Radicand Economics

Verkenning naar privacy, cybersecurity en publieke belangen

8 mei 2017

Radicand Economics

Rapport in opdracht van het Ministerie van Economische Zaken

Radicand Economics

KvK 58927212 | KvK vestigingsnummer 000028251989

De Veste 20, 3443 DZ Woerden

www.radicandeconomics.com

Inhoudsopgave

Radicand Economics

Voorwoord

Het Ministerie van Economische Zaken heeft Radicand Economics gevraagd om een reflectie over privacy, cybersecurity en publieke belangen. Deze publieke belangen hebben nieuwe dimensies gekregen door de digitalisering. Wat zegt de economische theorie over de publieke belangen van privacy en wat zijn daar de mogelijke beperkingen van? Wat is — vanuit een perspectief dat verder reikt dan dat van consumenten die afspraken met bedrijven maken over hun persoonsgegevens — het publieke belang van privacy? Een uitwerking van deze vraag heeft implicaties voor de wenselijkheid en vormgeving van overheidsinterventie. Verder zijn er parallellen met cybersecurity, eveneens met implicaties voor de rol van de overheid. Dit rapport bevat de resultaten van een verkenning naar deze vragen.

Dr. Paul de Bijl

http://radicandeconomics.com

Samenvatting

Wat is het publieke belang van privacy en welke parallellen zijn er met cybersecurity? Een uitwerking van deze vraag geeft inzicht in de mogelijke rol van de overheid.

Privacy is alomtegenwoordig en moeilijk in een eenvoudige definitie te vangen. Daarin zijn vele dimensies te onderscheiden. Ofschoon men bij privacy in het economische domein van marktinteracties vooral denkt aan het gebruik van persoonsgegevens voor commerciële doeleinden, zijn ook daar meer fundamentele aspecten relevant. Een inbreuk op de privacy kan meer schade toebrengen dan de waarde van de betrokken economische interacties suggereert. Behalve dat privacy voorziet in een individuele behoefte is er ook een maatschappelijk belang, vanwege positieve externe effecten voor de economie en de maatschappij. Privacy-inbreuken brengen schade toe aan vertrouwen — een noodzakelijke voorwaarde voor een goed functionerende maatschappij.

De economische theorie veronderstelt dat consumenten, wanneer zij voldoende inzicht hebben in de situatie waarin zij zich bevinden, beslissingen kunnen nemen die aansluiten bij hun preferenties. Deze benadering kan tekort schieten bij het adresseren van de fundamentele aspecten van privacy. Door privacy, bijvoorbeeld in de vorm van informatieprivacy, te bekijken vanuit markttransacties, geeft men veel — in het digitale domein al snel te veel — gewicht aan het vermogen van individuen om adequate afwegingen te maken. Ook onderschat zo'n benadering mogelijk het algemenere, maatschappelijk belang van privacy.

In het digitale domein hangen de publieke belangen van privacy samen met het feit dat burgers en consumenten niet in staat zijn om, op basis van geïnformeerde instemming, adequate afspraken met bedrijven te maken over huidig en toekomstig gebruik van hun persoonlijke data. Dat stelt de bestaande wet- en regelgeving op de proef — maar deze kampt met een vergelijkbaar probleem, namelijk dat innovatie in digitale technologie leidt tot onvoorziene gevolgen. Zowel afspraken over als de publieke belangen van privacy zijn niet goed 'contracteerbaar'. Vooral bedrijven die data verzamelen en verwerken zullen een voldoende sterke prikkel moeten ervaren om in het maatschappelijk belang te handelen.

Een oplossingsrichting voor de borging van niet-contracteerbare publieke belangen ligt in een wettelijke aansprakelijkheid bij de partij die het beste in staat is om welvaartsverliezen door onvoorzien misbruik zoals in *holdup* problemen te voorkomen (het risico, in onvoorziene situaties, op het profiteren van het feit dat sommige betrokkenen zich ondertussen in een afhankelijke situatie bevinden). Individuele burgers hebben dat grotere belang niet op het netvlies en ervaren, bij een inbreuk, in eerste instantie alleen een individuele impact. Een voldoende stevige aansprakelijkheid voor bedrijven ondersteunt dat zij, bij dataverwerking en innovatie in gegevensgebruik, rekening houden met de belangen

van consumenten en de maatschappelijke consequenties van privacyschendingen. De economische impact van een effectief aansprakelijkheidsregime ligt in het realiseren van het welvaartspotentieel dat anders verloren zou gaan. De maatschappelijke impact is overigens groter, vanwege het fundamentele belang van vertrouwen.

Bestaande privacyregels geven al invulling aan aansprakelijkheid. Onder de Wet bescherming persoonsgegevens (Wbp), en binnenkort onder de Algemene Verordening Gegevensbescherming (AVG), is een organisatie die persoonsgegevens verwerkt of laat verwerken aansprakelijk voor schade door overtredingen. De AVG zorgt ook voor strengere verplichtingen voor transparantie en verantwoording, als vorm van ex ante regulering van dataverwerkende bedrijven. In welke mate wet- en regelgeving effectief zal zijn om consumenten te beschermen is nog een open vraag. Omdat inbreuken op de privacy, en ook de schade die daaruit voortvloeit, voor consumenten beperkt waarneembaar zijn, is het lastig om goede afspraken te maken over compensatie voor geleden schade. Uit rechtspraak en aanvullende nationale wetgeving zal moeten blijken of de aansprakelijkheid voldoende stevig wordt om de prikkels van bedrijven de goede kant op te richten.

Ofschoon privacy en cybersecurity nauw aan elkaar gerelateerd zijn, spelen er andere prikkels en risico's op marktfalen. Ook lijkt niet-contracteerbaarheid belangrijker te zijn voor privacy dan voor cybersecurity. Bij diensten waar privacy een rol speelt gaan betrokkenen bewust interacties aan en is het zinvol om na te denken over de beperkingen van de afspraken die zij kunnen maken. Problemen met cybersecurity worden daarentegen door buitenstaanders met kwade bedoelingen veroorzaakt. Dat leidt tot andere beleidsimplicaties, maar er zijn wel overeenkomsten. Bij beide thema's kan men beargumenteren dat marktpartijen voldoende prikkels dienen te hebben om hun gedrag te verbeteren. Wet- en regelgeving dragen daar aan bij, al verschillen de implicaties met betrekking tot de mate van aansprakelijkheid die nodig is om prikkels op één lijn te krijgen met de publieke belangen.

1. Inleiding

De digitalisering heeft nieuwe dimensies gegeven aan vraagstukken rondom privacy.[1] In 1999 zei Scott McNealy, als CEO van Sun Microsystems: *"You have zero privacy anyway. Get over it."*[2] Dat was nogal scherp gesteld, maar toch: privacy is niet meer wat was. Er is een sterke dynamiek van technologische ontwikkelingen rondom digitale en online diensten. De mogelijkheden tot grootschalige verzameling en analyse van gegevens over personen en individueel gedrag zijn groter dan ooit. Digitale business modellen veranderen met de dag. Burgers en consumenten ontberen inzicht en overzien niet hoe de gegevens die zij vandaag (al dan niet bewust) verstrekken, morgen gebruikt kunnen worden. Sterker, misschien bemerken zij het niet eens als er misbruik plaatsvindt.

Wat is het publieke belang van privacy en welke parallellen zijn er met de problematiek van cybersecurity? Een uitwerking van de vraag naar publieke belangen, in het licht van de digitalisering, geeft inzicht in de mogelijke rol van de overheid. Dit rapport reflecteert over deze vraag vanuit een economisch kader dat rekening houdt met het maatschappelijk belang van privacy en de beperkingen om daar grip op te krijgen met wet- en regelgeving. De publieke belangen nauw samen met het feit dat burgers en consumenten niet in staat zijn om, op basis van geïnformeerde instemming, adequate afspraken met bedrijven te maken over het gebruik van hun persoonlijke data. Dat stelt de bestaande wet- en regelgeving op de proef — maar deze kampt met een vergelijkbaar probleem, namelijk dat de dynamiek van de technologie leidt tot onvoorziene gevolgen. De publieke belangen zijn niet goed 'contracteerbaar'.

De opbouw van dit rapport is als volgt. Paragraaf 2 geeft een duiding van het begrip privacy. Paragraaf 3 bespreekt de individuele en maatschappelijke waarde. Privacy heeft individuele waarde voor burgers en consumenten, maar de maatschappelijke waarde reikt verder. Paragraaf 4 geeft, in een notendop, een overzicht van de economische literatuur over privacy en bespreekt de beperkingen van een economische invalshoek die privacy beschouwt als onderdeel van transacties. Paragraaf 5 betoogt dat privacy gepaard gaat met 'niet-contracteerbaarheid', een begrip uit de economische theorie over contracten. Paragraaf 6 verkent de beleidsimplicaties daarvan. Paragraaf 7 legt een verband tussen privacy en cybersecurity en bespreekt de verschillen in beleidsimplicaties. Paragraaf 8 concludeert.

[1] Zie de recente studie "Opwaarderen: Borgen van publieke waarden in de digitale samenleving", door het Rathenau Instituut (Kool e.a., 2017).

[2] Citaat opgetekend door Manes (2000).

2. Wat is privacy?

Wat is privacy? Lang geleden al spraken Warren and Brandeis (1890), in navolging van een rechterlijke uitspraak uit 1888, van "the right to be let alone".[3] Deze omschrijving vormt nog steeds een belangrijk referentiepunt.[4] [5] Deze paragraaf bespreekt enkele definities en vervolgens een typologie van privacy. De wetgever maakt overigens een onderscheid tussen privacy en bescherming van persoonsgegevens. Door technologische ontwikkelingen kan men deze concepten echter steeds moeilijker uit elkaar halen.[6]

De beknoptheid van bovenstaande definitie suggereert misschien dat privacy een eenvoudig concept is, maar het tegendeel is het geval. Moore (2008) bespreekt hoe lastig het is om privacy te definiëren en behandelt diverse manieren om tegen het begrip aan te kijken. Zo is er een onderscheid tussen een normatieve en een niet-normatieve ('positieve') invulling.

Een normatieve uitwerking gaat over morele claims en verplichtingen: wanneer heeft iemand recht op privacy en wanneer mogen anderen zich niet opdringen in het persoonlijke domein? Een niet-normatieve uitwerking beschrijft de toestand van privacy. Deze doet zich voor wanneer een individu (lichaam), plaats of persoonlijke informatie niet toegankelijk is voor anderen.

Op basis van een bespreking van diverse definities komt Moore uit bij de volgende (normatieve) invulling: "[...] *privacy is control over when and by whom the various parts of us can be sensed by others*" (uit Parker, 1974; p. 281). Vervolgens omschrijft hij het recht op privacy als het zeggenschapsrecht (*right to control*) op toegang tot en gebruik van plaatsen, lichamen en persoonlijke informatie.[7] Een privacyrecht vertoont daarmee enige gelijkenis met een eigendomsrecht.

Solove (2006) werkt, in een veel geciteerd artikel, een taxonomie uit van vormen van (schade door) privacyschendingen (*privacy harm*). Deze classificatie is bedoeld als raamwerk voor juridische toepassingen. Het kader onderscheidt informatieverzameling, informatieverwerking, informatieverspreiding en indringing.[8]

---

[3] Zie Moore (2008).

[4] Van Dale omschrijft privacy als "de mogelijkheid om in eigen omgeving helemaal zichzelf te zijn. "http://www.vandale.nl/opzoeken?pattern=privacy&lang=nn (geraadpleegd 1 maart 2017).

[5] Wikipedia spreekt over het zelf bepalen "wie welke informatie over ons krijgt" en de wens om "onbespied en onbewaakt te leven". https://nl.wikipedia.org/wiki/Privacy (geraadpleegd 1 maart 2017).

[6] Moerel en Prins (2016).

[7] Zo maakt iemand die binnenwandelt bij een slapende persoon en deze over het hoofd aait, inbreuk op de privacy van deze persoon, ook al zou de indringer vergeetachtig zijn (Moore, 2008).

[8] Andere duidingen van privacy zijn bijvoorbeeld te vinden in Magi (2011), Westin (2003) en Regan (2015).

