Brassersplein 2
2612 CT Delft
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57
infodesk@tno.nl

TNO-rapport
2012 R10006

Stimulerende en remmende factoren van Privacy by Design in Nederland

Datum	1 mei 2012
Auteur(s)	Marc van Lieshout, Linda Kool, Gabriela Bodea, James Schlechter, Bas van Schoonhoven
Exemplaarnummer	
Oplage	
Aantal pagina's	116 (incl. bijlagen)
Aantal bijlagen	7
Opdrachtgever	Interne Kennisopbouw
Projectnaam	
Projectnummer	055.01073

Managementsamenvatting

Titel :	Stimulerende en remmende factoren van *Privacy by Design*
Auteur(s) :	Marc van Lieshout, Linda Kool, Gabriela Bodea, James Schlechter, Bas van Schoonhoven
Datum :	1 mei 2012
Opdrachtnr. :	Interne kennisopbouw
Rapportnr. :	TNO 2012 R10006

Persoonsgegevens en *Privacy by design*

Veel organisaties maken gebruik van persoonsgegevens van hun klanten voor een op maat toegesneden dienstverlening. Er is sprake van een trend: de hoeveelheid persoonsgegevens die in omloop is en de benutting van deze gegevens is de afgelopen jaren enorm gestegen. De commerciële belangen van de benutting van persoonsgegevens nemen daarmee eveneens toe. Voor consumenten biedt personalisering meerwaarde doordat diensten beter toegesneden zijn op persoonlijke voorkeuren en wensen. Met de toegenomen mogelijkheden om persoonsgegevens te verzamelen en te benutten wordt het voor bedrijven belangrijker om een goede afweging te maken tussen de benutting van deze gegevens en consumentenvertrouwen. Bij het opstellen van de bedrijfsstrategie zullen ontwikkeling van nieuwe diensten en afschermen van risico op misbruik van gegevens en aantasting van consumentenvertrouwen een grotere rol gaan spelen. Het belang van een goede omgang met deze gegevens neemt toe, al was het maar om negatieve incidenten en de daaraan gekoppelde (reputatie)schade voor te zijn. Maar mogelijk kunnen bedrijven zich ook positief profileren door te wijzen op een goede en vertrouwenwekkende omgang met aan hen toevertrouwde gegevens.
In een eerder stadium (1999) is al vanuit de overheid aandacht gevraagd voor instrumenten (*Privacy Enhancing Technologies*) die de overheid in kan zetten voor een goede bescherming van persoonsgegevens (motie Nicolai, Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 31). Deze motie had betrekking op overheidsinformatiesystemen. Problemen rond directe inpasbaarheid, onduidelijkheid van kosten en opbrengsten en gepercipieerde complexiteit van oplossingen belemmerden toen snelle invoering bij de overheid. Inmiddels is de benadering van gegevensbescherming verbreed en is ook de aandacht verbreed naar het bedrijfsleven.

Voor de bescherming van persoonsgegevens zijn verschillende instrumenten beschikbaar. Sommige van deze instrumenten zijn technisch van aard (zoals instrumenten om gegevens te versleutelen), andere instrumenten zijn organisatorisch van aard (zoals het uitvoeren van een *privacy audit*). De laatste tijd wordt veel verwezen naar *Privacy by Design* als methode om de privacy van personen over wie gegevens verzameld worden te beschermen, Een eenduidige definitie van *Privacy by Design* ontbreekt. In dit onderzoek spreken we van *Privacy by Design* wanneer

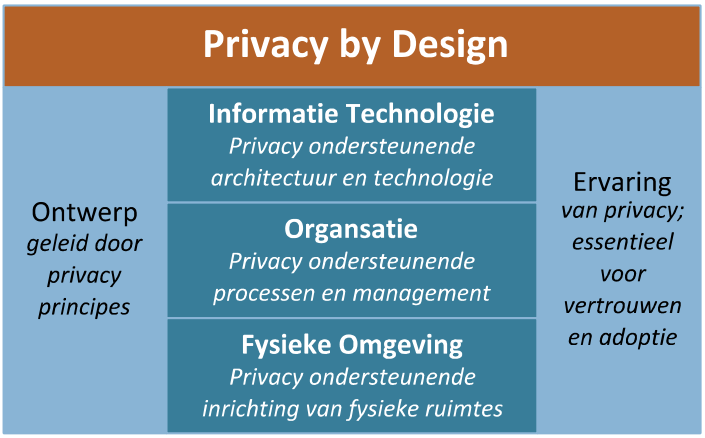
- de bescherming van de privacy van personen over wie gegevens verzameld worden (bijvoorbeeld consumenten) al bij het (vroegste) ontwerp van een systeem wordt meegenomen,

- er gebruik wordt gemaakt van organisatorische maatregelen om toegang tot en omgang met persoonsgegevens te regelen volgens bepaalde afspraken en voorschriften en
- er gebruik wordt gemaakt van technische maatregelen zoals versleuteling om toegang tot en omgang met persoonsgegevens af te schermen of te verhinderen.

