt aangevoerd door een nieuwe economie onderneming gevolgd door Telecom. De oude economie neemt een middenpositie in terwijl de overige nieuwe economie ondernemingen zich aan de onderkant van de ranking bevinden. De vertegenwoordigers van de nieuwe economie vormen dus beide uitersten van de ranking hetgeen impliceert dat de visie op privacy niet per se afhankelijk is van welke economie wordt vertegenwoordigd.

Ranking	Onderneming	NBG	Inactief	Reactief	Actief	Proactief
1	Qiy Foundation	0	0	0	11	24
2	KPN	4	0	6	23	2
3	UPC	5	0	6	23	1
4	ING	0	0	15	17	3
5	Rabobank	0	1	14	20	0
6	Philips	1	0	17	14	3
7	WhatsApp	9	4	12	10	0
8	Albert Heijn	10	1	17	7	0
9	G4S	10	0	21	4	0
10	Facebook	9	16	9	1	0
11	Google	7	17	10	1	0

Tabel 5. Ranking op gecumuleerde score bij actief en proactief (in aantallen)

5.2.9 Attitude per verdienmodel

Figuur 18 toont de visies op privacy vanuit het perspectief van de diverse verdienmodellen. De verschillende houdingen kunnen als volgt worden getypeerd: (1) online adverteren is inactief; (2) licenties & abonnementen is actief; (3) goederenverkoop is reactief; (4) contracten is reactief; en (5) geldproducten is reactief-actief.



Figuur 18. Overall attitude per verdienmodel

In hun onderlinge samenhang bevindt de meeste overlap zich in het reactief-actieve spectrum. De inactieve houding van online adverteren wijkt hier significant van af terwijl er bij licenties & abonnementen een afwijking naar proactief is waar te nemen.

Online adverteren

De houding van 'online adverteren' is inactief hetgeen wordt verklaard doordat dit verdienmodel afhankelijk is van de beschikbaarheid van gratis persoonsgegevens. Derhalve pretenderen de vertegenwoordigers (Facebook en Google) hogere doelen na te streven waarbij het openlijk en met meer mensen delen van informatie de sociale norm is.¹⁰⁹ De visie op privacy kan in dit verdienmodel worden getypeerd als 'privacy bestaat niet' hetgeen wordt bevestigd door Mark Zuckerberg, CEO van Facebook, wanneer hij stelt dat alle informatie standaard publiekelijk beschikbaar zou zijn geweest als hij opnieuw die keuze had kunnen maken. Uit de jaarverslagen van Facebook en Google blijkt dat beide bedrijven zich bewust zijn van de risico's van hun houding en een kanteling in het sentiment met voor hen negatieve consequenties niet uitsluiten.

Licenties & abonnementen

Het licentie & abonnementen model is niet afhankelijk van gratis persoonsgegevens. De actieve houding richting privacy is daarmee deels verklaard. Gekeken naar de individuele ondernemingen valt op dat zij zich nadrukkelijk uitlaten over het belang van privacy en zich verantwoordelijk voelen om die te beschermen. De visie op privacy kan in dit verdienmodel worden getypeerd als 'privacy is een basisrecht' waarbij het opvallend is dat de vertegenwoordigers van dit verdienmodel verschillende economieën vertegenwoordigen (nieuw en Telecom).

¹⁰⁹ http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#feed=/search?keyword=the+age+of+privacy+is+over

Goederenverkoop

De houding richting privacy in dit verdienmodel is reactief. Dit uit zich onder meer in: (1) de committering aan wet- en regelgeving; (2) respecteren van mensenrechten zoals verankerd in de universele verklaring van de rechten van de mens; en (3) beloftes dat zorgvuldig met persoons- en klantgegevens wordt omgegaan. De overwegend reactieve houding is opmerkelijk omdat beide vertegenwoordigers baat lijken te hebben bij maximaal inzicht in hun klanten. Dit wordt bijvoorbeeld bevestigd door de bonuskaart van Albert Heijn waarmee het koopgedrag wordt bijgehouden teneinde daarbij passende aanbiedingen te kunnen doen. Gegeven de aard van de producten, zal de koopfrequentie van klanten bij Albert Heijn aanzienlijk hoger liggen dan bij Philips. Dit doet vermoeden dat het belang van gepersonaliseerde aanbiedingen voor Philips kleiner is dan bij Albert Heijn. Toch zal ook Philips inzicht willen hebben in de voorkeuren van consumenten teneinde hun product-markt combinaties daarop af te stemmen. Daarnaast is er een privacy belang met name rondom de bescherming van medische gegevens die door de 'healthcare' producten worden gecreëerd. Ten aanzien van dit verdienmodel is het daarom aannemelijk dat een ontwikkeling in de visie op privacy zich nadrukkelijk zal manifesteren.

Contracten

Een stellingname richting privacy lijkt in dit verdienmodel het minst relevant te zijn. De houding is nadrukkelijk reactief waarbij de vertegenwoordiger(s) zich in algemene bewoordingen conformeren aan geldende wet- en regelgeving. Een mogelijke oorzaak voor het ontbreken van een uitgesproken visie op privacy is dat dit verdienmodel doorgaans op een 'business-to-business' markt van toepassing is. Inzicht in persoonsgegevens lijkt in een dergelijke markt niet bedoeld te zijn voor exploitatie maar meer voor het borgen van de condities waaronder contracten uitgevoerd worden. Bij G4S betekent dit bijvoorbeeld dat medewerkers integer en betrouwbaar moeten zijn hetgeen tijdens de sollicitatieprocedure wordt geverifieerd.

Geldproducten

De houding van dit verdienmodel is reactief-actief. De vertegenwoordigers realiseren zich het belang van privacy en hebben zichzelf hieromtrent een gedragscode opgelegd. De actieve houding komt vooral tot uiting in het benadrukken van het klantbelang waaraan niet getornd mag worden. De reactieve houding komt vooral voort uit het conformeren aan wet- en regelgeving bijvoorbeeld rondom marketing. Onderkennen de vertegenwoordigers de potentiële waarde van de gegevens waarover zij beschikken en wordt er soms nagedacht over hoe die te gelde kan worden gemaakt? De eerdere genoemde pogingen van ING hieromtrent¹¹⁰ lijken hier op te duiden.

Onderneming & attitude		Economie & attitude		Verdienmodel & attitude		Attitude onderneming is consistent met
Facebook	Inactief	Nieuw	Inactief-reactief	Online adverteren	Inactief	Verdienmodel
Google	Inactief	Nieuw	Inactief-reactief	Online adverteren	Inactief	Verdienmodel
Qiy Foundation	Proactief	Nieuw	Inactief-reactief	Licenties & abon.	Actief	Verdienmodel
WhatsApp	Reactief-actief	Nieuw	Inactief-reactief	Licenties & abon.	Actief	Economie
KPN	Actief	Telecom	Actief	Licenties & abon.	Actief	Economie & verdienmodel
UPC	Actief	Telecom	Actief	Licenties & abon.	Actief	Economie & verdienmodel
Philips	Reactief	Oud	Reactief-actief	Goederen verk.	Reactief	Verdienmodel
Albert Heijn	Reactief	Oud	Reactief-actief	Goederen verk.	Reactief	Verdienmodel
G4S	Reactief	Oud	Reactief-actief	Contracten	Reactief	Verdienmodel
ING	Reactief-actief	Oud	Reactief-actief	Geldproducten	Reactief-actief	Economie & verdienmodel
Rabobank	Reactief-actief	Oud	Reactief-actief	Geldproducten	Reactief-actief	Economie & verdienmodel

Tabel 6. Attitude vergelijking

Gekeken naar de houding van de individuele ondernemingen, de houding van de onderscheiden economieën en de houding van de verschillende verdienmodellen (tabel 6), valt op dat het verdienmodel meer samenhang

¹¹⁰ Zie hoofdstuk 1

lijkt te hebben met de attitude van een onderneming dan de economie. Uit de tabel blijkt dat de houding van ondernemingen richting privacy - met uitzondering van WhatsApp - het meest overeenkomt met de houding van het bijbehorende verdienmodel. De afwijking bij WhatsApp wordt verklaard door de inconsistenties tussen de pretenties en praktijken bijvoorbeeld met betrekking tot de toegang tot het adresboek en het voorbehoud om persoonsgegevens voor andere doelen te mogen gebruiken. Daarnaast blijkt uit de tabel dat de visies op privacy bij de vertegenwoordigers van de nieuwe economie het meest uiteenloopt. Het onderscheidende kenmerk is daarbij of een onderneming wel of niet afhankelijk is van gratis persoonsgegevens.

5.3 Conclusie

In de voorgaande paragrafen is antwoord gegeven op de vraag welke visies op privacy bij vertegenwoordigers van de oude en nieuwe economie waargenomen kunnen worden (deelvraag 3). Uit de onderzoeksresultaten kunnen de hierna genoemde conclusies worden getrokken.

Conclusie 1:

Privacy heeft, in het algemeen, voor ondernemingen (nog) geen urgentie.