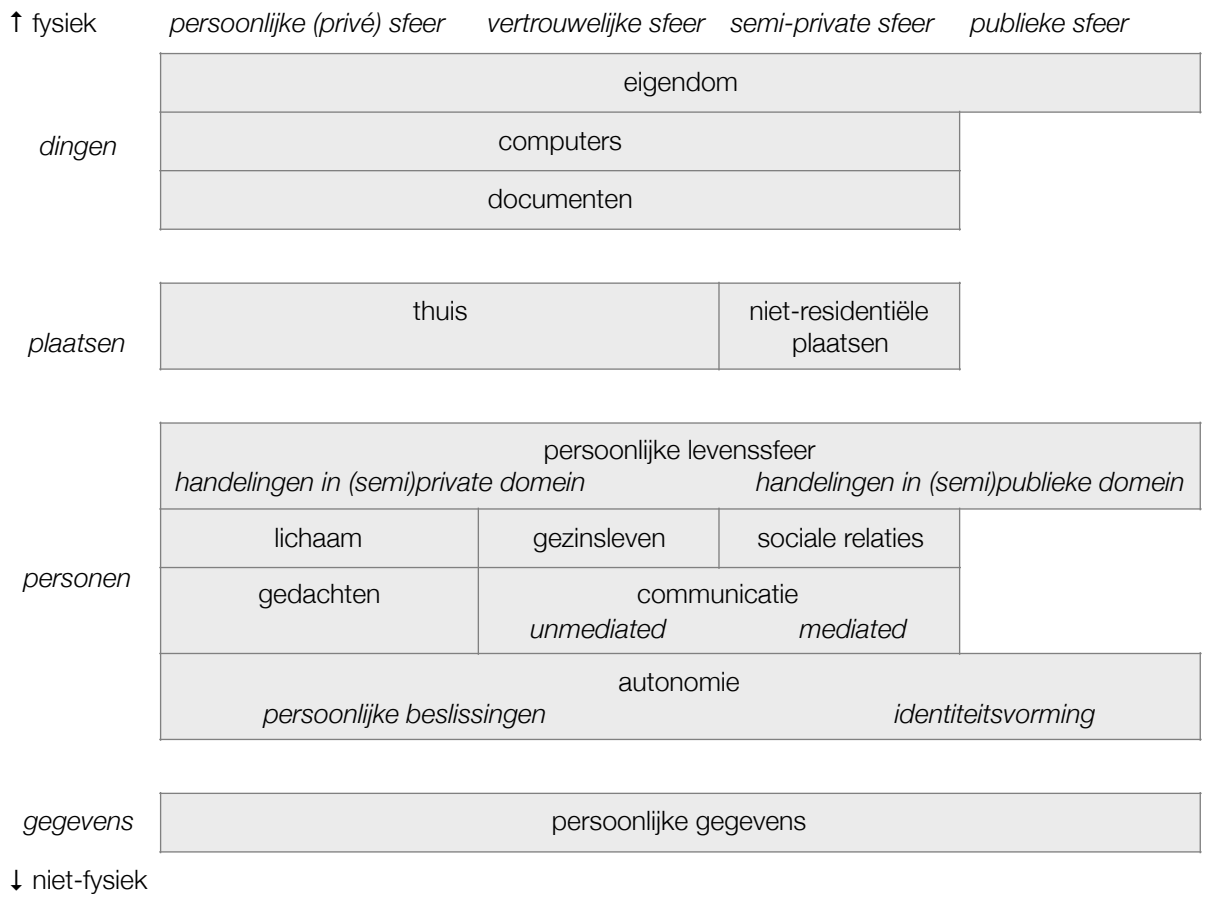
Koops et al. (2016) werken een inzichtelijke typologie van privacy uit op basis van een uitgebreide bespreking van de literatuur en een inventarisatie van grondwettelijke inbeddingen. Het doel is niet om voor te schrijven of om de relevantie van privacy te duiden, maar om structuur aan te brengen in het publieke debat. De voorgestelde indeling is daarmee vooral beschrijvend bedoeld.

Op basis van een inventarisatie van grondwettelijke inbeddingen in verschillende jurisdicties identificeren Koops et al. (2016) de volgende clusters:

1. *Privacy in het algemeen:* dit cluster omvat algemene formuleringen van het recht op privacy zoals opgenomen in grondwettelijke bepalingen.
2. *Privacy van plaatsen en eigendom:* dit cluster betreft bescherming van het thuis en andere plaatsen die onder de persoonlijke levenssfeer vallen, evenals de bescherming van informatie die gekoppeld is aan eigendom. In sommige jurisdicties zijn ook computers beschermd.
3. *Privacy van relaties:* dit cluster gaat over de bescherming van het gezinsleven, sociale relaties, communicatie (bijvoorbeeld via post of telecommunicatie) en documenten (bijvoorbeeld brieven).
4. *Privacy van personen (lichaam, geest, identiteit):* veel landen onderscheiden de bescherming van specifieke persoonsaspecten, zodat het zinvol is om deze in een eigen cluster op te nemen. Het cluster betreft de onschendbaarheid en integriteit van personen, de bescherming van gedachten, de autonomie van persoonlijke beslissingen en de beleving van persoonlijke identiteit.
5. *Privacy van persoonlijke gegevens:* dit cluster is vaak een separate paragraaf van de voorziening voor het algemene recht op privacy. Ofschoon sommige jurisdicties geen eigen voorziening voor deze vorm van bescherming kennen, is het zinvol om dit cluster, dat ook te bestempelen is als informatieprivacy, apart te benoemen.

Vervolgens werken de auteurs een typologie uit van objecten waar privacy-rechten betrekking op hebben. Tabel 1 bevat het resultaat. De horizontale as geeft het spectrum van de privésfeer tot het publieke domein weer. De verticale as rangschikt objecten naar de mate van tastbaarheid (*tangibility*).

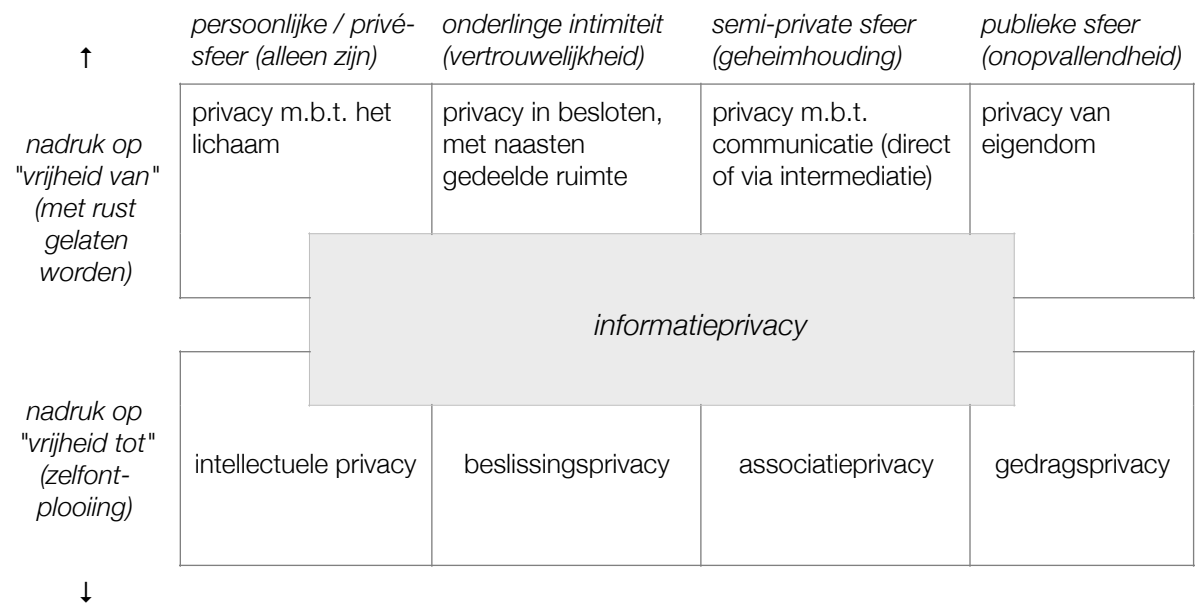
Tabel 1: objecten waar het recht op privacy betrekking op heeft (Koops et al., 2016)



Tabel 2 verbindt de hierboven onderscheiden objecten met verschillende soorten privacy. De horizontale as correspondeert met die in tabel 1. De verticale as onderscheidt 'negatieve' vrijheid (in de zin dat er geen inbreuk plaatsvindt) en 'positieve' vrijheid (in de zin van zelfbeschikking). De soorten privacy die men nu kan onderscheiden spreken, op enkele na, redelijk voor zich. Privacy van eigendom betreft het afschermen van privézaken wanneer men zich in een publieke ruimte begeeft. Een voorbeeld is een foto van een geliefde in een portefeuille. Associatieprivacy gaat over het bepalen met welke personen, groepen en gemeenschappen men relaties onderhoudt. Merk op dat informatieprivacy een speciaal type is, dat zich uitstrekt over de acht soorten van privacy zoals gedefinieerd door de twee assen. Het Rathenau Instituut benoemt diverse publieke waarden die samenhangen met digitalisering, die in grote lijnen overeenkomen met het idee achter tabel 2.[9]

[9] Kool e.a. (2017).

Tabel 2: typologie van privacy (Koops et al., 2016)



Tot zover het algemene begrip en de verschillende dimensies van privacy. De volgende paragraaf gaat, in overeenstemming met deze typologie, nader in op de waarde van privacy.

3. De waarde van privacy

Wat is de waarde van privacy? Wat is privacy waard? Deze vragen zijn niet hetzelfde. Deze paragraaf bespreekt de persoonlijke en maatschappelijke waarde van privacy. Deze waarde is niet nauwkeurig te becijferen, maar is zonder twijfel groot. We kunnen haar wel aanwijzen, maar het is ondoenlijk om haar vast te stellen.

3.1 Waarde voor het individu

Een bekende paradox is dat mensen in surveys rapporteren dat zij privacy belangrijk vinden, maar tegelijkertijd bereid zijn om privé-informatie prijs te geven in ruil voor een gratis dienst of korting, of voor slimme, toegespitste diensten.[10] Dat wil niet zeggen dat de waarde die mensen aan privacy toekennen klein is.[11] Integendeel, zoals ook blijkt uit de inbedding van privacy en gegevensbescherming in de Verdragen en het Handvest van de Grondrechten van de EU. Privacy en gegevensbescherming helpen mensen om een eigen persoonlijkheid te ontwikkelen, een onafhankelijk leven te leiden en verschaffen bepaalde vrijheden, zoals de typologie van privacy in tabel 2 liet zien. Dat suggereert ook dat de ethische component van online diensten (en daarmee van privacy) veelomvattender is dan bij goederen en diensten die niet met dataverzameling gepaard gaan — bijvoorbeeld omdat inbreuken op privacy direct gerelateerd zijn aan de menselijke waardigheid.[12]

De typologie van privacy in tabel 2 geeft in meer detail weer in welke dimensies de waarde van privacy tot uiting komt. Ten eerste hechten mensen eraan om met rust gelaten te worden. Zij ontlenen, afhankelijk van de situatie, nut aan alleen kunnen zijn, vertrouwelijkheid, geheimhouding en onopvallendheid. Ten tweede willen mensen vrijheid hebben om zichzelf te kunnen ontplooien. Daartoe hebben zij, afhankelijk van de situatie, baat bij het kunnen afschermen van wat zij denken en beslissen, met wie zij zich associëren en hoe zij zich gedragen.

De individuele waarde die mensen aan privacy toekennen is dus situatie-afhankelijk en kent vele facetten. Dat maakt de waarde van privacy sterk ambigu. Het is niet zinvol, laat staan mogelijk, om deze waarde in algemene zin te expliciteren of kwantificeren. Wel kan men de waarde van privacy in specifieke omstandigheden inschatten.

---

[10] Expertgroep Big data en privacy (2016).

[11] Syverson (2003).

[12] Buttarelli (2016), Kool e.a. (2017). Zie ook een interview met Giovanni Buttarelli (European Data Protection Supervisor), *Digidig*, 20 november 2016, http://www.digidig.it/2016/11/20/now-in-english-a-conversation-with-the-european-data-protection-supervisor/ (geraadpleegd op 22 april 2017).

Daar zijn verschillende manieren voor. In sommige jurisdicties kan een rechter een passende compensatie vaststellen bij een ongeoorloofd gebruik van persoonlijke informatie, bijvoorbeeld door de media.[13] Dergelijke compensaties vormen dan een (grove) benadering van de schade corresponderend met het verlies aan privacy voor het slachtoffer. Een andere manier is om mensen te vragen naar hun *willingness to accept* (WTA), ofwel de compensatie die zij passend vinden voor een aantasting van een bepaalde vorm van privacy. Een variant betreft de vraag naar de *willingness to pay* (WTP), ofwel de bereidheid om te betalen voor extra bescherming. Bovengenoemde methoden schatten de (economische) 'vraag' naar privacy, wat vergelijkbaar is met het schatten van vraagcurves voor producten en diensten die op markten verhandeld worden.