In figuur 1 zijn de bouwstenen gegeven die onderdelen vormen van *Privacy by Design*. We maken onderscheid tussen instrumenten voor de ontwerpfase (zoals een *Privacy Impact Assessment* en een ontwerpmethode waarin privacy is opgenomen), technische instrumenten (zoals versleuteling en instrumenten om de transparantie van de gegevensverwerking te vergroten), organisatorische instrumenten (zoals het aanstellen van een *Privacy Officer* en het maken van afspraken over toegang en gebruik van gegevens), ontwerpfactoren voor de ruimtelijke dimensie (zoals de ruimtelijke scheiding van gegevensregistratie en gegevensgebruik) en de ervaring van privacy die de personen over wie gegevens verzameld worden zelf hebben. In het onderzoek hebben we de volgende definitie van *Privacy by Design* gebruikt:

“Privacy by Design heeft als doel privacyschendingen zoveel mogelijk te vermijden door privacybescherming vanaf het begin van een (business)proces waar verzameling en verwerking van persoonsgegevens onderdeel van uitmaakt en tijdens de gehele levenscyclus van de gegevensverwerking systematisch ‘in te bakken’ in de organisatie en in de informatiesystemen die gebruikt worden. Het gaat bij *Privacy by Design* niet alleen om technische maatregelen maar ook om maatregelen in de bedrijfsvoering en de organisatie en om inbreng van de ervaring en houding van eindgebruikers (consumenten).”

Figuur 1: Bouwstenen voor *Privacy by Design*



Naast deze opdeling in bouwstenen zijn twee belangrijke functionaliteiten van *Privacy by Design* te onderscheiden: *privacy governance* en *privacy protection*. Ieder van deze functionaliteiten is te benaderen vanuit twee dimensies: een organisatorische en een technische. *Privacy governance* richt zich op het realiseren van een (organisatie-)beleid rond privacy waarbij verantwoordelijkheid en transparantie centraal staan in de verzameling, bewerking, verspreiding, opslag en vernietiging van persoonsgegevens. Startpunt hierbij is het betrekken van privacy-overwegingen bij het initiëren van nieuwe diensten en nieuwe organisatie-

activiteiten. *Privacy protection* richt zich op afscherming, versleuteling, anonimisering en minimalisering van persoonsgegevens die worden verzameld, bewerkt, etc. De organisatorische dimensie richt zich op processen en methoden die een organisatie kan invoeren voor *privacy governance* en voor *privacy protection*. Dit is bijvoorbeeld het instellen van auditprocedures, het aanstellen van *Privacy Officers* met bepaalde taken en verantwoordelijkheden, en het opstellen van regels en richtlijnen rond een Privacy Impact Assessment. De technische dimensie richt zich op tools en methoden die ingezet kunnen worden voor de technische realisering van *privacy governance* en *privacy protection*. Dit is bijvoorbeeld het gebruiken van protocollen en procedures van dataminimalisering, of het inzetten van cryptografische technieken voor anonimisering van gegevens.

Tabel 1: Dimensies en functionaliteiten van *Privacy by Design*

	Transparantie **Privacy governance** **'Privacy by policy'**	**Afscherming** **Privacybescherming** **'Privacy by Architecture'**
Organisatorisch	Privacy standaardelement in initiatiefase van nieuwe diensten Audits Privacy officers …	Toegang via pseudoniemen Access management …
Technologisch	Log files Data base audit interfaces Transparantietools …	Anonimisering Zero knowledge proofs Client side gegevensverwerking …

Het onderzoek

TNO richt zich in zijn onderzoeksprogramma op de verkenning en ontwikkeling van *Privacy by Design.* Eén van de vragen die TNO bezighoudt is wat stimulerende en remmende factoren zijn voor de toepassing van *Privacy by Design.* Het antwoord op deze vraag vergroot de kennis over de mogelijkheden en de problemen die organisaties ervaren als ze (een aspect van) *Privacy by Design* zouden willen invoeren. Dit kan richting geven bij het zoeken naar (innovatieve) oplossingen voor *Privacy by Design*.