Van de onderzochte ondernemingen is slechts 1 onderneming proactief. Telecom is overwegend actief maar verwevenheid van het thema met de hele organisatie is nog niet aan de orde gegeven de reactieve opstelling bij marketing. Alhoewel de oude economie privacy als een fundamenteel mensenrecht ziet, leidt dit vooralsnog niet tot een (pro)actieve voortrekkersrol maar lijkt conformering aan wet- en regelgeving belangrijker te zijn. Alhoewel privacy nu niet urgent lijkt te zijn, werden er in de interviews wel de volgende aanwijzingen gegeven dat het urgentiebesef toeneemt:

1. Hiaat tussen gepercipieerde privacy bij ondernemingen en individuen; daar waar privacy niet meer bestaat, is het publiek nog in de veronderstelling dit wel te hebben, aldus ING. De inspanningen van ondernemingen dienen daarom gericht te zijn op voorlichting, transparantie en openheid. Kortom, het eerlijke verhaal moet worden verteld.
2. De visie op privacy van Qiy heeft inmiddels de interesse gewekt van andere (oude economie) bedrijven en de overheid. Inmiddels zijn er overlegvormen opgestart teneinde te komen tot een overkoepelend afsprakenstelsel waarin de privacy van individuen wordt gegarandeerd.
3. Naarmate er meer medische apparatuur voor thuisgebruik beschikbaar komt en deze apparatuur slim kan communiceren, zal de urgentie van privacy voor Philips toenemen. Enerzijds betekent dit een oriëntatie op 'privacy by design' in het innovatieproces, anderzijds dient nagedacht te worden over de positionering van privacy rondom het beschikbaar komen van (nieuwe) medische gegevens.

Conclusie 2:

De positionering van privacy in de business modellen van de nieuwe economie vertegenwoordigers, impliceert een keuze uit een pro-privacy of een anti-privacy houding.

De olie van de business modellen van de nieuwe economie bedrijven is data ofwel persoonsgegevens. De mate waarin individuen controle hebben, is hierin onderscheidend. De huidige business modellen van Google en Facebook vereisen de beschikbaarheid van gratis persoonsgegevens; derhalve is hun anti-privacy of 'privacy doet er niet toe' verklaarbaar. WhatsApp pretendeert de privacy belangen te beschermen en is in haar business model niet afhankelijk van persoonsgegevens. Derhalve kiest WhatsApp voor inkomsten uit licenties & abonnementen waarin deze onafhankelijkheid is verankerd. Het bedrijf Qiy handelt ook in persoonsgegevens echter het is niet Qiy maar het individu die bepaalt welke gegevens met welk commercieel bedrijf worden gedeeld. De visie op privacy is zo gezien een onderscheidende factor bij de vertegenwoordigers van de nieuwe economie waarbij een neutrale houding richting privacy niet mogelijk lijkt.

Conclusie 3:

De houding van ondernemingen richting privacy houdt verband met het verdienmodel en de economie die wordt vertegenwoordigd.

De visie op privacy lijkt samen te hangen met de wijze waarop ondernemingen hun inkomsten realiseren. Zo lijkt online adverteren een pro-privacy houding uit te sluiten en omgekeerd is een anti-privacy houding bij het licenties & abonnementen verdienmodel niet aannemelijk. Ten aanzien van goederenverkoop is deze scheidslijn minder duidelijk aanwezig. Bij geldproducten is een pro-privacy houding het meest aannemelijk. In combinatie met conclusie 2, lijkt de houding van ondernemingen richting privacy derhalve voorspelbaar te zijn op basis van de economie die wordt vertegenwoordigd en het gekozen verdienmodel.

6 CONCLUSIE EN DISCUSSIE

6.1 Conclusie

In de voorgaande hoofdstukken is antwoord gegeven op de verschillende deelvragen waarmee tevens deel één van de onderzoeksvraag is beantwoord te weten: “Hoe manifesteren de verschillende visies op privacy zich in de business modellen van de oude en nieuwe economie?”. In dit afsluitende hoofdstuk zal worden gezocht naar het antwoord op deel twee van de onderzoeksvraag namelijk: “Welke verschuivingen in deze visies kunnen worden verwacht in de strijd tussen vertegenwoordigers van beide economieën?”. Hierbij zal zoals aangegeven¹¹¹ gebruik worden gemaakt van de transitie management theorie. Transitie management beoogt dus het realiseren van systemische wijzigingen en paradigma shifts in de inrichting en organisatie van de maatschappij en ondernemingen. Gekeken naar privacy lijkt de bescherming hiervan verankerd te zijn in de huidige dominante regimes. Het idee bij met name vertegenwoordigers van de nieuwe economie dat privacy niet relevant is of zelfs niet bestaat, kan als een niche worden gezien. In hoeverre de regimes rondom privacy gecompromitteerd raken, lijkt afhankelijk te zijn van de hierna genoemde factoren.

De sociale waarde van privacy

In hoofdstuk 2 is ingegaan op de relevantie van privacy; het stelt mensen in staat om zelf te kiezen in welke sociale relaties ze betrokken willen zijn. Privacy heeft dus een belangrijke sociale waarde die hoogstwaarschijnlijk alleen tegen een hoge prijs opgeofferd zal worden. Uit een online-enquête onderzoek onder 150.000 Nederlanders werd bijvoorbeeld duidelijk dat een overgrote meerderheid ontevreden is over de inrichting van de huidige samenleving. Gebleken is dat men aspecten als ‘bestaanskwaliteit’ en ‘solidariteit’ prevaleert boven meer welvaart en economische groei (Eijk, 23-4-2005). Het voorgaande impliceert dat de waarde die mensen aan privacy hechten eerder zal toenemen dan afnemen. Daniel Solove (2002) beschrijft hoe deze toenemende waarde zich de afgelopen eeuwen heeft ontwikkeld. Zo was het in vroeger eeuwen ‘normaal’ dat huizen door meerdere families werden bewoond, dat mensen openlijk hun behoefte deden, dat vrouwen fysiek werden gestraft en dat mensen (deels) naakt rondliepen. Nu worden familie, lichaam en huis als privé aangelegenheden gezien die voor onbevoegden zijn afgesloten. De toenemende aandacht die privacy sinds de opkomst van het informatietijdperk heeft gekregen, bevestigt eveneens de veronderstelling dat de sociale waarde van privacy zal toenemen. Daar waar ondernemingen deze waarde over- dan wel onderwaarden, ontstaan er risico’s op ‘tensions’ hetgeen de basis legt voor een ‘reconstitution’ transitie. Gekeken naar de sociale waarde van privacy, lijkt dit de meest dominante factor te zijn bij de verschuivingen in de visies op privacy. Derhalve kunnen hieromtrent de volgende hypotheses worden geformuleerd:

Hypothese 1:

Naarmate de sociale waarde van privacy meer wordt bedreigd, zullen regimes in toenemende mate kwetsbaarder worden.

Hypothese 2:

Naarmate de sociale waarde van privacy meer wordt beschermd, zullen regimes in toenemende mate worden gesteund.

Hypothese 3:

Des te meer de commerciële belangen van ondernemingen met privacy belangen conflicteren, des te meer tegenstand zullen deze ondernemingen ondervinden.

¹¹¹ Zie hoofdstuk 4

Technologische innovatie

Gekeken naar de toekomst is het aannemelijk dat technologie zich blijvend zal innoveren. Dit zal gemak met zich meebrengen maar ook bedreigingen kunnen niet worden uitgesloten. Meer gemak kan ontstaan door innovaties rondom biometrie en Nanotechnologie waardoor bijvoorbeeld het gebruik van contant geld of pinpassen overbodig is. Bedreigingen kunnen ontstaan als overheden niet meer in staat zijn om terreur, misdaad en fraude op een adequate manier te bestrijden tenzij mensen continue worden geobserveerd. In '1984' van George Orwell is voortdurende observatie noodzakelijk om de dictatuur te handhaven; niet uit te sluiten is dat voortdurende observatie noodzakelijk wordt om de democratie te handhaven? De technologie zou zich (theoretisch) ook zo kunnen ontwikkelen dat privacy belangen feitelijk geen rol meer spelen. Recent werd er door onderzoekers van de TU Delft een experiment uitgevoerd waarbij informatie werd verplaatst zonder dat die informatie door de ruimte reisde¹¹². Met dit zogenaamde 'teleporteren' lijkt de veiligheid gegarandeerd te zijn omdat informatie niet onderschept kan worden. Technologische innovatie kan enerzijds stress uitlokken bijvoorbeeld als regimes beloven de voordelen hiervan te exploiteren maar dat niet kunnen waarmaken. Anderzijds kan het leiden tot 'pressure' omdat het niches in staat stelt onderscheidende waardeproposities te leveren die het regime buitenspel plaatsen ('empowerment'). De volgende hypothesen kunnen rondom technologische innovatie worden geformuleerd:

Hypothese 4:

Naarmate technologische innovaties leiden tot meer gemak, zullen mensen in toenemende mate geneigd zijn om de negatieve privacy consequenties hiervan te accepteren.