Methoden gebaseerd op WTA en WTP leiden tot een geschatte waardering in termen van geld. Empirisch onderzoek laat zien dat dergelijke waarderingen van privacy weliswaar niet compleet arbitrair zijn, maar wel sterk afhangen van *framing* effecten en context.[14] [15] De verkregen waarderingen zijn daarom zeer kneedbaar en veranderlijk. Ook relevant is het feit dat privacy niet vergelijkbaar is met een verhandelbaar goed — het is veelal een component bij een economische transactie (of onderdeel van een bundel). Het is daarom bijzonder lastig om empirisch verkregen privacy-waarderingen te interpreteren.

Daarbovenop is het voor individuen moeilijk om rationele beslissingen over privacy te nemen, bijvoorbeeld omdat het lastig is om het nut van zelfontplooiing te benoemen, of omdat privacyschendingen zich met een zeer lage kans voordoen maar wel een grote impact hebben. Dat gebruikers van apps en social media websites vaak de privacy-voorwaarden negeren, zegt vermoedelijk meer over de onleesbaarheid van die voorwaarden dan over de waarde die zij aan privacy toekennen.[16]

3.2 Waarde voor de maatschappij

Naast een individuele waarde van privacy is er een maatschappelijke waarde. Die hangt samen met externaliteiten of externe effecten. Dat zijn baten of kosten voor partijen die daar niet voor gekozen hebben. Zij krijgen bijvoorbeeld wél te maken met de gevolgen van, maar worden niet betrokken bij een handeling of transactie. Deze derde partijen krijgen dan te maken met een *spillover* effect, zoals ook bij vervuilende productiemethoden.

---

[13] Hartshorne (2010).

[14] Acquisti et al. (2009).

[15] *Framing* betreft de wijze waarop keuzemogelijkheden worden verwoord, met als doel om bepaalde aspecten te benadrukken dan wel minder nadruk te geven.

[16] Shostack en Syverson (2004).

Benutting van persoonsgegevens kan bijdragen aan slimme, toegespitste diensten, waar niet alleen de consument maar ook de maatschappij van kan profiteren. Dan is er sprake van positieve externe effecten. Toepassingsgebieden zijn bijvoorbeeld de verkeersveiligheid, verduurzaming, en de zorg.[17] Het is op voorhand niet duidelijk wat het optimale niveau van privacy zou zijn. Strikte privacyregels zouden de maatschappelijke *spillovers* kunnen verminderen, bijvoorbeeld omdat het innovatie door bedrijven zou kunnen beperken.[18] Op dat argument valt wel wat af te dingen, omdat strikte regels voor duidelijkheid zorgen, wat leidt tot minder reguleringsonzekerheid. Dat is juist goed voor innovatieprikkels.

Privacyschendingen gaan vaak gepaard met negatieve externe effecten. Denk bijvoorbeeld aan het afketsen van kredietaanvragen of sollicitaties door slachtoffers van een privacyschending of identiteitsdiefstal, wier reputatie (mogelijk onterecht) beschadigd is.[19] Kredietverschaffers en werkgevers die op basis van oppervlakkige informatie beslissingen nemen, kunnen een kandidaat dan onterecht afwijzen. Dat kan de mogelijkheden tot ontwikkeling en zelfontplooiing blokkeren.

Een ander negatief extern effect treedt op wanneer de beslissing van een persoon om informatie te delen gevolgen heeft voor personen die ervoor kiezen om te zwijgen: naarmate meer niet-rokers zich kenbaar maken aan zorgverzekeraars, kunnen deze beter afleiden wie wél rookt.[20] Dit laatste aspect ondermijnt het model van *informed consent* (geïnformeerde instemming), wat voor economische analyses vaak een startpunt vormt (zie paragraaf 4). Niet alleen de belangen van degene op wie persoonsgegevens betrekking hebben doen ertoe. Ook de belangen van anderen, die geen partij zijn in een transactie, kunnen op het spel staan bij het verzamelen en overdragen van persoonlijke informatie.

In algemenere zin vloeit de maatschappelijke waarde van privacy voort uit het feit dat de maatschappij baat heeft bij privacy voor individuen.[21] Ten eerste zijn er de *spillovers* van vertrouwen en geheimhouding. Deze vormen van afscherming vergroten de effectiviteit van overleg en communicatie, wat goed is voor het functioneren van de economie en de maatschappij. Ten tweede profiteren collectiviteiten van betere mogelijkheden voor zelfontplooiing van individuen. Omgekeerd ondermijnen individuele privacy-inbreuken het functioneren van het grotere geheel, omdat zij het vertrouwen schaden, wat een noodzakelijke voorwaarde vormt voor vruchtbare interacties tussen individuen. Een ondermijning van het maatschappelijk vertrouwen is zeer moeilijk te repareren.

---

[17] Expertgroep Big data en privacy (2016).

[18] Bijlsma et al. (2014).

[19] Cavoukian (2009).

[20] MacCarthy (2011).

[21] Zie bijvoorbeeld Regan (2002, 2015) en Solove (2006).

Kortom, privacy heeft in haar essentie betrekking op veel meer dan interacties tussen bedrijven en consumenten. Het publieke belang van privacy is fundamenteler van aard dan de impact op het goed functioneren van markten waar persoonsgegevens en informatieprivacy een rol spelen.[22] Regan (2015, p. 63) stelt dat privacy steeds minder een 'privaat goed' is, waarvan betrokkenen het gewenste niveau kunnen bepalen of 'terugkopen' — het is veel meer een 'publiek goed' geworden, in de zin dat er externe effecten optreden en dat het raakt aan het functioneren van instituties.

De maatschappelijke waarde van privacy is, net als de individuele waarde, niet vast te stellen, maar laat zich, qua aard en belang, enigszins vergelijken met eigendomsrechten. Het ontbreken daarvan, of het tekortschieten van de handhaving van dergelijke rechten, zou niet alleen leiden tot enorme transactiekosten en welvaartsverliezen, het zou het functioneren van onze maatschappij op een fundamentele wijze aantasten. Vanuit een ruimer perspectief kan men privacy zelfs beschouwen als "[...] een voorportaal voor andere fundamentele rechten en vrijheden van het individu die gezamenlijk weer instrumenteel zijn voor het goed functioneren van onze democratische rechtsstaat" (Moerel en Prins, 2016, p. 33).

De implicatie van bovenstaande is dat het niet volstaat om beleid te baseren op bilaterale verhoudingen en onderhandelingen tussen bedrijven en gebruikers (al dan niet ondersteund door regulering). Zoals de volgende paragraaf laat zien, is dat vaak wel het uitgangspunt van economische analyses van privacy.

[22] Nehf (2003), Kool e.a. (2017).

4. Economische literatuur over privacy

Een economische benadering van privacy gaat uit van de waarderingen die individuen toekennen aan privacy en die tot uiting komen in hun preferenties. De economische theorie veronderstelt dat consumenten, wanneer zij voldoende inzicht hebben in de situatie waarin zij zich bevinden, beslissingen kunnen nemen die aansluiten bij hun preferenties. Waar bedrijven een prikkel hebben om zoveel mogelijk informatie over personen te verzamelen, kan het voor een consument rationeel zijn om vooral aandacht te geven aan het betreffende product en minder moeite te doen om de gevolgen voor privacy te doorgronden.[23] [24] Bijgevolg komt er minder privacy tot stand dan maatschappelijk gezien wenselijk kan zijn. Overheidsinterventie kan deze vorm van marktfalen vervolgens corrigeren. Dat is op zichzelf een sluitende redenering, maar wel afhankelijk van specifieke aannames, die het integrale perspectief op maatschappelijke en publieke belangen beperken.

4.1 Overzicht van de literatuur in een notendop

Acquisti et al. (2016) geven een uitgebreid overzicht van de economische literatuur over privacy. Zij onderscheiden daarin drie 'golven'.

De eerste golf kwam op in de jaren '70 van de vorige eeuw en bestond uit algemene economische argumenten over de gevolgen van het afschermen dan wel vrijgeven van persoonlijke gegevens die relevant zijn voor economische transacties. Op basis van zijn of haar preferenties met betrekking tot privacy, of van preferenties over de gevolgen van informatie-overdracht op de uitkomsten van transacties, kan een individu rationele beslissingen nemen aangaande persoonlijke gegevens. Deze beslissingen kunnen doorwerken op de effectiviteit van transacties, bijvoorbeeld omdat het vrijgeven van gegevens een informatie-asymmetrie tussen vragers en aanbieders verkleint. Omdat individuele afwegingen kunnen verschillen van wat maatschappelijke gezien optimaal is, leiden de keuzes van individuen niet automatisch tot welvaartsmaximalisatie. Dan is er een marktimperfectie, die mogelijk verminderd kan worden met het (via wet- en regelgeving) afdwingen van meer of minder privacy.

De tweede golf kwam op in de jaren '90, in reactie op de opkomst van informatietechnologie en de mogelijkheden om gebruikersdata op te slaan en te verwerken. Het volgende illustreert de problematiek die daarbij in beeld kwam. Een consument zou, in de hoop op het krijgen van een betere aanbieding, de rationele beslissing kunnen nemen om persoonsgegevens te delen met een bedrijf. Bijvoorbeeld het instemmen met het verzamelen en opslaan van

[23] Regan (2015).

[24] De gedragswetenschappen bieden hier aanvullende dan wel alternatieve verklaringen voor.

zoekgeschiedenis en persoonlijke data door Google. Naarmate de zoekmachine meer weet van de gebruiker, kan die relevantere zoekresultaten voorschotelen. Echter, wanneer Google deze gebruikersdata doorverkoopt aan derden, of gebruikt om commerciële uitingen op te nemen in de zoekresultaten, kan de gebruiker minder goed doorzien wat de impact is van het instemmen met de gebruiksvoorwaarden van de zoekmachine. Gebruikers kunnen dan blootgesteld worden aan negatieve externe effecten, bijvoorbeeld in de vorm van prijsdiscriminatie resulterend in hogere prijzen bij online aankopen.

De derde golf begon in het eerste decennium van de huidige eeuw en is nog niet ten einde. Deze ligt, met de trend naar digitalisering en online interacties, in het verlengde van de ICT-revolutie. Het is op steeds grotere schaal mogelijk om gebruikers- en gedragsgegevens te verzamelen, aggregeren en analyseren (*big data*), met name via zoekmachines, social media en websites. Er is een enorme kloof ontstaan tussen de inspanningen van bedrijven om online gedrag te volgen (*tracking*) en wat mensen daarover weten of veronderstellen.[25] Zodra zij online gaan, maken bedrijven "profielen" aan (*profiling*) om door te verkopen op veilingen voor gebruikersgegevens (*realtime bidding*). Dat gaat niet alleen met behulp van *cookies*, maar bijvoorbeeld ook via *beacons* waarmee het mogelijk is om toetsaanslagen en muisbewegingen te observeren. Zodoende komen bedrijven veel meer te weten dan alleen welke websites mensen bezoeken. De zo verkregen gegevens zijn waardevol voor adverteerders, die slimme technieken inzetten om, op basis van hun inzicht in gedrag en persoonskenmerken, advertenties op maat voor te schotelen (*behavioral targeting*). Achter de schermen van de portalen waarop burgers en consumenten met bedrijven in contact komen, bevindt zich dus een ongekende bedrijvigheid om advertenties toe te spitsen op individu, locatie en tijdstip.[26] Het business model van een bedrijf als Google is gebaseerd op een digitaal platform waarbij consumenten niet zozeer gebruikers zijn, maar vooral leveranciers van persoonlijke, commercieel relevante informatie, bijvoorbeeld voor de verkoop van online advertentieruimte.[27] In deze digitale wereld van grootschalige verwerking van en handel in data hebben veel consumenten een gebrekkig besef van de mate waarin zij de 'grondstof' leveren voor het productieproces van digitale platforms.

De economische literatuur, zowel qua theorie als empirie, laat in grote lijnen het volgende zien.[28] Ten eerste is er geen overkoepelende economische theorie van privacy. De reden is dat privacy sterk context-afhankelijk is. Ten tweede kan privacybescherming zowel gunstig als ongunstig uitpakken voor individu en maatschappij, wederom afhankelijk van de situatie.

---

[25] Zie bijvoorbeeld "Online Tracking and Behavioral Profiling", epic.org, https://epic.org/privacy/consumer/online_tracking_and_behavioral.html (geraadpleegd 22 april 2017).

[26] Zie ook Martijn en Tokmetzis (2016).

[27] Teece (2010).

[28] Acquisti et al. (2016).