In het kader van zijn eigen kennisontwikkeling heeft TNO onderzocht welke stimulerende en remmende factoren bedrijven ervaren als ze (een aspect van) *Privacy by Design* in willen voeren. De vraagstelling had drie elementen:

1. verkenning van stimulerende en remmende factoren,
2. duiding van de stimulerende en remmende factoren aan de hand van een model dat aangeeft welke soorten problemen op kunnen treden bij invoering van een innovatie, en
3. aan de hand van dit model onderzoek naar welke interventiestrategieën de overheid zou kunnen inzetten, om – indien gewenst – bepaalde problemen aan te pakken.

Oorspronkelijk was het doel om informatie te verzamelen door een brede survey onder Nederlandse bedrijven uit te voeren. Dit bleek in de praktijk niet haalbaar omdat de bereidheid om mee te werken bij bedrijven te gering bleek. Bedrijven ervoeren de survey als teveel gericht op compliance en te weinig op onderzoek

naar remmende en stimulerende factoren. Het onderzoek is vervolgens bijgesteld tot een verkenning naar de stimulerende en remmende factoren die 'voorlopende' bedrijven ervaren. Dit betekent dat de resultaten van het onderzoek niet representatief zijn voor het Nederlandse bedrijfsleven, maar een exploratief beeld geven van het deel daarvan wat op het gebied van het betrekken van privacy in de bedrijfsactiviteiten 'voorloper' is. De resultaten uit de in totaal 29 interviews zijn onderling consistent en vertonen een sterke overeenstemming met andere studies zoals de studie uit 2010 van London Economics over *Privacy Enhancing Technologies*.

Het begrip 'voorloper' duidt hier op bedrijven die een vorm van *Privacy by* Design in hun bedrijfsvoering hebben opgenomen en op bedrijven die *Privacy by Design* als onderdeel van hun productportfolio aanbieden. De term is afkomstig uit de innovatietheorie. De benadering van *Privacy by Design* als een innovatie bood een conceptueel kader waarbinnen stimulerende en remmende factoren geïdentificeerd konden worden. Hoewel de termen 'innovatie' en 'voorloper' kunnen suggereren dat (volledige) acceptatie van een innovatie de norm is en het een kwestie is van wachten tot de 'achterblijvers' dit ook inzien, is dit niet de insteek van het onderzoek. Of een vernieuwing aanslaat hangt van veel factoren af. Het ging in dit onderzoek om de identificatie van die factoren.

Conclusies remmende en stimulerende factoren

De hoofdconclusie van het onderzoek is dat er duidelijk meer remmende dan stimulerende factoren aanwezig zijn voor de invoering en toepassing van *Privacy by Design.* Deze factoren zijn op alle niveaus aanwezig: met betrekking tot de innovatie zelf, met betrekking tot de bereidheid en de mogelijkheden van organisaties om *Privacy by Design* in te voeren en toe te passen en met betrekking tot de invloed van de omgeving op invoering en toepassing.

Met betrekking tot de **innovatie** zelf zijn de volgende conclusies te trekken:

1. Het begrip *Privacy by Design* kent **geen eenduidige definitie**. Wel onderschrijven de meeste bedrijven de hierboven gegeven beschrijving van *Privacy by Design.* De verschillende onderdelen van *Privacy by Design* komen bij verschillende bedrijven in verschillende mate voor, maar bij alle voorlopers is de combinatie van maatregelen (technisch en organisatorisch, afscherming en transparantie) herkenbaar.
2. Invoering en toepassing van *Privacy by Design* heeft een – beperkt – positief effect op de bedrijfsvoering, maar de negatieve effecten overheersen volgens de geïnterviewden (*performance expectancy*). Wat betreft de moeite die het kost om *Privacy by Design* toe te passen (de *effort expectancy)* hangt een en ander sterk af van de context van invoering. We werken beide conclusies hieronder verder uit.
3. Veel indicatoren rond *performance expectancy* vallen negatief uit of zijn slechts bescheiden positief. Dit laatste geldt voor het **relatieve voordeel** dat invoering en toepassing van PbD een onderneming kan bieden. Bedrijven die bestaan van dienstverlening op basis van persoonsgegevens beschouwen privacy als een onderdeel van de bedrijfsstrategie, en hebben de indruk dat toepassing van *Privacy by Design* concurrentievoordeel kan bieden. Bedrijven die vooral ter ondersteuning van hun primaire processen veel persoonsgegevens verwerken beschouwen *Privacy by Design* vooral

als een *commodity*, waarvan men de indruk heeft dat toepassing geen concurrentievoordeel biedt.