Hypothese 5:

Naarmate technologische innovaties zullen leiden tot ontwrichting van de maatschappij, zullen mensen in toenemende mate geneigd zijn om, ter bestrijding van deze dreigingen, de negatieve privacy consequenties hiervan te accepteren.

Maatschappelijke omwentelingen

Evenals dat de visie van de Nederlander in de afgelopen decennia op verschillende (vaak morele) thema's is veranderd, is het voorstelbaar dat de verdere ontwikkeling van de netwerksamenleving zal leiden tot cultuurveranderingen en maatschappelijke omwentelingen. Een omwenteling kan zijn dat het 'normaal' wordt gevonden dat ondernemingen alles van jou weten zolang dit maar in jouw voordeel wordt gebruikt. Een andere omwenteling kan zijn dat de bescherming van privacy topprioriteit krijgt bijvoorbeeld als gevolg van een "expected huge technological collapse, security breach or 'Black Thursday' in the data ecosystem between 2016 and 2020" (Foundation Telecom, 2014). Naarmate ondernemingen niet in staat zijn zich hierop aan te passen, zullen de 'tensions' toenemen eveneens met een 'reconstitution' tot gevolg. Daar waar ondernemingen er wel in slagen om zich aan te passen, is een 'adaptation' transitie waarschijnlijker. Naar aanleiding van het voorgaande kan de hierna genoemde hypothese worden geformuleerd.

Hypothese 6:

De richting waarin de (maatschappelijke) visie op privacy zich ontwikkelt, is afhankelijk van welke privacy beschermende of bedreigende gebeurtenissen (kantelpunten) zullen plaatsvinden.

Kracht van de markt & kapitaal

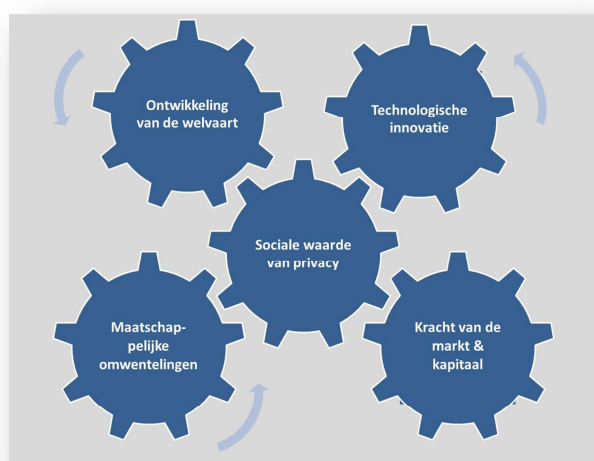
Naarmate regimes in toenemende mate worden bedreigd, zullen zij zich heftiger verzetten teneinde eliminatie te voorkomen. De slagingskans hiervan zal mede bepaald worden door de resterende invloed van het regime en de middelen die het beschikbaar heeft om verloren macht terug te krijgen. Anders gesteld: in hoeverre kan het regime zichzelf 'empoweren' en de transitie in een door haar gewenste richting sturen? In relatie tot privacy lijkt de oude economie zich reeds te oriënteren op een dergelijke 'empowerment' gegeven de lopende

¹¹² <http://www.scientias.nl/primeur-nederlandse-onderzoekers-teleporteren-informatie/101664>

gesprekken met het bedrijf Qiy voor het maken van verregaande afspraken waarin enerzijds de privacy van individuen wordt gegarandeerd en anderzijds ondernemingen kunnen profiteren van de beschikbaarheid van persoonsgegevens. De ambities van Qiy gaan daarbij zelfs zover dat over een 'alternatief internet' wordt gesproken. In dit scenario zal de paradigma shift door 'adaptation' tot stand komen en mogelijk zelfs leiden tot het uitsterven ofwel een 'backlash' van de opkomende niches (Haan & Rotmans, 2011). Het voorgaande leidt tot de hierna genoemde hypothese.

Hypothese 7:

Des te meer controle individuen over hun persoonsgegevens hebben, des te meer zullen zij geneigd zijn om derden gecontroleerd toegang tot deze gegevens te geven.



Figuur 19. Samenhang transitie condities

Ontwikkeling van de welvaart

Dat privacy in toenemende mate belangrijk wordt gevonden, lijkt samen te hangen met de toegenomen welvaart in de afgelopen decennia. Deze welvaart en de verbeterde sociale voorzieningen, heeft geleid tot een meer individualistische samenleving waarin het overgrote deel van de bevolking in staat is om voor zichzelf te zorgen. Anders gesteld: mensen zijn duidelijk minder afhankelijk van hun omgeving en lijken meer geneigd te zijn om 'warme' sociale relaties vooral in familieverband te onderhouden. Naarmate een maatschappij welvarender wordt, is het aannemelijk om conform de theorie van Maslow (1943) te veronderstellen dat de behoefte aan erkenning en zelfontplooiing toeneemt. Privacy creëert daarbij de condities om deze behoeftes te realiseren. Omgekeerd zal een afnemende welvaart betekenen dat mensen meer gericht zullen zijn op het realiseren van de primaire levensbehoeften dan op het beschermen van de eigen privacy. Gekeken naar de toekomst lijkt de kans op minder welvaart reëel onder meer vanwege vergrijzing, uitputting van natuurlijke bronnen en toenemende sociale tegenstellingen. In hoeverre de aanhoudende aantastingen van de koopkracht (Jakobs, 2013) hiervoor indicatief zijn, lijkt zo bezien een terechte vraag. Op basis van het voorgaande kunnen de hierna genoemde hypothesen worden geformuleerd.

Hypothese 8:

Naarmate de welvaart toeneemt, zal de behoefte aan meer privacy bij individuen toenemen.

Hypothese 9:

Naarmate de welvaart afneemt, zal de relevantie van privacy voor individuen afnemen.

Ten aanzien van de voornoemde factoren zullen veranderingen hoogstwaarschijnlijk nooit geïsoleerd plaatsvinden (figuur 19). Zo zal de keuze om een privacy bedreigende technologie te ontwikkelen, worden beïnvloed door de sociale waarde van privacy. Ook is het waarschijnlijk dat de sociale waarde van privacy zal afnemen als door terreur en misdaad de democratie onder druk wordt gezet. Een ander voorbeeld is als een regime strategische keuzes rondom privacy maakt en diensgevolge de aanjager wordt van bepaalde technologische ontwikkelingen. Zo bezien lijkt privacy een 'wicked problem' te zijn waarvan "de verwevenheid met andere maatschappelijke problemen en de worteling in onze maatschappelijke structuren en instituties maakt dat het niet in afzondering kan worden geanalyseerd en opgelost" (Rotmans, 2005). Dientengevolge zal de richting waarin de dominante visie op privacy zich zal bewegen, afhankelijk zijn van de ontwikkelingen die zich in onderlinge samenhang rondom de genoemde factoren zullen afspelen.

6.2 Discussie

6.2.1 Interpretatie van de resultaten

Ten aanzien van het concept privacy is het verrassend dat hiervoor geen universele definitie gegeven kan worden. Privacy blijkt daarentegen breed geïnterpreteerd te kunnen worden waarbij het betrekking kan hebben op uiteenlopende persoonsgebonden zaken van materiële en immateriële aard. Opmerkelijk is ook dat privacy een belangrijke voorwaarde blijkt te zijn voor het welbevinden van individuen maar ook voor een florerende democratie. Het schenden daarvan impliceert dat mensen zichzelf niet kunnen zijn en zich voortdurend in hun negatieve vrijheid beperkt voelen.

Ten aanzien van de onderzoeksresultaten bevestigen deze deels hetgeen vooraf werd verwacht. Dat Facebook en Google geen voorvechters van privacy zijn, is algemeen bekend. Dat banken en Telecom vertrouwelijk met persoonsgegevens omgaan, zal eveneens geen verrassing zijn. Verrassend is wel dat de nieuwe economie zowel voor- als tegenstanders van privacy vertegenwoordigt. Een neutrale houding richting privacy ligt daar niet voor de hand. Ten aanzien van de oude economie was vooraf de verwachting dat privacy een meer prominente rol zou spelen dan nu is aangetroffen. Typerend daarvoor is dat één onderneming in haar jaarverslag of 'business ethics' het woord privacy zelfs niet noemt. Opvallend is ook dat privacy in het algemeen nog geen urgentie heeft en ondernemingen terughoudend zijn in het maken van fundamentele keuzes ten aanzien van de positionering van privacy in hun business modellen.

6.2.2 Kanttekeningen bij het onderzoek

Het aantal ondernemingen dat in dit onderzoek is onderzocht is beperkt ($n=11$). Binnen deze populatie is de verbijzondering naar oude economie ($n=5$), nieuwe economie ($n=4$) en Telecom ($n=2$) dientengevolge ook beperkt.

Voor het duiden van de houding richting privacy is gebruik gemaakt van interviews en openbare bronnen. Bij een aantal (sub)indicatoren is het niet mogelijk gebleken om de houding richting privacy op basis van deze bronnen vast te stellen. Naarmate het aantal 'niet bekend gemaakt' indicatoren oploopt, neemt logischerwijs de kracht van de argumenten en conclusies af.