Ten derde zijn consumenten zich niet of te weinig bewust van bedreigingen voor privacy en de gevolgen van het delen dan wel beschermen van persoonlijke informatie. Daarom is er in de regel geen sprake van een daadwerkelijk geïnformeerde toestemming van consumenten bij interacties op markten. Ook hangen privacy-beslissingen door consumenten in sterke mate af van specifieke beslissingsregels die zij hanteren in onoverzichtelijke situaties. Private initiatieven, zoals zelfregulering door bedrijven om de transparantie over datagebruik te vergroten, of voorlichting gericht op het versterken van privacy-bewustzijn van consumenten, zijn niet toereikend. Zij creëren geen evenwichtigheid tussen het delen en afschermen van informatie, omdat zij onvoldoende belang toekennen aan de fundamentele aspecten en waarde van privacy — aspecten die consumenten moeilijk kunnen meenemen in concrete beslissingssituaties.

4.2 Beperkingen van een economische benadering

Een economische benadering van privacy kent logischerwijs beperkingen, zoals blijkt uit paragrafen 2 en 3. Een gangbare economische analyse, die coherent en intern consistent kan zijn, kan tekort schieten bij het adresseren van fundamentele aspecten van privacy.[29] De reden daarvoor is dat privacy, bijvoorbeeld wanneer het betrekking heeft op informatieprivacy, als probleem op het niveau van markttransacties gezien wordt. Dat geeft veel (mogelijk te veel) gewicht aan het vermogen van individuen om, met betrekking tot privacy in het digitale domein, adequate afwegingen te maken. Ook onderschat zo'n benadering het algemenere, maatschappelijk belang van privacy (zie paragraaf 3).

Een voorbeeld van een economische benadering is een studie naar het functioneren van de markt voor persoonsgegevens door Bijlsma et al. (2014). Deze studie bevat een heldere analyse en bespreekt belangrijke, relevante beleidsimplicaties. De auteurs stellen dat mensen zowel voor- als nadelen kunnen ondervinden van de toenemende verzameling en toepassing van persoonsgegevens. De auteurs stellen dat betrokkenen het beste zelf afwegingen over de voor- en nadelen van gegevensgebruik kunnen maken, omdat business modellen onderling verschillen en iedereen anders over privacy denkt. Individuele keuzevrijheid op een markt voor gebruiksrechten van persoonsgegevens verbindt burgers en bedrijven en stimuleert een innovatief gebruik van persoonsgegevens. Om deze markt goed te laten werken is er wel overheidsinterventie nodig, bijvoorbeeld om het vertrouwen van burgers te borgen en om ongewenste gevolgen van 'beperkte rationaliteit' van consumenten te ondervangen. Dergelijke maatregelen maken het mogelijk dat er passende privacy-overeenkomsten tot stand kunnen komen. Er is wel een afweging: naast vertrouwen is ook ruimte voor ondernemerschap en innovatie door bedrijven belangrijk.

[29] Nehf (2003), MacCarthy (2011).

Economische analyses zoals hierboven besproken geven inzicht in de imperfecties die optreden bij transacties waarbij privacy een rol speelt, en verhelderen de beleidsimplicaties. Vanwege de gekozen invalshoek (marktinteracties zonder externe effecten voor de maatschappij als geheel), zijn dergelijke analyses echter niet afdoende om de publieke belangen van privacy te duiden. Een survey onder klanten van supermarkten in de Verenigde Staten, over hun vermogen om afwegingen over privacy te maken, liet een interessant beeld zien.[30] Het ontbreekt mensen vaak aan basiskennis om een geïnformeerde afweging van kosten en baten te maken. Er zijn grote onderlinge verschillen in het inzicht dat mensen hebben in marketingpraktijken. Een groot deel gelooft ten onrechte dat wetgeving hen tegen prijsdiscriminatie beschermt. Zelfs wanneer mensen een afweging maken, doen zij dat vaak op basis van verkeerde informatie. Beter geïnformeerde mensen lijken, vreemd genoeg, juist onverschillig te worden: zij verschaffen weliswaar hun persoonsgegevens, maar niet op basis van een afweging van kosten en baten.

De beperkingen van een economische analyse van transacties waar privacy deel van uitmaakt, blijken uit de diverse aannames die eraan ten grondslag liggen — al dan niet impliciet. Een eerste aanname is dat privacy gaat over de mogelijkheid tot het uitoefenen van zeggenschap over persoonsgegevens, die bovendien verhandelbaar zijn. In het licht van de huidige technologische ontwikkelingen, aangewakkerd door digitalisering, en de toenemende reikwijdte van de commerciële verwerking van persoonlijke gegevens, knelt deze aanname steeds meer. Consumenten kunnen deze 'markt' amper overzien en de mogelijkheid om zeggenschap uit te oefenenen boet steeds meer in aan effectiviteit. De reden ligt in de digitalisering, die onder meer tot uiting komt in online activiteiten door consumenten. Zij hebben geen notie van de omvang en wijze van gegevensverzameling, laat staan dat zij inzicht hebben in de reikwijdte van analyses en koppeling van bestanden. In de toekomst komen daar de mogelijkheden voor dataverzameling op het *Internet of Things* bovenop. Het is de vraag of een sterkere handhaving van privacyregels dit gebrek aan inzicht kan compenseren.

Een tweede aanname is dat men privacy kan beschouwen als een aspect van transacties waar individuen specifieke waarderingen voor hebben. Zij begrijpen dus welke waarde privacy voor hen vertegenwoordigt. Onder deze aanname kunnen zij kosten en baten afwegen en indien nodig onderhandelen over een passende compensatie voor het gebruik van persoonsgegevens. Deze en de vorige aanname liggen ten grondslag aan het idee van geïnformeerde instemming, op basis waarvan consumenten zeggenschap over hun persoonsgegevens kunnen uitoefenen.[31] Wanneer consumenten 'beperkt rationeel' zijn,

[30] Turow (2016).

[31] MacCarthy (2011).

zouden extra rechten bescherming kunnen bieden. Paragraaf 5 bespreekt het concept van geïnformeerde instemming in het digitale domein.

Een derde veronderstelling is dat een privacy-overeenkomst relevante voorwaarden kan beschrijven voor verschillende vormen van gebruiksrechten van persoonsgegevens. Het gebruik van persoonsgegevens is dus in grote mate 'contracteerbaar' voor marktpartijen (ook hierover in paragraaf 5).

Een vierde aanname betreft de nadruk op de individuele waardering voor (en kosten van inbreuk op) privacy, wat zou kunnen impliceren dat daar de essentie in ligt. Paragraaf 3 onderstreepte juist het belang van de maatschappelijke *spillovers* van het waarborgen van privacy als argument voor overheidsinterventie — niet zozeer als een aspect van marktinteracties waarbij persoonsgegevens verzameld of overgedragen worden, maar als randvoorwaarde voor een goed functionerende maatschappij.

Kortom, hoewel een reguliere economische analyse tot relevante, weloverwogen beleidsimplicaties kan leiden, geeft zij geen compleet beeld. Er kan niet worden uitgesloten dat het niveau van privacy dat resulteert uit marktinteracties (al dan niet ondersteund door wet- en regelgeving) nog steeds niet correspondeert met individuele voorkeuren en maatschappelijk gewenste randvoorwaarden.[32] Dat kan een vermindering van het in de maatschappij aanwezige vertrouwen tot gevolg hebben, met de daarmee gepaard gaande kosten en ontwrichting. De volgende paragraaf werkt verder uit waarom toestemming van individuen en het aangaan van contractuele relaties met bedrijven onvoldoende basis bieden voor een redelijke maatvoering — gebaseerd op een gedeeld begrip en wederzijdse verstandhouding — bij de verzameling en verwerking van persoonlijke data.[33]

[32] Regan (2002).

[33] Juristen spreken van de rechtmatigheid van gegevensverwerking (Moerel en Prins, 2016, p. 34).

5. Privacy als incompleet contract

Het Rathenau Instituut deed onlangs de volgende constatering:

> "Het samenspel van het toenemend aantal handelende systemen zorgt voor een nieuwe laag van complexiteit, en mogelijke onvoorziene effecten: dat geldt voor de individuele burger waarbij het slimme huis vastloopt door de interacties tussen verschillende 'slimme' apparaten, maar ook op maatschappelijk niveau wanneer de beurs crasht door autonoom handelende algoritmen." (Kool e.a., 2017, p. 76.)

De ICT-revolutie, de opkomst van digitale platformen en de explosieve groei in het verzamelen, bewerken en verhandelen van (veelal persoonlijke) data zijn uitingen van technologische verandering. Zij vormen een systeem dat gekenmerkt wordt door complexiteit, dynamiek, een gebrek aan transparantie en tekortschietend begrip.[34] Deze eigenschappen maken een systeem moeilijk te bevatten, met als gevolg dat er onverwachte uitkomsten kunnen optreden.[35] Deze paragraaf beargumenteert dat de impact van technologie op privacy in toenemende mate leidt tot het verschijnsel van *unanticipated consequences*, ofwel onvoorziene gevolgen.[36]

5.1 Theorie van incomplete contracten

Het verschijnsel van onvoorziene gevolgen hangt samen met het idee van incomplete contracten uit de economische theorie. Complete (of volledige) contracten bieden, vaak via een procedurele insteek, effectieve bescherming tegen voorzienbare ongewenste uitkomsten. In zo'n contract specificeren partijen, ex ante, de rechtsgevolgen van elke mogelijke 'toestand van de wereld' die zich, ex post, kan voordoen.[37] Het contract dekt dan alle onzekerheden af.

Een contract is incompleet wanneer het niet mogelijk is om alle voor de transactie relevante eventualiteiten erin op te nemen. Het contract dat partijen opstellen kan de (toekomstige) toestand van de wereld dan niet helemaal afdekken.[38] In dat geval zijn bepaalde aspecten die relevant zijn om afspraken over te maken, niet 'contracteerbaar'.[39] Dan ontstaan er

---

[34] Regan (2015).

[35] Dorner (1989), besproken in Healy (2005).

[36] Healy (2005).

[37] 'Ex ante' betekent vóór ondertekening van het contract en 'ex post' verwijst naar de situatie na ondertekening.

[38] Maskin 2002).

[39] Dit concept heeft niet alleen betrekking op daadwerkelijke contracten, het kan ook gaan over de onmogelijkheid om harde afspraken te maken over specifieke variabelen die relevant zijn voor de uitkomst van een proces of transactie.

haperingen die leiden tot inefficiënties. Paragraaf 6 komt daarop terug in de context van het digitale domein en privacy.[40]

Juristen zien een contract vaak als een juridisch bindende belofte om in de toekomst een bepaalde handeling te verrichten, zoals het leveren van een dienst op een specifieke datum tegen een afgesproken vergoeding. Incompleetheid van een contract betekent voor juristen iets anders dan voor economen:

- Voor een jurist is een contract incompleet wanneer het voor sommige toestanden van de wereld niet voorschrijft hoe partijen dienen te handelen of wat hun verplichtingen zijn. Wanneer zo'n toestand zich voordoet, kan een rechter het contract ontbinden dan wel een default verplichting toepassen. De uitspraak van een rechter zal in de regel uitgaan van juridische principes en niet van de potentieel te realiseren 'waarde'.
- Voor een econoom is een contract incompleet wanneer het niet in staat is om voor elke toestand van de wereld te voorzien in verplichtingen die tot een efficiënte uitkomst (in termen van waardecreatie) leiden. Er hoeft weliswaar geen onduidelijkheid te zijn over de verplichtingen van partijen, maar het contract kan bij sommige eventualiteiten gebrekkig of onvoldoende specifiek zijn qua informatie.[41]

Wij hanteren in wat volgt de economische invulling van niet-contracteerbaarheid. Aan die niet-contracteerbaarheid kunnen verschillende oorzaken ten grondslag liggen:

1. sommige aspecten van de toestand van de wereld zijn niet algemeen waarneembaar, zodat bijvoorbeeld een rechter niet kan verifiëren of deze zich hebben voorgedaan;
2. sommige aspecten worden niet voorzien, of zijn niet vooraf te beschrijven, door contractpartijen;
3. het vraagt te veel inspanningen of kosten om de relevante aspecten van toekomstige toestanden van de wereld in een contract op te nemen.

Nu zou men kunnen stellen dat het er niet toe doet dat partijen de toekomstige toestand van de wereld niet kunnen voorzien of omschrijven, wanneer zij een contract ex ante afhankelijk kunnen maken van de *payoffs* (de uitkomsten die partijen realiseren uit de transacties die zij met elkaar aangaan) die zich in de toekomst kunnen voordoen.[42] Een voorwaarde daarvoor is echter dat die uitkomsten algemeen waarneembaar zijn — anders kan men daar geen contract over afsluiten. Door de snelle technologische ontwikkelingen rondom data is deze voorwaarde ondertussen problematisch geworden, zoals § 5.2 in meer detail bespreekt.

---

[40] Zie bijvoorbeeld Hart (1995).