4. Het effect van *Privacy by Design* op de **efficiëntie en effectiviteit van bedrijfsprocessen** zien de bedrijven als (licht) negatief. Het effect is overigens soms zo gering dat de geïnterviewde bedrijven het niet als belastend ervaren en het geen extra rem zet op de beslissing om *Privacy by Design* al dan niet toe te passen.
5. De bijdrage van *Privacy by Design aan* **het verkleinen van het risico op privacy-incidenten** ervaren de geïnterviewden als positief. Ook helpt *Privacy by Design* bedrijven om aan te tonen dat ze de juiste beveiligingsmaatregelen hebben getroffen en op de juiste manier omgaan met persoonsgegevens (*accountability)*. Dit heeft een **positief effect op de bedrijfsvoering** en dit kan ook **kostenbesparend** werken. De omvang van deze kostenbesparing is echter moeilijk te kwantificeren; hier zijn ook weinig betrouwbare gegevens over beschikbaar.
6. Met betrekking tot de **kosten** geven de bedrijven aan dat de kosten aan de technische kant in de regel bescheiden zijn ten opzichte van de kosten aan de organisatorische kant. De organisatorische kosten kunnen fors zijn vanwege personele consequenties en vanwege aanpassingen in de (primaire) bedrijfsprocessen. Wat betreft de kosten aan de technische kant hangt het sterk af of het gaat om invoering en toepassing in een bestaand of in een nieuw te ontwikkelen systeem. Bij toepassing op een bestaand systeem zijn de kosten relatief hoog. Dit is het ***legacy*probleem**. Bij toepassing in een nieuw te ontwikkelen systeem zijn de kosten aanzienlijk lager. De geïnterviewden hadden geen kennis over de precieze omvang van de kosten.
7. De geïnterviewden ervaren de **wetgeving als complex.** Voor veel bedrijven is het lastig om te weten waar ze precies aan moeten voldoen. De bestaande wetgeving laat daarbij ruimte voor interpretatie, waarbij het niet altijd duidelijk is welke interpretatie wenselijk is.
8. *Privacy by Design* is **geen 'plug and play'** innovatie maar heeft impact op bedrijfsprocessen, de cultuur binnen de organisatie, de verdeling van rollen en verantwoordelijkheden en soms ook op wat na invoering wel of niet meer mogelijk is (dienstverlening).

Met betrekking tot de **kenmerken van de organisatie** waarin de innovatie plaatsvindt zijn de volgende conclusies te trekken:

1. Aanbieders van systeemoplossingen missen bij hun klanten een duidelijke vraag naar producten voor privacybescherming. De geïnterviewde dataverwerkers missen actief meedenkende aanbieders. Er is geen duidelijke vraagarticulatie. Hier lijkt dus sprake te zijn van een "kip of ei" probleem: zonder vraag geen aanbod, en vice versa. De geïnterviewden geven aan dat zij denken dat de verschillen tussen de 'voorlopers' en de andere bedrijven waar het gaat om **kennis en bewustzijn** rond *Privacy by Design* groot zijn.
2. **Het bewustzijn van het belang van het voorkómen van privacyschendingen** (en daarmee reputatieschade) is wel gegroeid; dit leidt evenwel niet tot een duidelijke vraag naar *Privacy by Design.*

3. Een organisatie die *Privacy by design* wil invoeren heeft **medewerking van het topmanagement** nodig om dit te realiseren. Leiderschap dat uitstraalt dat privacybescherming belangrijk is voor de organisatie is noodzakelijk.
4. **De omvang van de organisatie** speelt op verschillende manieren een rol. Kleine organisaties geven aan moeite te hebben om de benodigde vaardigheden en kennis in huis te halen. Het legt snel een te groot beslag op de beschikbare middelen. Grote organisaties die in meer landen actief zijn, ervaren verschillen in cultuur binnen de organisatie als probleem. Daarnaast hebben ze last van de verschillende uitwerkingen van de Europese richtlijn rond privacy en gegevensbescherming in nationale wet- en regelgeving. Dit voorkomt dat er *economies of scale* en *economies of scope* ontstaan bij invoering en toepassing van *Privacy by Design*.
5. **Organisaties die veel persoonsgegevens verwerken**, als onderdeel van hun kernactiviteiten hebben meer oog voor privacybeschermende maatregelen dan organisaties bij wie de bewerking van persoonsgegevens secundair is.