Bij een drietal ondernemingen zijn interviews afgenomen. Een bijkomstigheid hiervan is dat de visie van deze ondernemingen op vrijwel alle indicatoren vastgesteld kon worden. In het onderlinge vergelijk creëert dit een onevenwichtigheid die op geaggregeerd niveau in beperkte mate wordt gecompenseerd doordat deze drie ondernemingen twee van de drie groepen vertegenwoordigen die in het onderzoek met elkaar worden vergeleken.

De houding van de niet-geïnterviewde ondernemingen is door de onderzoeker gedomineerd door het interpreteren van het empirische materiaal. Bij de drie overige bedrijven is de duiding tijdens het interview vastgesteld waarbij de geïnterviewden geneigd waren om 'sociaal wenselijke' antwoorden te geven.

Tijdens de interviews bleek dat de gebruikte taxonomie geschikt is voor het duiden van de houding van ondernemingen richting privacy. Het betreft echter een nieuwe, niet-gevalideerde taxonomie die door één onderzoeker is opgesteld.

Dit onderzoek is door de onderzoeker op persoonlijke titel uitgevoerd en kent derhalve geen opdrachtgever. Alhoewel het gekozen onderwerp overduidelijk maatschappelijke relevantie heeft, is de bedrijfskundige context gaandeweg tot stand gekomen.

6.2.3 Aanbevelingen voor vervolgonderzoek

Privacy is een vloeibaar begrip waarvan de interpretatie context, tijdperk en persoonsgebonden is. Een eerste aanbeveling betreft nader onderzoek naar de determinanten waardoor datgene wat zich rondom persoonsgegevens voordoet, door individuen als een privacyschending wordt gezien. Waarom kan Facebook bijvoorbeeld ongestoord persoonsgegevens exploiteren maar ING niet?

Privacy lijkt vooralsnog geen 'sense of urgency' te hebben met name voor de oude economie. Dit is verwonderlijk gezien de vele aandacht in de media en de dreigingen van de nieuwe economie. Zo oriënteren Facebook en Google zich op het aanbieden van financiële diensten en beschikken zij inmiddels in verschillende landen over een bankvergunning. De tweede aanbeveling betreft daarom onderzoek naar de redenen voor de huidige overwegend reactieve opstelling van de oude economie richting privacy.

Een nieuwe bedreiging voor privacy vormen de zogenaamde 'wearables'; het gebruik hiervan kan anderen een gevoel geven dat ze worden bespied. Het gebruik van deze technologie lijkt gevolgen te hebben voor de gangbare omgangsvormen. Nader onderzoek is nodig om inzicht te krijgen in de sociaal-maatschappelijke consequenties als het gebruik van deze 'wearables' verder toeneemt.

In dit onderzoek zijn een beperkt aantal bedrijven onderzocht. De vierde aanbeveling betreft het toetsen van de taxonomie bij een grotere populatie met extra dimensies voor het maken van onderlinge vergelijkingen. Gedacht kan worden aan: (1) omvang van de onderneming, denken SME bedrijven bijvoorbeeld anders over privacy dan multinationals?; (2) wijze waarop onderneming is gefinancierd, denken beursgenoteerde bedrijven anders over privacy dan privaat gefinancierde ondernemingen?; (3) domicilie en cultuur, in hoeverre wordt privacy beïnvloed door het vestigingsland en de cultuur?

Ten aanzien van de verwachte verschuivingen in de visies op privacy, zijn in de vorige paragraaf een aantal hypotheses geformuleerd. De laatste aanbeveling betreft nader onderzoek rondom deze hypotheses vanuit verschillende paradigma's zoals de psychologie, economie en sociologie.

7 BIJLAGEN

7.1 Bibliografie

- Ahold. (2013). *Annual report*.
- Allmer, T. (2011). A critical contribution to theoretical foundations of privacy studies. *Journal of Information, Communication & Ethics in Society*, 83-101.
- Bartels, G. (9-3-2014). Minderhedenproblematiek is voorbij, privacy is nu een issue. *Trouw*.
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35, 1017-1041.
- Bird, S. J. (2013). Security and privacy: Why privacy matters. *Science and Engineering Ethics*.
- Bloem, J., Doorn, M. v., Duivestijn, S., Manen, T. v., & Ommeren, E. v. (2013). *Privacy, technologie en de wet: Big Data voor iedereen door goed design*. Sogeti VerkenningInstituut Nieuwe Technologie VINT.
- Bruin, B. d. (2010). The liberal value of privacy. *Law and Philosophy*, 505-534.
- Castells, M. (2000). Materials for an exploratory theory of the network society. *British Journal of Sociology*.
- CBP. (2012). *Jaarverslag*. Den Haag: College bescherming persoonsgegevens.
- CBP. (2014). *Het CBP in 2013*. Den Haag: College bescherming persoonsgegevens.
- Coget, J.-F., Yamauchie, Y., & Suman, M. (2002). The internet, social networks and loneliness. *IT & Society*.
- Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Info Systems*, 23: 401-417.
- Devezas, T. C., Linstone, H. A., & Santos, H. J. (2005). The growth dynamics of the internet and the long wave theory. *Technological Forecasting & Social Change*, 72: 913-935.
- Eijk, V. (23-4-2005). Een baan, een huis, kinderen—maar geen controle: De grootste peiling ooit. *NRC Handelsblad*.
- Facebook. (2013). *Annual report*.
- Financieel dagblad. (10-3-2014). ING geeft adverteerder inzicht in klantgedrag. *Financieel dagblad*.
- Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven Types of Privacy. In S. Gutwirth, R. Leenes, P. d. Hert, & Y. Pouillet, *European Data Protection: Coming of Age* (pp. 3-32). Dordrecht: Springer.
- Foundation Telecom. (2014). *The Futures of Privacy*.
- Franklin, A. S. (2009). On loneliness. *Geografiska Annaler: Series B, Human Geography*.
- Friedewald, M., & Pohoryles, R. J. (2013). Technology and privacy. *Innovation: The European Journal of Social Science Research*.
- Fuchs, C. (2011). An alternative view of privacy on Facebook. *Open Access Information*, 140-165.
- Fuchs, C. (2012). The political economy of privacy on Facebook. *Television New Media*, 13(2), 139-159.
- Geels, F. (2004). From sectoral systems of innovation to socio-technical systems: insights about dynamics and change from sociology and institutional theory. *Research Policy*.
- Google Inc. (2012). *Annual report*.
- Goold, B. J. (2009). Surveillance and the political value of privacy. *Amsterdam Law Forum*.
- Groot, A. d. (1964). *Methodologie*. 's Gravenhage: Mouton.
- Haan, H. d., & Rotmans, J. (2011). Patterns in transitions: Understanding complex chains of change. *Technological Forecasting & Social Change*.
- Harper, J. (2004). Understanding privacy – and the real threats to it. *Cato Institute Policy Analysis*.
- Hirshleifer, J. (1980). Privacy: It's origin, function, and future. *The Journal of Legal Studies*, 9(4), 649-664.
- Huxley, A. (1932). *Brave New World*.
- Jakobs, B. (2013). Macro-economische politiek voor een uitweg uit de crisis (deel II). *ESB Groei & Conjunctuur*.
- Kemp, R., & Moore, A. D. (2007). Privacy. *Library Hi Tech*, 25, 58-78.
- KPN. (2013). *Integrated Annual Report*.
- Kuner, C., Cate, F. H., Miljard, C., & Svantesson, D. J. (2011). Privacy—an elusive concept. *International Data Privacy Law*, 1.