[41] Scott en Triantis (2005).

[42] Maskin en Tirole (1999).

5.2 Onvoorzien en onopgemerkt misbruik van persoonsgegevens

In een publicatie over *privacy engineering* bespreekt het Amerikaanse National Institute of Standards and Technology (NIST) het risico op een gebrek aan voorspelbaarheid van de motivatie voor het verzamelen van persoonsgegevens en handelingen die daarmee verricht kunnen worden.[43] Voorspelbaarheid komt tegemoet aan zorgen over onaangename verrassingen die een maatschappelijke terugslag kunnen veroorzaken. Een datasysteem verricht een 'problematische handeling' wanneer het niet voldoet aan de voorwaarde van voorspelbaarheid. NIST geeft daar de volgende voorbeelden van:

1. *Onvoorziene toe-eigening:* persoonlijke gegevens worden gebruikt op manieren waar een individu bezwaar tegen zou hebben of extra compensatie voor had willen hebben, zonder dat er een marktfalen is dat de mogelijkheid om daarover te onderhandelen beperkt. Persoonsgegevens worden dan gebruikt op manieren die verder gaan dan de verwachtingen of toestemming van de betreffende persoon.
2. *Onvoorziene openbaring:* samenvoeging en analyse van grote en/of verschillende gegevensbestanden leidt tot niet-contextueel gebruik van data of stelt een individu (of facetten van een individu) op onverwachte manieren bloot aan privacyschendingen.

Onvoorziene toe-eigening (punt 1) vormt een reëel risico in het digitale domein, waarin geavanceerde analyses van *big data* mogelijkheden verschaffen om persoonlijke informatie over consumenten te ontdekken die, op basis van de onderliggende gegevens, in beginsel onopgemerkt zou dienen te blijven. Een voorbeeld betreft een data-analyse van geaggregeerde, geanonimiseerde bestanden die, door deductie of het combineren met andere bestanden, leidt tot het omzeilen van de anonimisering.[44] Het niet kunnen anticiperen op technologische ontwikkelingen rondom data-analyse en het gebrek aan notie van de wijze waarop gegevens gebruikt worden beperken de mogelijkheid om daar vooraf afspraken over te kunnen maken.

'Context' (in punt 2) verwijst naar de omstandigheden van het verzamelen, verwerken, ontsluiten en vasthouden van persoonsgegevens. Voorbeelden van contextuele factoren zijn de aard en frequentie van directe interacties tussen een individu en het systeem, de goederen en diensten die het systeem levert, de typen persoonsgegevens die redelijkerwijs noodzakelijk zijn om het systeem te laten functioneren, het begrip dat individuen hebben van de verzameling en verwerking van gegevens door het systeem en de kennis die het systeem heeft over de privacy-voorkeuren van individuen. Het niet kunnen voorzien van ontwikkelingen in technologie en business modellen beperkt de contracteerbaarheid.

[43] NIST (2014).

[44] King en Forder (2016).

Voorbeelden van schade die bovengenoemde problematische handelingen kunnen veroorzaken zijn, aldus NIST (en in grote lijnen conform de typologie van privacy in paragraaf 2), een vermindering van vrijheid tot zelfbeschikking en zelfontplooiing, een onbalans in de machtsverhouding tussen individuen en bedrijven, een verlies aan vertrouwen dat consumenten hebben in de omgang met persoonsgegevens door bedrijven en economische schade door het uitblijven van een faire uitkomst in transacties waarin persoonsgegevens een rol spelen. Een economische analyse vanuit markttransacties kan deze aspecten van schade hooguit deels in beeld brengen (zie paragraaf 4).

Merk op dat sommige schade niet alleen onvoorzien kan zijn ten tijde van het aangaan van een overeenkomst, maar later ook onopgemerkt kan blijven. Bij het overdragen van persoonsgegevens aan een digitaal platform dat deze data vervolgens doorverkoopt, bijvoorbeeld aan een partij die deze koppelt met andere bestanden, kan een individu op een gegeven moment niet meer achterhalen wat daar de consequenties van zijn — ook al krijgt hij of zij op een later moment te maken met hogere prijzen door prijsdiscriminatie in een ongerelateerde markt. Er kan dus sprake zijn van *onvoorzien en onopgemerkt gebruik/ misbruik van persoonsgegevens*.[45] Privacy heeft daarmee kenmerken van een *credence good*, ofwel een goed waarvan een koper de kwaliteit noch voor aankoop, noch na aankoop kan waarnemen.

5.3 Niet-contracteerbaarheid van privacy

Innovatieve producten en diensten worden vaak een succes omdat zij in een behoefte voorzien. De vervulling van die behoefte kan zwaarder wegen dan het (gepercipieerde) verlies aan privacy. Dat suggereert dat consumenten een geïnformeerde beslissing nemen. Toen het enkel ging om het 's avonds sluiten van de gordijnen was daar nog sprake van. Burgers en consumenten zijn echter in steeds grotere mate onwetend over de manieren waarop bedrijven met hun persoonsgegevens omgaan. De vorige paragraaf benoemde dat het voor consumenten steeds moeilijker wordt om te voorzien wat bedrijven met hun data kunnen en zullen gaan doen, wat wijst op een risico op onvoorzien en onopgemerkt gebruik of misbruik van persoonsgegevens. Dat komt op diverse manieren aan de oppervlakte in de afspraken die partijen over privacy (proberen te) maken.

De gebruikersvoorwaarden die consumenten voorgeschoteld krijgen, zijn qua lengte en complexiteit niet te begrijpen.[46] Aanbieders stellen deze voorwaarden vaak niet zozeer op om afnemers te informeren, maar om aansprakelijkheid af te wentelen. Zij staan in geen verhouding tot de feitelijke *agency* van consumenten, ofwel het vermogen om macht of

[45] De Bijl (2017).

[46] Moerel en Prins (2016).

invloed uit te oefenen op wat er met hun persoonsgegevens gebeurt. Gebruikerstoestemming (*user consent*) vormt dan ook een gebrekkige basis voor het maken en handhaven van afspraken, ook omdat inherente cognitieve en psychologische beperkingen invloed hebben op het proces van het verlenen van toestemming.[47] Consumenten denken, wanneer ze een privacyverklaring zien, dat ze beschermd zijn, en vinden het vervolgens niet meer nodig om deze te lezen.[48] Zij kunnen eenvoudigweg niet voorzien wat de gevolgen zijn van het aangaan van een gebruikersovereenkomst, ook al bevat die gedetailleerde privacy-voorwaarden. De door bedrijven geboden keuzemogelijkheden lijken vooral ingegeven te zijn door marketing-overwegingen.[49] Daarnaast verzamelen bedrijven soms zoveel gegevens als maar mogelijk is, met als doel om nieuwe business modellen te exploreren. De dynamiek in de ontwikkeling van business modellen is zeer groot. Consumenten ontbreekt het daarom aan kennis van en zicht op de toekomst.[50] De gegevensverzameling gaat mogelijk verder dan wat strikt noodzakelijk is voor de betreffende dienstverlening, juist omdat data in de toekomst op nieuwe manieren te gelde gemaakt zouden kunnen worden. Individuen zijn zich niet bewust van de vergaande mogelijkheden en impact van data-analyse.[51] De correlaties die kunnen resulteren uit analyses met technieken voor *big data* maken het steeds moeilijker om te begrijpen hoe zij benadeeld kunnen worden.[52] Zoals Moerel en Prins (2016, p. 199) stellen:

> "De gedachte dat individuen in de huidige samenleving nog met voldoende kennis zorg kunnen dragen voor de bescherming van hun persoonsgegevens, is naïef. Kennis is niet langer een werkbaar instrument voor het realiseren van een geïnformeerde positie en daarmee de weg naar bewuste privacy-keuzes."

Privacy-overeenkomsten zijn dus te beschouwen als incomplete contracten. Zij geven consumenten slechts beperkt grip op de activiteiten die bedrijven met hun gegevens uitvoeren.

Vanuit een ruimer perspectief, dat ook big data omvat, en vanwege een argumentatie vergelijkbaar met de redenering zoals hierboven, zijn de publieke belangen van privacy voor beleidsmakers niet goed contracteerbaar. Zeno-Zencovich en Codiglione (2016, p. 57) stellen:

---

[47] Carolan (2016).

[48] Hoofnagle (2016).

[49] Shostack en Syverson (2004).

[50] Moerel en Prins (2016, p. 119) wijzen op de kennisachterstand bij burgers en consumenten, en niet zozeer op het onvermogen om toekomstige ontwikkelingen te kunnen anticiperen. Dat laatste zou men onder de kennisachterstand kunnen scharen.

[51] Mantelero (2016).

[52] Ohm (2014), geciteerd in Regan (2015, p. 64).

> "Big data are not a destination but a transit point towards what appears to be still a *terra incognita* in the development of societies increasingly influenced, at all their levels, by digital technologies."

Het niet kunnen anticiperen op technologische ontwikkelingen en business modellen maakt dat wet- en regelgeving er slechts in beperkte mate grip op kunnen krijgen. In die zin zijn de publieke belangen van privacy niet contracteerbaar. De volgende paragraaf verkent de beleidsimplicaties van deze observatie.

6. Implicaties voor overheidsinterventie

Privacy laat zich moeilijk in harde afspraken vastleggen. Consumenten hebben noch inzicht noch reële keuzemogelijkheden, laat staan dat zij op de toekomstige gevolgen van hun (vaak onbewuste) keuzes kunnen anticiperen. Wet- en regelgeving kan evenmin voorzien wat technologische ontwikkelingen gaan brengen. Privacy, evenals het publieke belang ervan, is daarom beperkt contracteerbaar. Deze paragraaf verkent de beleidsimplicaties van deze observatie.

6.1 Impact van risico's op onvoorziene situaties

Een eenvoudig voorbeeld. Een autoverzekeraar voorziet auto's van een zwarte doos om het rijgedrag van verzekerden te volgen. Hij belooft hen een premiekorting bij goed rijgedrag. We zullen zien dat het in geval van een incompleet contract moeilijk is om zo'n verzekering succesvol in de markt te zetten, ook al hebben alle partijen daar in beginsel baat bij. De redenering is als volgt. Stel dat de verzekeraar, door voortschrijdende analysemethoden, op een gegeven moment uit het rijgedrag kan afleiden dat een verzekerd individu een gezondheidsaandoening heeft die de lichamelijke motoriek aantast en daardoor extra risico loopt. Wat te doen? De verzekerde had niet verwacht dat de zwarte doos, naast rijgedrag, ook heel andere informatie zou kunnen blootleggen. De verzekeringsvoorwaarden voorzagen daar niet expliciet in, maar de verzekeraar is, op basis van algemene bepalingen in de voorwaarden, van mening dat hij het bestaande contract mag openbreken om de premie te verhogen. Overstappen naar een andere verzekeraar gaat, in een wereld waar verzekeraars beseffen dat concurrenten ondertussen meer weten dan de schadegeschiedenis, mogelijk gepaard met een medische toets en zou tot premieverhoging kunnen leiden. Er is een *hold-up* probleem: verzekeraar en verzekerde zitten aan elkaar vast terwijl de initiële afspraken niet meer toereikend zijn. Zij moeten nu gaan heronderhandelen. Ex ante, ofwel vóór het aangaan van een verzekering, deelden zij het belang van een verzekering op maat. Ex post, ofwel nadat de verzekering is afgesloten, komen de vruchten daarvan op het spel te staan. Wanneer partijen dat risico voorzien, maar daar van tevoren geen harde afspraak over kunnen maken, vallen zij vermoedelijk terug op een verzekering zonder zwarte doos. Dat leidt tot een welvaartsverlies, omdat beide partijen baat kunnen hebben bij een verzekering met monitoring van rijgedrag.

In bovenstaand voorbeeld lag de niet-contracteerbaarheid in het aan de oppervlakte komen van nieuwe, persoonlijke informatie, die de betrokkene liever niet ontsloten had zien worden. De niet-contracteerbaarheid kan ook liggen in het ontdekken van nieuwe verdienmodellen door een bedrijf. Stel dat de verzekerde en verzekeraar afspraken maken over de verzameling van persoonsgegevens. Wanneer de privacy-overeenkomst een compleet

contract is, kunnen zij vooraf afspreken wat te doen wanneer het bedrijf later een nieuwe toepassing bedenkt om de data te gelde te maken. De overeenkomst kan bijvoorbeeld specificeren dat de consument dan een extra vergoeding krijgt. Dat is anders wanneer een contract incompleet is. Stel dat de verzekeraar, met behulp van voortschrijdende technieken, een business model ontwerpt met een andere insteek dan het oorspronkelijke verdienmodel, dat hij naast de autoverzekering in de markt kan zetten. Er zijn dan verschillende situaties denkbaar, zoals de volgende:

- Het is onduidelijk of het nieuwe business model wel of niet onder de bepalingen van de originele overeenkomst valt. Een rechter is mogelijk niet in staat om daar een uitspraak over te doen. De klant zou willen heronderhandelen over een extra vergoeding, maar de benodigde inspanning weegt niet op tegen de onzekerheid of deze resultaat heeft.
- Het bedrijf brengt de nieuwe activiteit onder in een andere, buitenlandse entiteit. Dit ontgaat de afnemer. Deze weet wel dat een dergelijke situatie op zou kunnen treden, maar kan niet voorzien op welke wijze en realiseert zich dat hij daar machteloos tegenover staat.