Met betrekking tot de invloed van de **externe omgeving** zijn de volgende conclusies te trekken:

1. **De kennis over en de uitwerking van praktische oplossingen** voor *Privacy by Design* is voldoende hoog. Afnemers van systeemoplossingen hebben zelf de kennis in huis en vaak ook de technische kennis om een en ander op de juiste manier te implementeren. Ze ervaren geen gebrek in aanbod aan de kant van de systeemleveranciers. Wel ervaren de afnemers een gebrek aan pro-activiteit aan de kant van de aanbieders. Overigens geldt deze conclusie voor de ‘voorlopers’. De ‘voorlopers’ geven zelf aan dat ze verwachten dat de kennis bij andere afnemers gering of afwezig zal zijn
2. De ‘voorlopers’ **missen een onafhankelijk en op bedrijven gericht platform dat informeert** over beste aanpakken en dat ervaringen over invoering en toepassing van *Privacy by Design* kan delen. Daar hoort ook informatie over de interpretatie van het wettelijk kader bij en een uiteenzetting van professioneel opdrachtgeverschap rond privacyvraagstukken. .
3. Geïnterviewde bedrijven geven aan dat de **toezichthouder een geringe rol speelt** bij de beslissing van de organisatie om *Privacy by Design* toe te passen. De toezichthouder biedt weinig ondersteuning rond praktische aangelegenheden. Ook ervaren zij geen positieve prikkels vanuit de toezichthouder die het aantrekkelijk maken om in *Privacy by Design* te investeren.
4. **Het wettelijk kader** is een motief om naar *Privacy by Design* te kijken. De aangekondigde herziening van de Europese dataprotectierichtlijn leidt bij ‘voorlopers’ tot een aanscherping van hun privacybenadering.
5. De geïnterviewde bedrijven zien voordeel in **gestandaardiseerde en** – eventueel – **gecertificeerde oplossingen** die verduidelijken aan welke voorschriften voldaan moet worden.

6. **De vraag vanuit consumenten** om privacybeschermende maatregelen is gering. Wel merken bedrijven dat consumenten kritischer worden en privacybescherming belangrijker gaan vinden en geven aan dat dit in de toekomst mogelijk wel een grotere rol kan gaan spelen.

Uit de internationale vergelijking komen de volgende aanvullende inzichten:

1. De conclusies uit de nationale interviews worden door de internationaal geïnterviewden grotendeels bevestigd.
2. De invulling die in verschillende landen aan de toezichthouder gegeven wordt verschilt sterk. In enkele gevallen wordt het toezicht op privacywetgeving gecombineerd met het toezicht op informatierechten van burgers (in Nederland de Wet Openbaarheid Bestuur); in Nederland is dit niet het geval. Ook de focus van de toezichthouder verschilt sterk: in Nederland ligt deze op handhaving, waar bijvoorbeeld in Canada of het Verenigd Koninkrijk de toezichthouders sterk de nadruk leggen op ondersteuning.
3. In tegenstelling tot drie van de vijf landen die bestudeerd zijn (Canada, Verenigd Koninkrijk, Verenigde Staten) heeft Nederland geen algemene verplichtstelling van een Privacy Impact Assessment in de publieke sector. Wel volgt uit de Wbp de noodzaak van een privacyrisicoanalyse, in relatie tot het gevraagde passende beveiligingsniveau. Daarnaast kent de Wpb een 'voorafgaand onderzoek' dat eveneens als een PIA te interpreteren is. Bij aanvaarding van de EU Verordening over gegevensbescherming zal de PIA in de gehele EU verplicht worden. Overigens betreft het hier een voorstel. De uiteindelijke verordening kan (aanzienlijk) afwijken van dit voorstel. .

Belangrijkste stimulerende en remmende factoren

In Tabel 2 geven we een overzicht van de belangrijkste stimulerende en remmende factoren die we in de studie gevonden hebben op basis van desk research en de interviews.

Tabel 2: Belangrijkste stimulerende en remmende factoren voor invoering van *Privacy by Design*

Stimulerende factoren	Remmende factoren
Effectiviteit van PbD om privacyschendingen te verkleinen	Potentieel grote (organisatorische) impact op organisatie
Mogelijkheid om *accountability* zichtbaar te maken	Aanwezigheid van verouderde IT-systemen
Leiderschap dat positief tegenover *Privacy by Design* staat	Op elkaar wachtende partijen
	Gebrek aan bewustzijn over belang/noodzaak van privacybescherming en mogelijkheden van PbD
	Complexiteit van wetgeving
	Ontbreken stimulerende rol van de toezichthouder

De organisatie van de markt en het innovatiesysteem

Op basis van de verkregen inzichten in stimulerende en remmende factoren heeft TNO onderzocht hoe deze factoren begrepen kunnen worden als vormen van een imperfecte markt dan wel een niet goed functionerend innovatiesysteem. Van een imperfecte markt is sprake wanneer er factoren zijn die een normaal functioneren van de markt van vraag en aanbod belemmeren. Van een niet goed functionerend innovatiesysteem is sprake wanneer er factoren zijn die belemmerend doorwerken op relaties en interacties tussen partijen in een innovatiesysteem.