- Lee, D.-J., & Ahn, J.-H. (2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection. *MIS Quarterly*, 423-444.
- Lieshout, M. v., Friedewald, M., Wright, D., & Gutwirth, S. (2013). Reconciling privacy and security. *Innovation: The European Journal of Social Science Research*, 119-132.
- Loorbach, D., & Rotmans, J. (2010). The practice of transition management: Examples and lessons from four distinct cases. *Futures*.
- Loorbach, D., & Wijsman, K. (2013). Business transition management: exploring a new role for business in sustainability transitions. *Journal of Cleaner Production*.
- MacDermott, S., & Smith, J. R. (2013). *The future of privacy: A consumer-oriented approach to managing personal data online*. Wiley.
- Maslow, A. H. (1943). A Theory of Human Motivation. *Psychological Review*, 370-396.
- Mooradian, N. (2009). The importance of privacy revisited. *Ethics Information Technology*.
- Muller, E., Kummeling, H., & Bron, R. (2007). *Veiligheid en privacy*. De Haag: Boom Juridische uitgevers.
- Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, 17: 559-596.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*.
- NRC Handelsblad. (15-2-2014). Privacy sluit medische data niet af van studie.
- Nye, D. (2002). The 'privacy in employment' critique: a consideration of some of the arguments for 'ethical' HRM professional practice. *Business Ethics: A European Review*.
- Oltshoorn, P. (2013). *Privacy bestaat niet*. Amsterdam: Adfo Groep.
- Orwell, G. (1949). 1984. Amsterdam: N.V. De Arbeiderspers.
- Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 977-988.
- Posner, R. A. (1981). The economics of privacy. *The American Economic Review*, 71(2), 405-409.
- PRESCIENT. (2011). *Legal, social, economic and ethical conceptualisations of privacy and data protection*.
- Prins, C. (2006). Property and Privacy: European Perspectives and the Commodification of our Identity. In L. Guibault, & P. Hugenholtz, *The Future of the Public Domain* (pp. 223-257). Kluwer Law International.
- Rabobank Groep. (2013). *Jaarverslag*.
- Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 323-333.
- Reiman, J. H. (1976). Privacy, intimacy and personhood. *Philosophy & Public Affairs*.
- Rotmans, J. (2005). *Maatschappelijke innovatie: tussen droom en werkelijkheid staat complexiteit*. Rotterdam: DRIFT.
- Rubinstein, I. S., & Good, N. (2012). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal*.
- Shafer, S. M., Smith, H. J., & Linder, J. C. (2005). The power of business models. *Business Horizons*.
- Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 1087-1155.
- Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 477-564.
- Solove, D. J. (2008). "I've got nothing to hide" and other misunderstandings of privacy.
- Swanborn, P. G. (2004). Kwalitatief onderzoek en exploratie. *KWALON 26*.
- Swire, P. (2012). Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment. *North Carolina Law Review*.
- Teece, D. J. (2010). Business Models, Business Strategy and Innovation. *Long Range Planning*.
- Tilburg, R. v., Tulder, R. v., Francken, M., & Rosa, A. d. (2012). *Duurzaam ondernemen waarmaken*. Van Gorcum.
- Tulder, R. v. (2010). *Corporate Responsibilities in Turbulent Times*. Peking: China Economics Publishing House.
- Tulder, R. v. (2011). *Issues and Trade-offs: Exercises in Critical Thinking, Leadership and Decision-Making in a Bargaining Society*.
- Tulder, R. v., & Zwart, A. v. (2006). *International business-society management. Linking corporate responsibility and globalization*. Routledge, Oxon.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4, 193-220.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

7.2 Privacy taxonomie van Solove (2006)

(SUB)ACTIVITEIT	BETEKENIS	POTENTIËLE EFFECTEN
Informatie verzameling:		
Surveillance	Het observeren, af luisteren of opnemen van iemands activiteiten. Surveillance kan daarbij openlijk of heimelijk plaatsvinden.	- Verhoogd risico op toekomstige benadeling - Onbalans in sociale of institutionele machtsverhoudingen - Onderdrukking van het ontplooiën van waardevolle activiteiten - Ontwikkelen van sociaal gewenst gedrag - Belemmeren van vrijheid, creativiteit en ontwikkeling
Ondervraging	Verschillende vormen van (dwingende) ondervraging of peilen naar informatie.	- Onbalans in sociale of institutionele machtsverhoudingen - Manipulatie van verkregen informatie - Orkestreren van gewenste uitkomsten
Informatie verwerking:		
Aggregatie	Het verzamelen van gefragmenteerde gegevens en het combineren daarvan waardoor de informativiteit wordt vergroot.	- Mogelijkheden voor gepersonaliseerde advertenties - Onthulling van verborgen feiten - Ongewenste machtsverhoudingen
Identificatie	Het koppelen van informatie aan een individu.	- Voorkomen van misinformatie - Voorkomen van illegale handelingen - Verhoogd risico op benadeling vanwege openbaarheid van de identiteitskenmerken - Verliezen van unanimiteit
Onveiligheid	Het onveilig behandelen en beschermen van informatie.	- Identiteitsfraude - Verhoogd risico op toekomstige benadeling
Tweedehands gebruik	Het zonder toestemming gebruiken van informatie voor andere doeleinden dan waarvoor het is verkregen.	- Schending van de eigen waardigheid - Verhoogd risico op toekomstige benadeling - Verlies van controle over eigen informatie - Gevoel van machteloosheid en kwetsbaarheid bij het individu
Uitsluiting	Het niet informeren van individuen over de gegevens die bedrijven en instanties van hen bewaren en het onthouden van mogelijkheden om daarop correcties te eisen.	- Gevoel van machteloosheid en kwetsbaarheid bij het individu - Verminderd verantwoordelijkheidsbesef bij de data houders
Informatie verspreiding:		
Schending van vertrouwelijkheid	Het onthullen van informatie wat in vertrouwen is verkregen.	- Een gevoel van verraden te zijn - Verlies van vertrouwen in bestaande en nieuwe relaties - Verhoogd risico op toekomstige benadeling - Schending van de eigen waardigheid
Ontsluiting	Het ontsluiten persoonlijke waarheden aan anderen.	- Aantasting van reputatie - Terughoudendheid om activiteiten te ontplooiën ter bevordering van de eigen ontwikkeling

(SUB)ACTIVITEIT	BETEKENIS	POTENTIËLE EFFECTEN
		- Onderdrukking van het contacten leggen met anderen - Belemmeren van vrijheid - Bedreiging van veiligheid - Verhoogd risico op toekomstige benadeling
Blootstelling	Het blootstellen van fysieke en emotionele eigenschappen die als oorspronkelijk worden beschouwd en waarvan schending als vernederend wordt ervaren.	- Verlies van waardigheid - Belemmering om deel te nemen aan de maatschappij
Toegenomen benaderbaarheid	Het eenvoudiger beschikbaar stellen en benaderen van persoonsgegevens met name op het Internet.	- Verhoogd risico op ontsluiting van persoonsgegevens - Opgeven van privacy
Afpersing	Het manipuleren van een individu onder dreiging van het onthullen van diens geheimen.	- Verlies van controle over eigen handelen
Inbezitneming	Het zonder toestemming gebruiken van iemands identiteit of persoonlijkheid voor doelen van anderen.	- Verlies van waardigheid - Inmenging in persoonlijke vrijheid - Belemmering van de eigen ontwikkeling
Verdraaiing	Het negatief manipuleren van iemands meningsvorming over een individu.	- Verhoogd risico op stigma, vernedering en reputatieschade - Verslechtering van welzijn en welbevinden
Invasie:		
Indringing	Het ongewild indringen in iemands leven waarbij er een interruptie plaatsvindt in de activiteiten van het individu.	- Gevoel van ongemak en discomfort - Verstoring van activiteiten
Inmenging bij besluitvorming	Het ongewild inmengen in het besluitvormingsproces van individuen met betrekking tot persoonlijke zaken.	- Verlies van zelfbeschikking - Verhoogd risico op reputatieschade

7.3 Taken van het CBP

De taken van het CBP zijn:

1. Toezicht; dit betreft het toezien op de naleving en toepassing van wetten die het gebruik van persoonsgegevens regelen zoals:
 - a. Wet bescherming persoonsgegevens (Wbp)
 - b. Wet politiegegevens (Wpg)
 - c. Wet gemeentelijke basisadministratie (Wet GBA)
 - d. Wet justitiële en strafvorderlijke gegevens (Wjsg)
2. Advisering; dit betreft het adviseren van de regering en/of het parlement met betrekking tot voorgenomen wet- en regelgeving aangaande het gebruik van persoonsgegevens.
3. Voorlichting, informatieverstrekking en verantwoording; dit betreft het geven van helderheid aan belanghebbenden over de wettelijke normen ten aanzien van privacy. Daarnaast betreft het informatieverstrekking via de websites www.cbpweb.nl en www.mijnprivacy.nl en de jaarverslaglegging.
4. Internationale taken; dit betreft de vertegenwoordiging in verschillende internationale organen zoals de Artikel 29-werkgroep.

De Wet bescherming persoonsgegevens (Wbp) regelt de privacy rechten en verplichtingen van burgers, bedrijven en de overheid. Dit betreft de volgende rechten:

1. Recht op informatie; dit verplicht verantwoordelijken om betrokkenen vooraf te informeren over het gebruik van de verkregen persoonsgegevens.
2. Recht op inzage; individuen hebben het recht om organisaties te vragen naar de gegevens die de organisatie over hen heeft. De organisatie heeft daarbij de verplichting om dit verzoek, met inachtneming van de wettelijke regels, te honoreren.
3. Recht op correctie en verwijdering; dit betreft het recht om de eigen gegevens of die van eigen kinderen te verbeteren, aan te vullen, te verwijderen of af te schermen.
4. Recht van verzet; dit betreft onder andere de afscherming tegen ongewenste benaderingen zoals 'direct marketing' maar ook reclames via de brievenbus.