In beide situaties kan de verzekerde huiverig worden om de dienst optimaal te benutten, of om überhaupt zo'n verzekering af te sluiten, terwijl de kwaliteit ervan afhangt van de verstrekte persoonsgegevens. Net als in het eerdere voorbeeld 'onderinvesteren' partijen in hun relatie — een bekende inefficiëntie in situaties met incomplete contracten. In een algemenere context van een digitale dienst haalt een consument dan niet alles eruit wat erin zit. Dat resulteert in een waardeverlies.

6.2 Oplossingsrichting

In Nederland geeft — vooralsnog — de Wet bescherming persoonsgegevens (Wbp) invulling aan de Europese Data Protectie Richtlijn. De Wbp gaat primair uit van het doel waarvoor gegevens gebruikt worden. Partijen mogen verder niet meer gegevens verwerken dan noodzakelijk is voor het gestelde doel. Het belang ervan speelt in mindere mate een rol.[53]

De beoordeling van het doel waarvoor gegevens zijn verzameld gebeurt momenteel aan de hand van de volgende criteria:[54]

1. *Doelspecificatie:* worden de gegevens alleen voor specifieke en rechtmatige doelen verzameld en verwerkt?
2. *Verenigbaar gebruik:* worden de gegevens niet verder verwerkt wanneer dat onverenigbaar is met deze doelen?

[53] Moerel en Prins (2016).

[54] Moerel en Prins (2016).

Vanaf 25 mei 2018 komt de Algemene Verordening Gegevensbescherming (AVG) in de plaats van de Wbp.[55] [56] Deze verordening bepaalt de rechten van individuen en de plichten voor partijen die persoonsgegevens (alle tot een persoon herleidbare gegevens) verwerken. Het principe in de Wpb dat mensen geïnformeerd worden over welke persoonsgegevens worden verzameld en verwerkt, wat daarmee gebeurt en wat het doel daarvan is, blijft overeind staan met de Verordening. Verder kent Nederland al de Wet Meldplicht Datalekken, die vergelijkbare bepalingen kent als de AVG. De Verordening versterkt de bestaande uitgangspunten: zij stelt scherpere eisen aan organisaties die gegevens verzamelen en geeft burgers meer zeggenschap over hun gegevens. Het doel is om meer bescherming te bieden. Zo krijgen bedrijven die gegevens verwerken bijvoorbeeld een grotere verantwoordelijkheid en verantwoordingsplicht. Consumenten krijgen, onder meer, gemakkelijker toegang tot hun persoonsgegevens en hebben de vrijheid om deze over te dragen aan een andere dienstverlener.

In het digitale domein kan men van consumenten echter niet verwachten dat zij kunnen voorzien aan welke privacy-risico's zij bloot (komen te) staan, zoals uiteengezet in paragraaf 5. Als zij al zouden bemerken dat heronderhandelen aan de orde zou zijn, bijvoorbeeld doordat een leverancier op een nieuwe mogelijkheid is gestuit om gebruikersgegevens te gelde te maken, zijn zij niet in staat om een vuist te maken tegen een groot bedrijf. Het valt daarom te rechtvaardigen dat de overheid voor een grensstellend kader zorgt dat burgers beschermt tegen zowel voorziene als onvoorzienbare effecten van innovatie in dataverwerking.[57] De wetgever dient zich er daarbij bewust van te zijn dat zij, in de dynamiek van digitale markten, continu achter de ontwikkelingen aanloopt.

Vanuit een economisch perspectief ligt de oplossingsrichting voor problemen van niet-contracteerbaarheid in het streven naar efficiëntie, ofwel in het voorkomen van een verlies aan potentieel te realiseren waarde.[58] In situaties waar een contract niet in voorziet, is het wenselijk dat de betrokken partijen naar het gezamenlijke belang — de gezamenlijk te realiseren waarde — kijken. Wanneer zij daar niet uitkomen, zou de partij met de sterkste prikkel om het gezamenlijk belang te dienen, zeggenschap dienen te hebben. Het is echter

---

[55] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). Zie de factsheets over deze hervorming op http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404.

[56] Een verordening introduceert direct recht in lidstaten, met dezelfde kracht als het nationale recht.

[57] Moerel en Prins (2016, p. 112).

[58] Dat perspectief dient in de context van privacy voldoende ruim te zijn, zodat ook de waarde voor de maatschappij in beeld is. Wanneer een dataverwerker een gerechtvaardigd belang-toets uitvoert, zal hij de impact op de samenleving moeilijk kunnen duiden. Individuele bedrijven kunnen de bredere maatschappelijke belangen, die vaak op een langere termijn tot uiting komen, niet goed inschatten. Moerel en Prins (2016) stellen daarom dat de overheid een referentiepunt voor het belang van privacy in het digitale domein dient aan te reiken.

lastig om, in de context van privacy in een relatie tussen bedrijf en afnemers, vorm te geven aan deze voorwaarde. Men kan van burgers niet verwachten dat zij voldoende verantwoordelijkheid kunnen dragen voor de handhaving van gegevensbescherming en de borging van privacy.[59] Bij privacy-inbreuken zijn zij meestal niet in staat om in kaart te brengen wie verantwoordelijk was en wat de schade is.

Voor traditionele goederen en diensten kan de oplossing in de allocatie van eigendomsrechten liggen. Deze geven in onvoorziene situaties zeggenschap om knopen door te hakken. Denk aan een aannemer die zijn eigen huis verbouwt: bij onaangename verrassingen zal hij, als eigenaar, niet moeilijk doen over extra werkzaamheden (wat anders ligt als hij het huis van een ander verbouwt). In consumentenmarkten zijn de allocatie van eigendom en zeggenschap helaas geen realistische opties.

Een oplossingsrichting met betrekking tot privacy ligt in een wettelijke aansprakelijkheid bij de partij die het beste in staat is om welvaartsverliezen door onvoorzien misbruik en in *holdup* problemen te voorkomen, met name in geval van een onevenwichtige machtsverhouding bij heronderhandelingen.[60] Die partij is logischerwijs (zie de bespreking in de eerdere paragrafen) de aanbieder van de dienst. Ook wanneer afnemers expliciet toestemming hebben gegeven voor gegevensgebruik en een privacy-overeenkomst een aanbieder vrijwaart van schade, zou aansprakelijkheid voorrang moeten krijgen. Het onderliggende idee is om het afwentelen van negatieve externe effecten te ontmoedigen. Dat gebeurt door het 'internaliseren' van het externe effect, ofwel door aanbieders de kosten van dat afwentelen te laten dragen (terwijl zij anders baten zouden incasseren).[61]

Aansprakelijkheid voor aanbieders van digitale diensten ondersteunt de bescherming van de maatschappelijke belangen van privacy. Individuele burgers hebben dat grotere belang niet goed op het netvlies en ervaren, bij een inbreuk, in eerste instantie alleen een individuele impact. Bedrijven zullen een voldoende sterke prikkel moeten ervaren om in het maatschappelijk belang te handelen. Een substantiële wettelijke aansprakelijkheid kan dat ondersteunen, opdat bedrijven, bij dataverwerking en innovatie in gegevensgebruik, rekening houden met maatschappelijke consequenties.

Een bijkomend voordeel van aansprakelijkheid voor gegevensverwerkers is dat consumenten, bij transacties waarbij persoonsgegevens verzameld worden, minder te vrezen hebben van onvoorzienbare datatoepassingen waarvan zij zowel de kans op, als de kosten en baten, niet kunnen inschatten en verdisconteren. Aansprakelijkheidsregels kunnen de

[59] Moerel en Prins (2016, p. 114).

[60] Kaplow en Shavell (1996).

[61] Zie Van Eeten (2011) voor een toepassing van deze redenering binnen de context van cybersecurity.

inefficiëntie door gebrekkige contracteerbaarheid en de daaruit voortvloeiende negatieve externe effecten mitigeren.

Privacyregels geven al invulling aan aansprakelijkheid. Onder de Wbp is een organisatie die persoonsgegevens verwerkt of laat verwerken aansprakelijk voor schade door overtredingen. Bij het inhuren van een extern bedrijf voor gegevensverwerking is er dus sprake van ketenaansprakelijkheid. Dit blijft zo onder de AVG, die verder reikt dan de Richtlijn die eraan vooraf ging.[62] [63]

Een eigenaar van een website die een advertentievenster verhuurt aan advertentienetwerken die privacyregels schenden, zou zich niet moeten kunnen verschuilen achter het feit dat hij daar niet over gaat. Dat is vergelijkbaar met een warenhuis dat ruimte verhuurt aan 'shop-in-shops'. Ketenaansprakelijkheid kan een prikkel geven om ketenverantwoordelijkheid in te vullen. Dat houdt in dat marktpartijen elkaar informeren en afspraken maken over de doorgifte van data.[64] De partij die in directe relatie met consumenten staat, heeft dan een zorg- en verantwoordingsplicht.

Het is nog een open vraag in welke mate de aansprakelijkheid, zoals opgenomen in de AVG, voldoende *bite* zal hebben om consumenten te beschermen tegen privacy-inbreuken met een impact die verder gaat dan de omvang van markttransacties. De AVG (Art. 82) biedt de mogelijkheid van vergoeding van geleden schade, ook immaterieel, maar heeft minder oog voor collectieve belangen. Om aansprakelijkheid een effectieve invulling te geven, is de vraag hoe ver de aansprakelijkheid moet reiken: tot en met de individuele schade door inbreuk voor hun afnemers, of verder, rekening houdend met de impact op de maatschappij? Consumenten zijn mogelijk niet in staat om achteraf te onderhandelen over compensatie voor geleden schade. Dat is temeer het geval omdat sommige inbreuken op de privacy slecht waarneembaar zijn, of omdat mogelijke schade zich niet direct in haar volle omvang manifesteert. In het verlengde hiervan zouden compensatiebedragen simpelweg te laag kunnen zijn om dwingende prikkels aan bedrijven te geven.

De hoogte van vergoedingen zou misschien beter gericht kunnen worden op het bijsturen van uitkomsten dan op compensatie. Van Eeten (2011) wijst er, vanuit een efficiëntie-oogpunt en binnen de context van cybersecurity, op dat het corrigeren van prikkels voor marktspelers prioriteit dient te krijgen boven het vergoeden van daadwerkelijk geleden schade. Wanneer aansprakelijkheid voor schade bij betrokkenen onvoldoende sterke prikkels voor preventie geeft, kan de boetemogelijkheid bij inbreuken op de Verordening

[62] Van Alsenoy (2017).

[63] Het reikt buiten het kader van deze verkenning om dieper op de juridische aspecten in te gaan.

[64] Het onderliggende idee is vergelijkbaar met de handreiking voor digitale zorgplichten voor bedrijven, opgesteld door de Cyber Security Raad (2016). Deze is gericht op het vergroten van de veiligheid in de keten op basis van effectieve afwegingen en passende maatregelen op alle niveaus in de keten.

misschien soelaas bieden. De AVG (die hogere boetes mogelijk maakt) stelt dat boetes doeltreffend en afschrikwekkend moeten zijn, dus daar kan ruimte liggen. Moerel en Prins (2016, p. 115) opperen nog de mogelijkheid van *public interest litigation* (het strategisch procederen voor mensen- en burgerrechten, gericht op de behartiging van maatschappelijke belangen) als aanvulling op toezicht op naleving van de regelgeving. Uit de invulling van de AVG via rechtspraak en aanvullende nationale wetgeving zal (bijvoorbeeld) moeten blijken of de aansprakelijkheid voldoende stevig wordt, welke complementaire rol nationale wetgeving zal gaan spelen en hoe de AVG zich gaat verhouden tot de Europese regels voor eCommerce met betrekking tot aansprakelijkheid.[65]

Het sterker sturen op aansprakelijkheid sluit aan op de visie van Moerel en Prins (2016) dat toestemming en de contractuele relatie tussen partijen niet meer effectief zijn als zelfstandige grondslagen voor gegevensverwerking. Zij pleiten voor een beoordeling primair vanuit gerechtvaardigd belang, die verder kijkt dan de individuele belangen. Natuurlijk is een privacy-overeenkomst relevant om te beoordelen of er sprake is van een gerechtvaardigd belang, maar een procedurele benadering biedt vaak onvoldoende garanties voor gegevensbescherming: het is ondoenlijk om alle denkbare vormen van onbedoeld gegevensgebruik in een kader te vatten of met verantwoordingsplichten te voorkomen. Moerel en Prins (2016, p. 123) beargumenteren dat aansprakelijkheid voor schade van consumenten — ook vanuit het perspectief van het maatschappelijk belang — effectiever is dan het vooraf afspreken van een vergoeding voor gegevensgebruik.