In tabel 2 staan de belangrijkste conclusies rond het optreden van imperfecties in de markt en het innovatiesysteem genoemd.

Tabel 3: Vormen van imperfecties bij invoering en toepassing van *Privacy by Design*

Imperfecties in de markt	Imperfecties in het innovatiesysteem
Positieve externaliteiten *Weinig aandacht voor maatschappelijke voordelen. Baten zijn lastig te kwantificeren.*	**Belemmeringen in infrastructurele voorzieningen en investeringen** *Niet gevonden*
Publieke goederen en toe-eigening *Niet gevonden*	**Lock-in en padafhankelijkheid** *Legacysystemen ervaren lock in en padafhankelijkheid. Dit belemmert adoptie van privacyvriendelijke alternatieven*
Informatie-asymmetrie *Niet gevonden*	**Institutionele belemmeringen** *Gebrek aan harmonisatie; complexe wetten; toezichthouder met beperkte beschikbaarheid en geringe ondersteuning*
Niet-effectieve marktwerking *Grote bedrijven zetten de toon met betrekking tot het belang van* Privacy by Design. *Dat maakt markttoetreding voor kleinere bedrijven met innovatieve aanpakken moeilijker.*	**Falende interacties** *Te weinig interactie tussen verschillende partijen. Gebrekkige informatie-uitwisseling over wensen, behoeften, oplossingen en best practices*
	Onvoldoende vaardigheden en kennis *Mogelijk probleem bij volgers*

1. **Positieve externaliteiten** wijzen op voordelen die een innovatie kan hebben maar die de innoverende partij niet kan verzilveren. Bij invoering van *Privacy by Design* is te signaleren dat de kosten gedragen worden door de innoverende partij terwijl de baten (versterking van de gegevensbescherming) toe kunnen vallen aan andere partijen waaronder de personen over wie gegevens verzameld worden. De voordelen voor de innoverende partij, zoals het voorkómen van ongewenste gegevensverspreiding, zijn moeilijk te kwantificeren Dit leidt ertoe dat een kosten-baten analyse voor *Privacy by Design* moeilijk is te maken.

2. Er is in zekere mate sprake van **niet-effectieve marktwerking** doordat vragende partijen (de dataverwerkers) meer verwachten van de aanbiedende partijen waar deze aanbieders (de systeemleveranciers) vanwege het ontbreken van voldoende (en voldoende gearticuleerde) vraag nog afwachtend zijn. Daarnaast vragen consumenten nauwelijks om privacybeschermende maatregelen. De grote dienstenaanbieders hebben weinig concrete interesse in *Privacy by Design* waardoor met name kleine(re) en innovatieve(re) bedrijven het moeilijker hebben om de markt te betreden.
3. De toepassing van *Privacy by Design* wordt niet gehinderd door een probleem dat de ene partij de technologie ontwikkelt en de ander deze kosteloos kan toepassen, als was het een publiek goed. Ook lijkt er geen sprake van verschillen in toegang tot en gebruik van informatie over *privacy by Design* (**informatie asymmetrie**).
4. Met betrekking tot de organisatie van relaties en interacties tussen partijen in het innovatiesysteem rond *Privacy by Design* is er geen probleem in kennisontwikkeling en spreiding van nieuwe resultaten. Er is geen aantoonbare noodzaak voor aanvullende onderzoeksprogramma's of investeringen in de onderzoeksinfrastructuur.
5. Er is sprake van **padafhankelijkheid en lock-in** doordat bedrijven niet zomaar van de ene op de andere dag op een ander systeem over kunnen stappen. Het is in de regel met name kostbaar om nieuwe privacy-beschermende technologieën in legacysystemen in te voeren.
6. Er is sprake van **institutionele belemmeringen** doordat het wettelijk kader rond privacy en gegevensbescherming complex is (complexe en niet-geharmoniseerde wetten en regelingen) en doordat de toezichthouder niet voldoende zichtbaar is in het stimuleren van *Privacy by Design.* Positieve prikkels ontbreken.
7. **Falende interacties** tussen aanbiedende en afnemende partijen (te weinig informatiedeling over behoeften, wensen, oplossingen en *best practices*) verhinderen een goed functionerend 'ecosysteem' rond Privacy by Design.
8. Tot slot constateren de voorlopende partijen een **kennis- en vaardigheden** probleem bij andere partijen dat belemmert om *Privacy by Design* in te voeren.