7.4 Privacy taxonomie

Indicator	Subindicator	Inactief	Reactief	Actief	Proactief
Grondhouding	Visie Algemene visie op privacy	Wij willen mensen verbinden en hen stimuleren om persoonlijke informatie en belevingen met anderen te delen.	In onze overwegingen speelt privacy een rol voornamelijk voor zover er hieromtrent wet- en regelgeving geldt.	Wij vinden dat iedereen een recht op privacy heeft waarin de bescherming van persoonsgegevens is verankerd.	Wij zijn verantwoordelijkheid voor de privacy van belanghebbenden en baseren onze handelwijze op wederzijds vertrouwen.
	Belang Belang van privacy	De privacy belangen van individuen zijn voor ons ondergeschikt aan hogere doelen.	Wij erkennen het belang van privacy en stemmen onze handelwijze af op regelgeving en signalen van belanghebbenden.	Wij vinden privacy belangrijk omdat het bijdraagt aan de ontwikkeling van individuen. De belangen van een individu staan voor ons centraal.	Wij vinden privacy belangrijk omdat het de condities schept waaronder de maatschappij als geheel naar behoren kan functioneren.
	Zeggenschap Visie op zeggenschap over persoonsgegevens	Wij vinden dat persoonsgegevens vrijelijk voor commerciële doeleinden gebruikt mogen worden.	Wij vinden dat persoonsgegevens zonder toestemming gebruikt mogen worden mits wordt voldaan aan wettelijke regels.	Wij vinden dat individuen medezeggenschap hebben over de wijze waarop persoonsgegevens worden verkregen, verwerkt en verspreid.	De zeggenschap over de eigen persoonsgegevens ligt volledig bij individuen.
	Markt voor persoonsgegevens Visie op de markt voor persoonsgegevens	Een markt waarin persoonsgegevens vrijelijk kunnen worden verhandeld vinden wij belangrijk.	Het vrijelijk verhandelen van persoonsgegevens is toegestaan voor zover wordt voldaan aan wettelijke regels.	Het vrijelijk verhandelen van identificeerbare persoonsgegevens voor commerciële doeleinden wijzen wij af. Mits geanonimiseerd, kunnen persoonsgegevens voor andere doelen worden verhandeld.	Een markt voor persoonsgegevens vinden wij voorstelbaar mits gegevens worden geanonimiseerd, tegen een faire vergoeding worden verhandeld en aan alle belangen van betrokkenen tegemoet wordt gekomen.
	Markt voor privacy Visie op de markt voor privacy	Wij zien geen toegevoegde waarde voor een markt die zich richt op het beschermen van privacy.	Een markt voor privacy vinden wij nuttig voor zover dit ons helpt om reputatieschade en wetsovertredingen te voorkomen.	Wij vinden het bestaan van een markt voor privacy enhancing producten en diensten belangrijk.	Samen met belanghebbenden zoeken wij actief naar mogelijkheden om de markt voor privacy enhancing producten en diensten te stimuleren.
	Mensenrecht Visie op privacy als mensenrecht	Het recht op privacy is een achterhaalde gedachte.	In voorkomende gevallen kan een recht op privacy nuttig zijn.	Het recht op privacy is een basisrecht.	Privacy is naast vrijheid, democratie en gelijke behandeling een fundamentele waarde waarop een maatschappij wordt gebouwd.
Compliance	Wettelijke regels Toepassing van wettelijke regels	Wij zijn alert op privacywetgeving die onze doelen ondermijnt en zullen hier actief tegen ageren.	Rondom privacy houden wij ons aan de geldende wet- en regelgeving.	Wet- en regelgeving wordt door ons ruim geïnterpreteerd. Wij zijn bereid om rondom privacy verder te gaan dan de wetgever van ons eist.	
	Privacy policy Gebruik van een privacy policy	Wij vinden het niet relevant om te voorzien in een privacy policy waarin onze houding richting privacy is uitgewerkt.	Bij het formuleren van onze privacy policy laten wij ons leiden door wet- en regelgeving.	Wij vinden het belangrijk dat ons privacy policy transparant en begrijpelijk is. In onze formuleringen laten wij ons leiden door de belangen van de betrokkenen.	Wij streven naar gestandaardiseerde privacy policy formuleringen. Wij nemen de leiding om die samen met anderen voor onze branche te ontwikkelen.
	Cookies Gebruik van internet cookies	Rondom het toepassen van cookies zijn privacy belangen voor ons niet relevant.	Rondom het gebruik van cookies voor commerciële doeleinden houden wij rekening met privacy belangen voor zover daarvoor wettelijke verplichtingen gelden.	Wij realiseren ons dat cookies privacy bedreigend kunnen overkomen. Alvorens cookies voor commerciële doelen te gebruiken, vragen wij eerst om toestemming.	Wij gebruiken geen internet cookies.
	Keurmerk en/of gedragscode Gebruik van een privacy keurmerk	Wij hanteren geen privacy keurmerk en/of gedragscode. Een dergelijk keurmerk biedt ons inziens geen toegevoegde waarde.	Een privacy keurmerk en/of gedragscode kan in voorkomende gevallen nuttig zijn.	Met een privacy keurmerk en/of gedragscode geven wij uiting aan onze overtuiging dat privacy belangrijk is.	Een privacy keurmerk en/of gedragscode vinden wij belangrijk. Wij zetten ons in om samen met stakeholders dit keurmerk verder te ontwikkelen en betekenis te geven.
	Doelbinding Gebruik van verkregen persoonlijke gegevens	Wij gebruiken persoonsgegevens ook voor andere doelen dan waarvoor deze zijn verkregen.	Rondom doelbinding hanteren wij een enge interpretatie van de regels en laten eigen belangen daarbij prevaleren.	Wij gebruiken persoonsgegevens niet voor andere, niet-gerelateerde doelen dan waarvoor deze zijn verkregen.	
	Belangenorganisaties Participatie in privacy belangenorganisaties	Wij zien geen toegevoegde waarde in het bestaan van privacy belangenorganisaties.	In voorkomende gevallen kunnen privacy belangenorganisaties nuttig zijn. Het opvolgen van aanbevelingen zullen wij per geval beoordelen.	Wij participeren in privacy belangenorganisaties of andere gremia waarin privacy belangen aan de orde komen.	
Communicatie & informatiedeling	Zichtbaarheid Zichtbaarheid en transparantie richting belanghebbenden	Het actief informeren van belanghebbenden inzake het gebruik van persoonsgegevens heeft voor ons geen prioriteit.	Wij informeren belanghebbenden over het gebruik van hun persoonsgegevens volgens de daarvoor geldende wettelijke eisen.	Wij voelen ons verplicht om belanghebbenden te informeren over de wijze waarop persoonsgegevens worden gebruikt. Wij komen onze beloften na.	Zichtbaarheid en transparantie inzake het gebruik van persoonsgegevens is de basis voor wederzijds vertrouwen. Wij nemen verantwoordelijkheid om hierin alle stakeholders maximaal te betrekken.