Aansprakelijkheid alleen zal vermoedelijk niet afdoende zijn. In het digitale domein zijn de strengere verplichtingen voor transparantie en verantwoording nuttig vanwege de complementaire rol. Deze vereisten ondersteunen, als vorm van ex ante regulering, de verantwoordelijkheid van bedrijven om zorg te dragen voor privacy. Zo bevat de AVG verplichtingen voor risico-analyses en impact assessment voor compliance en voor het documenteren van dataverwerking.

In aanvulling hierop kan 'responsieve regulering', waarbij regelgeving en handhaving gevoed worden door opgedane empirie en ervaring, de effectiviteit en legitimiteit van deze vorm van interventie voeden.[66] Maatschappelijke ontwikkelingen geven dan stapsgewijze invulling aan beleid en regulering, en absorberen (idealiter) de eventualiteiten die in een eerder stadium nog niet voorzien werden. Recent riep het Rathenau Instituut al op tot een periodieke politieke discussie in de Eerste en Tweede Kamer, over de governance van maatschappelijke en ethische vraagstukken rondom digitalisering.[67] Verder riep de Expertgroep Big data en privacy (2016) op tot experimenteerruimte voor de ontwikkeling van nieuwe toepassingen

[65] Zie bijvoorbeeld Golla (2017), Keller (2017) en Metzger (2017).

[66] Moerel en Prins (2016).

[67] Kool e.a. (2017).

met nog onbekende mogelijkheden en datavereisten, in het licht van het spanningsveld door doelbinding.[68] Een flexibel kader voor regulering sluit aan bij de zoektocht van het duiden van het maatschappelijk belang van privacy. Dat kan eveneens helpen om dataverwerking niet 'dicht te reguleren'. Ten eerste zou dat innovatie door marktpartijen kunnen ondermijnen — al is het voor innovatieprikkels vermoedelijk het belangrijkste dat bedrijven duidelijkheid hebben (strenge maar eenvoudige regelgeving kan *regulatory uncertainty* beperken en zo innovatie ten goede komen). Ten tweede zouden Europese lidstaten te veel uit de pas kunnen gaan lopen met ontwikkelingen op andere continenten.

Een aansprakelijkheidsregime helpt consumenten overigens niet wanneer bedrijven eerder verzamelde data gebruiken om nieuwe verdienmodellen te ontwikkelen. Dan hoeft er namelijk geen directe schade voor consumenten te zijn. Vanuit een economisch perspectief hebben zij dan mogelijk wél te maken met opportuniteitskosten, welke bestaan uit het niet meedelen in nieuwe, additionele revenuen van het bedrijf. Een gebruikersovereenkomst kan dat, met instemming van consumenten, uitsluiten — maar zoals besproken zijn dergelijke overeenkomsten in beginsel al problematisch, sowieso vanwege de niet-contracteerbaarheid van de impact van technologische ontwikkelingen. Juristen zullen gemiste opbrengsten vermoedelijk niet als schade bestempelen, maar desalniettemin is het interessant om te verkennen of consumenten aanspraak zouden moeten kunnen maken op nieuwe winstbronnen, die niet onder een gespecificeerd doel vielen.

Een andere oplossingsrichting, ook in lijn met de economische theorie van incomplete contracten, zou kunnen liggen in eigendomsrechten met betrekking tot persoonlijke gegevens. Een mogelijk standpunt is dat de consument of burger altijd eigenaar blijft van zijn of haar persoonlijke gegevens en gedragsdata, ook al zijn deze verzameld door of overgedragen aan een bedrijf. Dat zou hun juridische positie weliswaar kunnen versterken, maar stelt hen nog niet in staat om daadwerkelijke zeggenschap uit te kunnen oefenen, bijvoorbeeld omdat privacy-inbreuken evengoed onopgemerkt kunnen blijven.[69] Dat neemt niet weg dat eigenaarschap van persoonlijke data in de toekomst belangrijker kan worden, bijvoorbeeld met de opkomst van nieuwe diensten en platformen. Aansprakelijkheidsregels zouden dan aangescherpt kunnen worden, omdat bedrijven die data verzamelen en verwerken dan een grotere verantwoordelijkheid (namelijk over andermans eigendom) zouden gaan dragen. De implicaties voor privacy daarvan laten zich nog niet uittekenen, gegeven dat deze ontwikkeling nog in de kinderschoenen staat.

---

[68] Zie ook "Verantwoord innoveren met big data", J.-H. Hoepman, *Het Financieele Dagblad* 15 oktober 2016.

[69] Een vergelijkbaar argument geldt voor het het versterken van gebruiksrechten als substituut voor eigendomsrechten. Tjong Tjin Tai (2016) betoogt dat zowel het bezit als gebruik van data nadere privaatrechtelijke erkenning nodig heeft. Verder bepleit hij een eigendomsrechtelijke benadering (mogelijk in afwijking van het traditionele eigendomsbegrip), in termen van bevoegdheden en rechten, van gedigitaliseerde informatie.

7. Opties voor cybersecurity

In het digitale domein is privacy nauw gerelateerd aan cybersecurity, omdat beide betrekking hebben op preventie van schade door verstoring, uitval of misbruik van ICT-systemen.[70] [71] Vanuit dat ruimere kader kan men een onderscheid maken tussen data- en privacyschendingen (het ongeautoriseerd verzamelen, ontsluiten of gebruiken van persoonlijke gegevens) en veiligheidsincidenten (zoals het hacken en platleggen van IT-systemen en digitale diefstal van intellectueel eigendom). Bij data- en privacyschendingen zijn het vaak bedrijven die, in een grijs gebied, maatschappelijk ongewenste activiteiten verrichten, maar in beginsel streven naar naleving van wet- en regelgeving. Wanneer regels te weinig grip geven op hun gedrag zodat het grijze gebied groot is, kan het helpen om hen aansprakelijk te maken voor schade, zoals besproken in de vorige paragraaf. Bij cybersecurity zijn er meestal externe actoren in het spel — kwaadwillenden zonder boodschap aan wet- en regelgeving — waar goedwillende bedrijven en consumenten slachtoffer van kunnen worden.

Net als bij privacy gaat cybersecurity ook gepaard met externe effecten. Bij systemen die een cruciale maatschappelijke rol vervullen, zoals het Kadaster en de Belastingdienst, is dat direct duidelijk.[72] In het commerciële domein heeft de maatschappij eveneens baat bij private inspanningen om de veiligheid van ICT te vergroten. Onze economie kan alleen goed functioneren wanneer burgers en bedrijven vertrouwen hebben in digitale infrastructuren. Verder zou men kunnen beargumenteren dat de inspanningen om de cybersecurity te borgen niet goed contracteerbaar zijn: bedrijven hebben, los van wet- en regelgeving, enige speelruimte om eigen keuzes te maken. Dat argument lijkt hier minder prominent, in vergelijking met de problematiek van privacy. Hoe dan ook, ook zonder dat laatste argument geldt, vanwege externe effecten, dat het zaak is om de prikkels van bedrijven en andere partijen op één lijn te krijgen met de maatschappelijke belangen.

Voortbordurend op bovenstaand onderscheid tussen risico's omtrent privacy en cybersecurity, zullen bedrijven zich met betrekking tot privacy genoodzaakt voelen om hun processen en IT-systeem zodanig in te richten dat de risico's op problematische datahandelingen beheersbaar worden.[73] Dat gebeurt binnen een context waarbij privacy-

---

[70] Cyber Security Raad (2015).

[71] Een veel gehoord argument is dat het vergroten van veiligheid onvermijdelijk gepaard gaat met een verlies aan privacy — een argument dat overigens bekritiseerd wordt, zie bijvoorbeeld Solove (2011) en Van Lieshout e.a. (2013). Dat betreft echter veiligheid in het algemeen, en niet specifiek cybersecurity.

[72] "Het Kadaster is een fundament van de samenleving, verwaarloos het niet", nrc.nl 15 februari 2017, https://www.nrc.nl/nieuws/2017/02/15/cyberkwetsbaarheid-het-kadaster-is-een-fundament-van-de-samenleving-verwaarloos-het-niet-6694115-a1546096.

[73] NIST (2014).

inbreuken kunnen plaatsvinden terwijl het systeem op zichzelf functioneert zoals beoogd. In geval van een inbreuk kan het systeem aangepast worden om de zorgvuldigheid van gegevensbewerking te vergroten. Risico-analyses richten zich daarom vooral op eigen datahandelingen. Bij cybersecurity ligt dat anders, omdat er sprake is van sabotage van het systeem door buitenstaanders. Dat blijft mogelijk onopgemerkt. Risico-analyses richten zich dan minder op de eigen processen en zorgvuldigheid, en meer op het weren van ongewenste invloeden van buitenaf. Waar in het geval van privacy de mogelijkheden van het vergroten van het inzicht van consumenten beperkt zijn, geldt voor cybersecurity dat bedrijven zich bewust dienen te zijn van de aard van de risico's, zodat zij adequate maatregelen kunnen nemen.[74] De overeenkomst met de privacy-problematiek is dat de primaire verantwoordelijkheid ook hier bij bedrijven ligt. Daar kan men, net als in de voorgaande analyse, (onder meer) prikkels aan koppelen via aansprakelijkheid,[75] zij het dat de onderliggende argumentatie en de maatvoering anders zijn. De beleidsimplicaties zullen daarom verschillen.

Van Eeten (2011) bespreekt vier beleidsopties gericht op het vergroten van de veiligheid rondom informatietechnologie: (i) ex ante veiligheidsregulering; (ii) ex post aansprakelijkheid; (iii) verplichte melding van incidenten en ondersteuning van gedupeerden; en (iv) aansprakelijkheid van intermediaire partijen zoals ISP's en financiële dienstverleners. De eerste optie, ex ante regulering, kwam al naar voren in de vorige paragraaf, als complementair instrument (naast aansprakelijkheid). De tweede optie, ex post aansprakelijkheid, werd eveneens in het voorgaande deel besproken, om de prikkels van bedrijven op één lijn met publieke belangen te krijgen. Zo pleit cybersecurity-expert Hyppönen ervoor om fabrikanten van apparatuur aansprakelijk te maken voor lage veiligheidsniveaus, zodat zij zich meer inspannen om de online-verbindingen te beveiligen.[76] In het geval van cybersecurity werkt dat mogelijk wel anders dan bij privacy. Van Eeten observeert dat strikte aansprakelijkheid voor bedrijven weinig zinvol lijkt. Incidenten vloeien immers voort uit crimineel gedrag door derden. Wellicht zou een lichte vorm van aansprakelijkheid, bijvoorbeeld met een vooraf bepaalde schadevergoeding bij specifieke incidenten, voldoende kunnen zijn om bedrijven aan te zetten om voldoende veiligheidsinspanningen te verrichten. De derde optie, meldplicht en ondersteuning van gedupeerden, is specifiek voor veiligheidsinbreuken: bedrijven mogen deze dan niet geheim houden, omdat de buitenwereld baat heeft bij openheid. De vierde optie, aansprakelijkheid van ISP's en financiële dienstverleners, rust op een efficiëntie-argument. Ook al zijn banken niet degene die frauderen met credit cards, en zijn ISP's niet degenen die botnets installeren,

---

[74] Zie bijvoorbeeld de aanbevelingen in Verhagen (2016).

[75] Zie bijvoorbeeld Kool e.a. (2017, p. 169).

[76] "'Maak fabrikanten van apparaten aansprakelijk voor cyberveiligheid'", interview met Mikko Hyppönen, nrc.nl 17 maart 2017, https://www.nrc.nl/nieuws/2017/03/17/maak-fabrikanten-aansprakelijk-7413124-a1550707.

zij verkeren wel bij uitstek in een positie om daar tegen op te treden, wat niet geldt voor consumenten en internetgebruikers.

Ofschoon de concrete beleidsimplicaties ten aanzien van privacy en cybersecurity zullen verschillen, zijn er, op een abstracter niveau, wel overeenkomsten. Bij beide thema's kan men, vanuit een economisch perspectief, beargumenteren dat marktpartijen voldoende prikkels dienen te hebben om hun gedrag te verbeteren. Wet- en regelgeving draagt daar aan bij, al kan een nadruk op compensatie van schade soms niet volstaan voor de preventie van ongewenst gedrag.