Aanbevelingen

De gesignaleerde imperfecties in het functioneren van de markt en het innovatiesysteem rondom *Privacy by Design* bieden de overheid de mogelijkheid om gericht te interveniëren. Of er voor de overheid voldoende reden is om ook daadwerkelijk actie te ondernemen, is geen onderdeel geweest van de studie. De mogelijke interventies komen voort uit een door TNO opgesteld afwegingskader, waarbij vooral aandacht is voor 'zachte maatregelen' die genomen kunnen worden om het speelveld rondom *Privacy by Design* verder vorm te geven.

Een aantal gesignaleerde imperfecties kan worden weggenomen door het instellen van een of meer **platforms** die kennis en ervaringen verenigen en beschikbaar stellen aan derden. Deze platforms hebben met name een informerende rol. Partijen die informatie willen over mogelijkheden om privacy (sterker) in de bedrijfsvoering op te nemen, hebben nu moeite om de juiste informatie te vinden.

Een platform kan aan deze behoefte voldoen. Aard en inbedding van het platform/de platforms staan open. Dit kan op verschillende manieren vorm krijgen: vanuit specifieke bedrijfsbranches, vanuit de toezichthouder, vanuit koepelorganisaties, vanuit onafhankelijke organisaties. Een platform zet verschillende belanghebbenden bij elkaar en versnelt het proces van kennisopbouw en kennisdeling. Belangrijke insteek van een platform is het bij elkaar brengen van verschillende perspectieven (juridisch, technologisch, organisatorisch). Door de aard van de privacyvraagstukken is de combinatie van deze perspectieven nodig om tot effectieve kennisopbouw te komen.

Aanvullend onderzoek naar positieve prikkels die uit *Privacy by Design* te halen zijn, kan bijdragen om meer inzicht te krijgen in de effecten van *Privacy by Design* op de bedrijfsmodellen. Nu overheerst het beeld dat privacy vooral een kostenpost is, terwijl de (maatschappelijke) baten aan anderen toevallen. Positieve prikkels zouden kunnen bestaan uit vrijwaring van bemoeienis als een organisatie aannemelijk kan maken een bepaald niveau van privacybescherming en risico-management rond persoonsgegevens te hebben gerealiseerd. Met het toenemende economisch belang van dienstverlening gebaseerd op persoonsgegevens wordt het ook belangrijker om een beter inzicht te verkrijgen in de positieve en negatieve (economische) effecten van toepassing van *Privacy by Design*. Ook is aanvullend onderzoek nodig naar de inpassing van privacy-oplossingen in bestaande systemen. Dit kan helpen om een beter inzicht te krijgen in mogelijke alternatieve aanpakken en in de doorrekening van deze aanpakken voor de onderneming.

Voorlichting, cursussen en onderwijsmateriaal op verschillende niveaus (kortlopende cursussen, inbouw in bestaande curricula; technische, juridische en/of organisatorische insteek) bieden mogelijkheden om een groter bewustzijn rond privacybeschermende maatregelen te realiseren en na te gaan welke maatregelen precies nodig zijn voor een onderneming. Het kan ook helpen om de vraagarticulatie te verbeteren en om aan de aanbiederskant te werken aan een grotere verscheidenheid aan aanbod. Tot slot kan het verduidelijken hoe professioneel opdrachtgeverschap met betrekking tot privacy en bescherming van persoonsgegevens eruit kan zien.

Sterkere vormen van interventie richten zich op het onderzoeken van de behoeften om tot **standaardisering** van processen en afspraken te komen. Dit kan zowel op brancheniveau als door de overheid worden geïnitieerd. Duidelijk is dat draagvlak nodig is bij de branches om tot succesvolle implementatie te komen. Hetzelfde geldt indien **certificering** nagestreefd wordt (bijvoorbeeld van auditprocedures). Certificering en standaardisering draagt bij aan professionalisering van de aanpak.

Harmonisatie van wetgeving is een harde interventie. Dit wordt momenteel voorbereid door het voorstel van herziening van de huidige dataprotectierichtlijn (95/46/EU). Door aan te koersen op een verordening beoogt de Europese Commissie de harmonisatie tussen landen te vergroten.