Indicator	Subindicator	Inactief	Reactief	Actief	Proactief
	Informatiedeling Het delen van informatie met derde partijen	In onze overwegingen om informatie met derden te delen, is privacy van ondergeschikt belang.	In onze overwegingen om informatie met derden te delen, houden wij ons aan de geldende wet- en regelgeving en reageren wij op negatieve signalen.	Bij het delen van informatie met derden waarborgen wij de privacy belangen van individuen.	Wij delen geen informatie met derden.
	Zwarte lijsten Gebruik en verspreiding van 'zwarte lijsten' met dubieuze debiteuren en wanbetalers	Bij het gebruik en de verspreiding van zwarte lijsten houden wij geen rekening met privacy belangen.	Voor zover dit wettelijk verplicht is, houden wij rekening met de privacy belangen van personen op zwarte lijsten.	Zwarte lijsten worden door ons alleen intern gebruikt. Wij werken niet mee aan het openbaar maken van wanbetalers.	Wij houden rekening met de privacy belangen van wanbetalers.
	Openbaarheid Openbaarheid van salarissen en/of aandelenposities van medewerkers en/of bestuurders	Wij houden geen rekening met de privacy belangen van bestuurders en medewerkers bij het publiceren van informatie over beloningen en andere financiële informatie.	De publicatie van financiële gegevens waaronder beloningen, doen wij volgens de regels.	Wij realiseren ons dat er verschillende belangen en verplichtingen gelden rondom de publicatie van financiële gegevens. In deze afweging zijn privacy belangen voor ons belangrijk.	Negatieve consequenties voor de privacy belangen accepteren wij niet op voorhand. Samen met belanghebbenden zoeken wij naar mogelijkheden voor betere privacy bescherming.
Marketing	Marketing strategie Visie op te hanteren marketing strategie	Wij vinden dat marketing strategieën zoals direct marketing, personalized marketing actief gebruikt mogen worden. Eventuele privacy belangen van individuen vinden wij niet relevant.	Het gebruik van direct en personalized marketing vinden wij geschikte marketing strategieën. Wet- en regelgeving hieromtrent trachten wij na te komen. Wij reageren op negatieve signalen.	Alvorens de persoonsgegevens van individuen voor marketing doeleinden te gebruiken, vragen wij hiervoor eerst hun toestemming (permission based marketing).	Wij vinden dat individuen zelf de controle moeten hebben over welke persoonsgegevens wanneer en aan wie worden ontsloten (customer managed relations).
	Customer intelligence Visie op het toepassen van customer intelligence	Wij willen zoveel mogelijk van onze klanten weten. Het gebruik van klantgegevens voor het verkrijgen van nieuwe inzichten rondom hun gewoontes, voorkeuren en andere leefpatronen, moedigen wij aan.	Wij gebruiken persoonsgegevens voor het ontwikkelen van inzichten in voorkeuren en leefgewoontes. Wij respecteren wet- en regelgeving en reageren op negatieve reacties.	Bij het toepassen van customer intelligence verzekeren wij ons dat de privacy belangen van klanten niet worden geschaad. Wij gebruiken alleen geanonimiseerde gegevens dan wel gegevens waarvoor de klant ons toestemming heeft gegeven.	
	Kwaliteit & dienstverlening Visie op gebruik persoonsgegevens t.b.v. kwaliteit en dienstverlening	Rondom het verzamelen van klant- en/of verbruiksgegevens ten behoeve van het verbeteren van onze kwaliteit en het verbeteren en verbreden van onze dienstverlening, spelen ons inziens geen privacy belangen.	Bij het verzamelen van klant- en/of verbruiksgegevens ten behoeve van het verbeteren en verbreden van onze kwaliteit en dienstverlening, houden wij ons aan wet- en regelgeving.	Wij realiseren ons dat klant- en/of verbruiksgegevens de privacy kan raken. Wij verzamelen alleen geanonimiseerde gegevens dan wel gegevens waarvoor de klant ons toestemming heeft gegeven.	
	Economische voordelen Visie op economische voordelen in ruil voor persoonsgegevens	Het stimuleren van individuen om persoonsgegevens beschikbaar te stellen in ruil voor bepaalde voordelen, wordt door ons aangemoedigd.	Bij het aanmoedigen van individuen om in ruil voor economische voordelen hun persoonsgegevens beschikbaar te stellen, kijken wij uit geen wetten te overtreden of risico's op imago schade op te lopen.	Wij zijn terughoudend in het aanbieden van economische voordelen in ruil voor persoonsgegevens. In onze overwegingen om hier gebruik van te maken, is privacy bescherming een noodzakelijke voorwaarde.	
HRM	Cameratoezicht Toepassing van cameratoezicht	Wij zien geen problemen in het zonder hun medeweten plaatsen van individuen onder cameratoezicht.	Rondom het gebruik van cameratoezicht houden wij ons aan wet- en regelgeving. Eventuele aanvullende bepalingen leggen wij in gedragscodes vast.	Cameratoezicht schaad de privacy belangen en zien wij als indringing in de persoonlijke levenssfeer.	Cameratoezicht is een uiting van gemist vertrouwen. Wij betrekken stakeholders in onze pogingen om dit vertrouwen te herstellen.
	Screening Screening van sollicitanten	In onze overwegingen om eventueel screening toe te passen zouden wij sollicitanten hieromtrent niet informeren.	In onze overwegingen om eventueel screening toe te passen zullen wij sollicitanten hieromtrent vooraf informeren.	In onze overwegingen om eventueel screening toe te passen zullen wij sollicitanten hieromtrent vooraf toestemming vragen.	
	Verzuim Controle bij verzuim vanwege ziekte	Rondom verzuim vragen wij nadrukkelijk naar de aanleiding, aard en duur van verwachte afwezigheid. Wij vinden het van belang om inzicht te hebben in de medische details.	Rondom verzuim vragen wij naar voor ons relevante informatie. Wij reageren op signalen van derden omtrent onrechtmatige handelingen.	Wij realiseren ons dat informatie rondom verzuim de privacy kan raken. In de communicatie met betrokkenen respecteren wij hun integriteit en nemen verantwoordelijkheid om geen grenzen te overschrijden.	Onze procedure rondom verzuim is samen met alle stakeholders opgesteld. De bescherming van de privacy is hierin verankerd.
	Levenssfeer Inzicht in persoons- en persoonlijke levenssfeer gegevens	Wij vinden het belangrijk om over zoveel mogelijk informatie van (kandidaat) medewerkers te beschikken uiteenlopend van leefgewoonten en medische en religieuze gegevens.	Wij verzamelen alle voor het dienstverband noodzakelijke persoonsgegevens. Wij zullen voldoen aan wettelijke verplichtingen rondom het verzamelen, verwerken en ontsluiten van persoonsgegevens.	Wij zijn ons bewust dat alle gegevens van (kandidaat) medewerkers de privacy kunnen raken. Wij verzamelen alleen gegevens die noodzakelijk zijn voor het dienstverband en daaruit voortvloeiende verplichtingen.	In overleg met stakeholders hebben wij afspraken gemaakt welke gegevens wij van (kandidaat) medewerkers verzamelen en voor welke doelen. In deze afspraken is vastgelegd welke gegevens verplicht en welke vrijblijvend kunnen worden gedeeld.
	Gedragscode Gebruik van gedragscodes	Wij zien geen meerwaarde in gedragscodes rondom HRM waarin de privacy belangen van (kandidaat) medewerkers wordt beschermd.	In onze overwegingen om een gedragscode te onderschrijven, laten wij ons leiden door mogelijke consequenties op onze reputatie alsmede eventuele gevolgen voor de efficiëntie van ons HRM beleid.	Met het onderschrijven van een gedragscode geven wij uiting aan onze overtuiging dat privacy belangrijk is.	Een gedragscode rondom HRM vinden wij belangrijk. Wij zetten ons in om samen met stakeholders dit keurmerk verder te ontwikkelen en betekenis te geven.

Indicator	Subindicator	Inactief	Reactief	Actief	Proactief
	Personeelsbeleid Verankering van privacy in het personeelsbeleid	De privacy belangen van (kandidaat) medewerkers heeft voor ons geen prioriteit in het personeelsbeleid. Wij hebben geen functionaris die is belast met privacy.	Ten aanzien van privacy voldoen wij in ons personeelsbeleid aan geldende wetgeving. Gemaakte afspraken met belangenorganisaties komen wij na.	De verankering van privacy in ons personeelsbeleid vinden wij belangrijk. Wij geven hiermee uiting aan onze verantwoordelijkheid om de privacy belangen van (kandidaat) werknemers te beschermen.	Bij het verankeren van privacy in ons personeelsbeleid betrekken wij de stakeholders. Op basis van een gedeelde verantwoordelijkheid zijn wij in staat om hieromtrent duurzame vernieuwingen te realiseren.
Innovatie & technologie	Technologie Visie op technologie	Wij vinden dat er ruim baan gegeven moet worden aan technologische ontwikkeling desnoods als daardoor privacy belangen in het gedrang komen. In dat geval zou belemmerende wetgeving aangepast moeten worden ten gunste van technologie.	Technologische innovaties dienen te voldoen aan de geldende wet- en regelgeving.	Technologische voortuitgang vinden wij belangrijk. Bij de beoordeling van innovaties laten wij ons primair leiden door de consequenties voor privacy. Wij staan negatief tegenover innovaties die de privacy aantasten.	Technologie biedt oplossingen voor wezenlijke maatschappelijke vraagstukken maar kan daarbij privacy bedreigend zijn. Samen met alle stakeholders zoeken wij naar oplossingen zonder dat dit ten koste gaat van privacy.
	Preventie Visie op preventie	In ons innovatiebeleid krijgt het voorkomen van privacyschendingen geen aandacht. Wij staan positief tegenover het gebruiken en/of ontwikkelen van 'privacy invasive' technologieën (PIT).	In ons innovatiebeleid voorzien wij in preventieve maatregelen voor de bescherming van privacy voor zover dit bijdraagt aan meer efficiëntie of mogelijke reputatieschade voorkomt.	In ons innovatiebeleid hebben privacy belangen van individuen prioriteit. Wij anticiperen op mogelijke privacy inbreuken en doen geen concessies aan preventieve maatregelen om die tegen te gaan.	In ons innovatiebeleid is de bescherming van privacy verankerd. In onze ambities om hieromtrent vernieuwend te zijn, betrekken wij in- en externe stakeholders. Samen met hen bepalen wij de spelregels.
	Privacy instellingen Visie op standaard privacy instellingen	Onze producten en diensten zijn standaard gebaseerd op openheid en toegankelijkheid. De privacy instellingen voor zover aanwezig, dienen door gebruikers zelf geactiveerd te worden.	De standaard privacy instelling in onze producten en diensten bepalen wij op basis van de wensen van onze (potentiële) klanten.	De privacy instellingen in onze producten en zijn standaard ingesteld op maximale privacy. Eventuele afwijkingen op deze instellingen staan wij toe voor zover die niet conflicteren met onze visie op privacy.	Onze producten en diensten zijn standaard ingesteld op maximale privacy. Samen met stakeholders streven wij naar vernieuwingen waarmee belangentegenstellingen worden opgeheven.
	Functionaliteit Visie op functionaliteit versus privacy belangen	Bij het vaststellen van de functionaliteit van onze producten en diensten, is privacy van ondergeschikt belang.	Wij vinden functionaliteit belangrijker dan privacy belangen. Waar nodig zullen wij met regelgeving rekening houden.	Wij streven naar volledige functionaliteit zonder verlies van privacy. Onze inspanningen zijn er op gericht om aan geen van beiden concessies te doen.	Wij richten ons op vernieuwingen waarmee het spanningsveld tussen privacy en functionaliteit kan worden opgelost. In deze discussie betrekken wij in- en externe stakeholders.
	Beveiliging Visie op beveiliging van informatie	In onze producten en diensten houden wij geen rekening met de beveiliging van informatie	Rondom de beveiliging van informatie voorzien wij in maatregelen voor zover daarmee inefficiënties, risico's op reputatieschade en inbreuken op wetgeving worden voorkomen.	Wij voelen ons verantwoordelijk voor de privacy belangen van betrokkenen. Wij voorzien in beveiligingsmaatregelen die aan deze belangen tegemoet komen.	
Society & instituties	Veiligheid Veiligheid en bestrijding van terreur, misdaad en fraude	Wij vinden dat er geen beperkingen mogen zijn voor het creëren van veiligheid. Persoonsgegevens moeten vrijelijk beschikbaar zijn voor terreur-, misdaad en fraudebestrijding.	In onze meningsvorming over de tegenstelling tussen privacy en veiligheid, laten wij ons leiden door de maatschappelijke opinie hieromtrent als ook door geldende wet- en regelgeving.	Veiligheid en privacy zien wij als gelijkwaardige, fundamentele grondrechten. Eventuele belangentegenstellingen zullen wij per geval beoordelen.	In onze besluitvorming met tegenstellingen tussen privacy en veiligheid, betrekken wij alle stakeholders teneinde te komen tot out-of-the box oplossingen waarmee recht wordt gedaan aan alle belangen.
	Marktwerving Visie op privacy versus marktwerving	De bescherming van privacy belangen van individuen is ondergeschikt aan het stimuleren van de markt.	In onze meningsvorming over de tegenstelling tussen privacy en stimulering van markt en kapitaal, laten wij ons leiden door de maatschappelijke opinie hieromtrent en/of wet- en regelgeving.	In onze visie mag het stimuleren van de markt niet ten koste gaan van de privacy van individuen.	In onze besluitvorming met tegenstellingen tussen privacy en marktwerving, betrekken wij alle stakeholders teneinde te komen tot out-of-the box oplossingen waarmee recht wordt gedaan aan alle belangen.
	Onderzoeksbelangen Visie op privacy versus onderzoeksbelangen	De privacy belangen van individuen zijn voor ons ondergeschikt aan onderzoeksbelangen.	In onze meningsvorming over het gebruik van persoonsgegevens ten behoeve van onderzoek, laten wij ons leiden door de maatschappelijke opinie en geldende wet- en regelgeving.	Wij staan positief tegenover het gebruik van geanonimiseerde persoonsgegevens ten behoeve van onderzoeksbelangen.	In onze besluitvorming met tegenstellingen tussen privacy en onderzoeksbelangen, betrekken wij alle stakeholders teneinde te komen tot out-of-the box oplossingen waarmee recht wordt gedaan aan alle belangen.
	Samenleving Visie op de samenleving	Wij zien de samenleving als een open netwerk van sociale relaties. Wij stimuleren mensen om contacten te leggen en met anderen verbonden te zijn.	Wij zien de samenleving als een geheel van sociale en economische relaties. Wij reageren op ontwikkelingen die hieromtrent onze bedrijfsvoering kunnen beïnvloeden.	Wij zien de samenleving als een geheel van sociale en economische relaties. Wij faciliteren de behoefte van mensen om een veilige haven te hebben waarin ze zichzelf kunnen zijn.	