Samenvattend, ofschoon privacy en cybersecurity nauw aan elkaar gerelateerd zijn, zijn er andere mechanismen in het spel die de prikkels bepalen om te handelen in de geest van maatschappelijke belangen. Ook lijkt niet-contracteerbaarheid een belangrijker ingrediënt te zijn voor de problematiek van privacy dan voor cybersecurity. Immers, bij diensten waar privacy een rol speelt gaan betrokkenen bewust interacties aan en is het zinvol om na te denken over de beperkingen van de afspraken die zij kunnen maken, terwijl problemen van cybersecurity door buitenstaanders met kwade bedoelingen worden veroorzaakt.

8. Conclusie

Privacy is alomtegenwoordig en, vermoedelijk daardoor, moeilijk in een eenvoudige definitie te vangen. Ofschoon men bij privacy in het economische domein van marktinteracties vooral denkt aan het gebruik van persoonsgegevens voor commerciële doeleinden, zijn ook daar meer fundamentele aspecten relevant. Borging van privacy geeft bijvoorbeeld vrijheid tot zelfontplooiing. Een inbreuk op de privacy kan meer schade toebrengen dan de waarde van economische interacties suggereert.

Door privacy, bijvoorbeeld in de vorm van informatieprivacy, te bekijken vanuit markttransacties, geeft men veel — in het digitale domein al snel te veel — gewicht aan het vermogen van individuen om adequate afwegingen te maken. Ook onderschat zo'n benadering mogelijk het algemenere, maatschappelijk belang van privacy.

De impact van technologie op privacy leidt in toenemende mate tot het verschijnsel van onvoorziene gevolgen. Het wordt voor consumenten steeds moeilijker wordt om te voorzien wat bedrijven met hun data kunnen en zullen gaan doen. Dat impliceert een risico op onvoorzien en onopgemerkt gebruik of misbruik van persoonsgegevens. Beleidsmakers kunnen eveneens moeilijk anticiperen op technologische ontwikkelingen en de dynamiek van nieuwe business modellen. Privacy, evenals het publieke belang ervan, is daarom beperkt contracteerbaar. Dit aspect lijkt, vanuit een beleidsperspectief, belangrijker te zijn voor privacy dan voor cybersecurity.

Vooral bedrijven zullen een voldoende sterke prikkel moeten ervaren om in het maatschappelijk belang te handelen. Een substantiële wettelijke aansprakelijkheid kan dat ondersteunen, zodat bedrijven, bij dataverwerking en innovatie in gegevensgebruik, ervoor kiezen om rekening te houden met de belangen van consumenten en de maatschappelijke consequenties van privacyschendingen. Wanneer consumenten begrijpen dat bedrijven een sterke prikkel hebben om de privacy van hun afnemers te beschermen, zullen zij meer vertrouwen krijgen bij het verschaffen van persoonlijke gegevens. Dat is, omdat het interacties aanmoedigt waar consumenten anders huiverig voor zouden zijn, goed voor innovatie, en daarmee voor de creatie van waarde. Het welvaartsverlies van niet-contracteerbaarheid wordt daarmee verminderd. Dat effect kan misschien nog versterkt worden door het mogelijk te maken dat consumenten aanspraak kunnen maken op nieuwe winstbronnen, die niet onder een initieel gespecificeerd doel vielen (de 'schade' voor consumenten betreft dan een ex post *opportunity cost*). Het zou interessant zijn om dat idee nader te verkennen.

In welke mate de wettelijke aansprakelijkheid, zoals opgenomen in de AVG, effectief zal zijn om consumenten te beschermen is op dit moment nog een open vraag. Uit de invulling van de AVG via rechtspraak en aanvullende nationale wetgeving zal moeten blijken of de

aansprakelijkheid voldoende stevig wordt om de prikkels van bedrijven de goede kant op te richten.

Bij cybersecurity spelen er andere prikkels en risico's op marktfalen. Problemen met cybersecurity worden veroorzaakt door buitenstaanders met kwade bedoelingen. Dat leidt tot andere beleidsimplicaties, maar er zijn wel overeenkomsten. Net als bij privacy dienen marktpartijen voldoende prikkels te hebben voor maatschappelijk optimaal gedrag. Wet- en regelgeving dragen daar aan bij, al verschillen de implicaties met betrekking tot de mate van aansprakelijkheid die nodig is om prikkels op één lijn te krijgen met de publieke belangen.

Referenties

Acquisti, A., L. John en G. Loewenstein (2009), "What is privacy worth?", paper gepresenteerd op de *Twenty First Workshop on Information Systems and Economics* (WISE), 14-15 december 2009, Phoenix, AZ.

Acquisti, A. C. Taylor en L. Wagman (2016), "The Economics of Privacy", *Journal of Economic Literature* 54(2), p. 442-492.

Bijlsma, M. B. Straathof en G. Zwart (2014), "Kiezen voor privacy: Hoe de markt voor persoonsgegevens beter kan", CPB Policy Brief 2014/04, Centraal Planbureau.

Buttarelli, G. (2016), "Ethics at the Root of Privacy and as the Future of Data Protection", lezing Berkman Center for Internet and Society, Harvard University / MIT Internet Policy Initiative en MIT Media Lab, 19 april 2016.

Carolan, E. (2016), "The continuing problems with online consent under the EU's emerging data protection principles", *Computer Law & Security Review* 32, p. 462-473.

Cavoukian, A., (2009), "Privacy Externalities, Security Breach Noti cation and the Role of Independent Oversight", discussion paper, Eighth Workshop on the Economics of Information Security, University College, London, 24 juni.

Cyber Security Raad (2015), "Handreiking cybersecurity voor de bestuurder", Den Haag.

De Bijl, P.W.J. (2017), "Digital technology and public policy", ACM Academy Lecture, 21 februari, ACM, Den Haag.

Expertgroep Big data en privacy (2016), "Licht op de digitale schaduw: Verantwoord innoveren met big data", rapport aan de minister van Economische Zaken

Dorner, D. (1989), *The Logic of Failure: Why Things Go Wrong and What We Can Do To Make Them Right*, Metropolitan Books, New York (Engelse vertaling 1996).

Golla, S. (2017), "Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR", *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)* 8.

Hart, O. (1995), *Firms, Contracts, and Financial Structure*, Oxford University Press.

Hartshorne, J. (2010), "The Value of Privacy", *Journal of Media Law* 2(1), p. 67-84.

Healy, T. (2005), "The Unanticipated Consequences of Technology", Markkula Center for Applied Ethics, Santa Clara University. https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/the-unanticipated-consequences-of-technology/

Hoofnagle, C.J. (2016), "Alan Westin's Privacy Homo Economicus", presentatie, FTC PrivacyCon Conference, 14 januari.

Kaplow, L. en S. Shavell (1996), "Property rules versus liability rules: An economic analysis", *Harvard Law Review* 109, p. 715-790.

Keller, D. (2017), "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation", Stanford Law School Center for Internet and Society SSRN: https://ssrn.com/abstract=2914684.

King, N.J. en J. Forder (2016), "Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data", *Computer Law & Security Review* 32, p. 696-714.

Kool, L., J. Timmer, L. Royakkers en R. van Est (2017), "Opwaarderen: Borgen van publieke waarden in de digitale samenleving", Rathenau Instituut, Den Haag.

Koops, B-J., B. Clayton Newell, T. Timan, I. Škorvánek, T. Chokrevski en M. Galič (2016), "A Typology of Privacy", Tilburg Law School Research Paper No. 09/2016, te verschijnen in *University of Pennsylvania Journal of International Law*.

MacCarthy, M. (2011), "New Directions in Privacy: Disclosure, Unfairness and Externalities", *I/S* 6(3), p. 1-88.

Magi, T.J. (2011), "Fourteen Reasons Privacy Matters: A Multidiscipinary Review of Scholarly Literature", University of Vermont, University Libraries Faculty and Staff Publications, Paper 4.

Manes, S. (2000), "Full Disclosure: Private Lives? Not Ours!", *Computerworld*, 1 mei 2000. http://www.computerworld.com.au/article/20046/full_disclosure_private_lives_ours_/

Mantelero, A. (2016), "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law & Security Review* 32, p. 238-255.

Martijn, M. en D. Tokmetzis (2016), *Je hebt wél iets te verbergen: Over het levensbelang van privacy*, De Correspondent.

Maskin, E. (2002), "Incomplete Contracts: On indescribable contingencies and incomplete contracts", *European Economic Review* 46, p. 725-733.

Maskin, E. en J. Tirole (1999), "Unforeseen Contingencies and Incomplete Contracts", *Review of Economic Studies* 66, p. 83-114.

Metzger, A. (2017), "Data as Counter-Performance: What Rights and Duties do Parties Have?", *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)* 8.

Moore, A. (2008), "Defining Privacy", *Journal of Social Philosophy* 39(3), p. 411-428.

Moerel, L. en C. Prins (2016), "Privacy voor de homo digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things",

in: *Homo Digitalis*, Preadviezen 2016, Nederlandse Juristen-Vereniging, Wolters Kluwer, p. 9-124.

Nehf, J.P. (2003), "Recognizing the Societal Value in Information Privacy", *Washington Law Review* 78(1), p. 1-92.

NIST (2014), "Privacy Engineering Objectives and Risk Model — Discussion Deck: Objective-Based Design for Improving Privacy in Information Systems", Computer Security Division van het National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC.

Ohm, P. (2014), "Changing the Rules: General Principles for Data Use and Analysis," in" J. Lane, V. Stodden, S. Bender en H. Nissenbaum (red.), *Privacy, Big Data, and the Public Good*, Cambridge University Press, p. 96-111.

Parker, R.B. (1974), "A Definition of Privacy", *Rutgers Law Review* 27, p. 275-296.

Regan, P. (2002), "Privacy as a Common Good in the Digital World", *Information, Communication & Society* 5(3), p. 382-405.

Regan, P. (2015), "Privacy and the Common Good: Revisited", in: B. Roessler en D. Mokrosinska (red.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*, Cambridge University Press, p. 50-70.

Scott, R.E. en G.G. Triantis (2005), "Incomplete Contracts and the Theory of Contract Design", *Case Western Reserve Law Review* 56(1), p. 187-201.

Shostack, A. en P. Syverson (2004), "What price privacy? (and why identity theft is about neither identity nor theft)", in: L.J. Camp en S. Lewis (red.), *Economics of Information Security*, Kluwer Academic Publishers, p. 129-142.

Solove, D.J. (2006), "A Taxonomy of Privacy", *University of Pennsylvania Law Review* 154(3), p. 477-560.

Solove, D.J. (2011), *Nothing to Hide: The False Tradeoff between Privacy*, Yale University Press.

Syverson, P. (2003), "The Paradoxical Value of Privacy", Naval Research Laboratory, Washington, DC.

Teece, D. (2010), "Business Models, Business Strategy and Innovation", *Longe Range Planning* 43, p. 172-194.

Tjong Tjin Tai, E. (2016), "Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving", in: *Homo Digitalis*, Preadviezen 2016, Nederlandse Juristen-Vereniging, Wolters Kluwer, p. 241-306.

Turow, J., M. Hennessy en N. Draper (2016), "The Tradeoff Fallacy", presentatie, FTC PrivacyCon Conference, 14 januari.

Van Alsenoy, B. (2017), "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and E-Commerce Law* (*JIPITEC*) 7.

Van Eeten, M. (2011), "Gedijen bij onveiligheid: Afwegingen rond de risico's van informatietechnologie", in: D. Broeders, M.K.C. Cuijpers en J.E.J. Prins (red.), *De staat van informatie*, WRR / Amsterdam University Press, p. 133-163.

Van Lieshout, M., M. Friedewald, D. Wright en S. Gutwirth (2013), "Reconciling privacy and security", *Innovation: The European Journal of Social Science Research* 26(1-2), p. 119-132.

Verhagen, E. (2016), "De economische en maatschappelijke noodzaak van meer cybersecurity", rapport op verzoek van de Cyber Security Raad.

Warren, S. en L. Brandeis (1890), "The Right to Privacy," *Harvard Law Review* 4, p. 193-220.

Westin, A.F. (2003), "Social and Political Dimensions of Privacy", *Journal of Social Issues* 59(2), p. 431-453.

Zeno-Zencovich, V. en G.G. Codiglione (2016), "Ten legal perspectives on the 'Big Data Revolution' ", *Concorrenza E Mercato (Antitrust, Regulation, Consumer Welfare, Intellectual Property)* 26, p. 29-57.