7.5 Taxonomie subindicatoren

Indicator	Subindicator	Omschrijving
Grondhouding	Visie	Duidt de visie van ondernemingen op privacy en de mate waarin privacy wel of niet belangrijk wordt gevonden.
	Belang	Duidt de redenen waarom ondernemingen privacy wel of niet belangrijk vinden.
	Zeggenschap	Duidt de mate waarin individuen zeggenschap hebben over door henzelf verstrekte gegevens.
	Markt voor persoonsgegevens	Duidt hoe ondernemingen denken over de verhandelbaarheid van persoonsgegevens.
	Markt voor privacy	Duidt in hoeverre ondernemingen toegevoegde waarde zien in een markt voor privacy en 'privacy enhancing technologies' (PET).
	Mensenrecht	Is privacy een mensenrecht of zijn er andere, hogere doelen ten faveure waarvan privacy mag worden ingeleverd? Deze subindicator geeft aan hoe ondernemingen over deze vraag denken.
Compliance	Wettelijke regels	Duidt de algemene houding van ondernemingen richting privacy gerelateerde wet- en regelgeving.
	Privacy policy	Duidt in hoeverre ondernemingen het gebruik van privacy policies belangrijk vinden.
	Cookies	Duidt hoe ondernemingen denken over het gebruik van cookies in relatie met privacy belangen.
	Keurmerk en/of gedragscode	Duidt in hoeverre ondernemingen het belangrijk vinden om middels een keurmerk of gedragscode uiting te geven aan de relevantie van privacy.
	Doelbinding	Duidt in hoeverre ondernemingen zich binden aan doelbinding ofwel, het al dan niet gebruiken van persoonsgegevens voor andere doelen dan waarvoor deze zijn verkregen.
	Belangenorganisaties	Duidt in hoeverre ondernemingen participeren in belangenorganisaties rondom privacy.
Communicatie & Informatiedeling	Zichtbaarheid	Duidt in hoeverre ondernemingen hun visie op privacy zichtbaar uitdragen.
	Informatiedeling	Duidt in hoeverre persoonlijke gegevens worden gedeeld met derde partijen.
	Zwarte lijsten	Duidt het gebruik van 'zwarte lijsten' en de mate waarin ondernemingen rekening houden met de privacy belangen van wanbetalers, fraudeurs, e.d.
	Openbaarheid	Duidt de mate waarin ondernemingen openheid geven over de beloningsstructuur en compensaties.
Marketing	Marketing strategie	Welke marketing strategieën worden door ondernemingen gebruikt? In hoeverre heeft een klant controle over het gebruik van zijn persoonlijke gegevens? Deze subindicator geeft aan hoe ondernemingen over deze vragen denken.
	Customer intelligence	Duidt hoe ondernemingen omgaan met persoonsgegevens ten behoeve van 'customer intelligence' (CI) activiteiten.
	Kwaliteit en dienstverlening	Duidt hoe ondernemingen denken over het aanwenden van persoonsgegevens ten behoeve van kwaliteitsverbetering en dienstverlening.
	Economische voordelen	Duidt in hoeverre ondernemingen economische voordelen verbinden aan het beschikbaar stellen van persoonlijke gegevens.
HRM	Cameratoezicht	Duidt de houding van ondernemingen richting het gebruik van cameratoezicht op het werk.
	Screening	Het screenen van sollicitanten beoogt het detecteren van eventuele

Indicator	Subindicator	Omschrijving
		belastende feiten als ook het vaststellen van de juistheid en volledigheid van hun CV en presentatie. Deze subindicator geeft aan hoe ondernemingen hierover denken.
	Verzuim	Duidt in hoeverre ondernemingen rekening houden met de privacy rechten en belangen van medewerkers bij verzuim.
	Levenssfeer	Duidt de mate waarin ondernemingen inzicht wensen te hebben in de persoonsgegevens als ook de persoonlijke levenssfeer van medewerkers.
	Gedragscode	Duidt in hoeverre ondernemingen het belangrijk vinden om middels gedragscodes uiting te geven aan de wijze waarop zij invulling geven aan het personeelsbeleid.
	Personeelsbeleid	Duidt in hoeverre privacy in het algemeen is verankerd in het personeelsbeleid.
Innovatie & technologie	Technologie	Duidt in hoeverre ondernemingen vinden dat privacy ondergeschikt is aan technologische vooruitgang.
	Preventie	Duidt in hoeverre ondernemingen bij de ontwikkeling van nieuwe producten en diensten voorzien in maatregelen tegen mogelijke 'privacy invasive events'.
	Privacy instellingen	Duidt welke standaard privacy instellingen ondernemingen hanteren in hun producten en diensten.
	Functionaliteit	Duidt in hoeverre privacy ondergeschikt is aan functionaliteit of vice versa.
	Beveiliging	Hoe belangrijk is de beveiliging van gegevens voor ondernemingen? Welke maatregelen worden er hieromtrent getroffen? Deze subindicator geeft aan hoe ondernemingen hierover denken.
Society & instituties	Veiligheid	Duidt hoe ondernemingen denken over het opofferen van privacy ten behoeve van meer veiligheid.
	Marktwerving	Duidt in hoeverre ondernemingen achter het stimuleren van de markt ten koste van privacy staan.
	Onderzoeksbelangen	Duidt in hoeverre ondernemingen zich kunnen vinden in het inleveren van privacy ten behoeve van onderzoek.
	Samenleving	Hoe kijken ondernemingen naar de samenleving? Hoe wordt gekeken naar de verschillende soorten relaties die daarin bestaan? Wordt er ruim baan gegeven aan openheid of ligt de focus op het creëren van een veilige haven voor individuen? Deze subindicator geeft aan hoe ondernemingen hierover denken.