Tot slot, de overheid kan in zijn rol als **launching customer** een voorbeeldfunctie vervullen en een impuls geven aan een aantal van de hierboven gesignaleerde vraagstukken. Dit is in lijn met de eerder genoemde motie (motie Nicoloai) die de overheid hiertoe aanzet.

Inhoudsopgave

Managementsamenvatting **2**
Persoonsgegevens en *Privacy by design* 2
Het onderzoek 4
Conclusies remmende en stimulerende factoren 5
Belangrijkste stimulerende en remmende factoren 8
De organisatie van de markt en het innovatiesysteem 9
Aanbevelingen 10

Voorwoord **14**

1 Inleiding **15**
1.1 Privacy by Design 15
1.2 Doel en onderzoeksvraag 16
1.3 Aanpak 16
1.4 Verantwoording 18
1.5 Leeswijzer 18

2 Trends en ontwikkelingen **20**
2.1 De datamaatschappij 20
2.2 De economische waarde van gegevens 24
2.3 De privacyparadox 27
2.4 Noodzaak van betere afscherming van persoonsgegevens 29

3 Privacy by Design **30**
3.1 Inleiding 30
3.2 Privacy of bescherming van persoonsgegevens? 31
3.3 De aanpak van privacybescherming in de praktijk 33
3.4 Privacy by Design: van principe tot methode 35

4 Privacy by Design: meten van diffusie en adoptie **42**
4.1 Inleiding 42
4.2 Diffusie van innovaties 42
4.3 Het gehanteerde model voor diffusie van PbD-innovaties 46
4.4 Imperfecties in markten en in innovatiesystemen 51
4.5 Aanpak empirisch onderzoek 53

5 Resultaten **57**
5.1 Privacy by Design 57
5.2 De praktijk 59
5.3 Innovatiekenmerken van Privacy by Design 61
5.4 Organisatorische kenmerken 66
5.5 Externe omgeving 70
5.6 Internationaal perspectief 76
5.7 Analyse 82

6 Conclusies en aanbevelingen **91**
6.1 Positieve externaliteiten/spillovers 92
6.2 Niet-effectieve marktwerking 92
6.3 Lock-in en padafhankelijkheid 92

6.4 Institutionele belemmeringen 93
6.5 Falende interacties 93
6.6 Onvoldoende vaardigheden en kennis 93
6.7 Ter afsluiting 94

7 Literatuurlijst 95

Appendix 1 Het Privacy Maturiteitsmodel 98

Appendix 2 Overzicht adoptiefactoren 102

Appendix 3 Dataverwerkend Nederland 104

Appendix 4 Voorstel voor Europese verordening voor dataprotectie 108

Appendix 5 Overzicht geïnterviewde organisaties 110

Appendix 6 Interviewprotocol 112

Appendix 7 Leden klankbordgroep 116

Voorwoord

Op basis van de Beleid- en Toepassingsgerichte Kennis (BTK-) middelen die TNO beschikbaar krijgt van het ministerie van Economische zaken, Landbouw en Innovatie heeft TNO een studie uitgevoerd naar de toepassing van *Privacy by Design* in het Nederlandse bedrijfsleven. Voorliggend rapport is hier het resultaat van. Het onderzoek past in de activiteiten die TNO onderneemt rond privacy en identity management. Dit onderzoek wordt inmiddels gebundeld in het Privacy & Identity Lab, een expertisecentrum waarin TNO samenwerkt met de Radboud universiteit, de Universiteit van Tilburg en SIDN.

Het onderzoek dat tot deze rapportage heeft geleid, is begeleid door een klankbordgroep die bestaat uit vertegenwoordigers van twee ministeries (naast ELI ook het ministerie van Veiligheid en Justitie) en het Nederlandse bedrijfsleven (VNO-NCW/MKB en ICT Office). De klankbordgroep heeft onderzoeksaanpak en resultaten bekeken en van commentaar voorzien.

De verantwoordelijkheid voor de rapportage ligt geheel bij TNO. Met de resultaten van dit onderzoek versterkt TNO zijn eigen kennisbasis. TNO hoopt dat de resultaten en aanbevelingen ook voor andere partijen van belang zullen zijn.

1 Inleiding

1.1 Privacy by Design

Het toenemend (mobiel) internetgebruik en de opkomst van technieken als Internet of Things en Cloud Computing zorgen voor toenemende verzameling en gebruik van gegevens. Het gaat om triljoenen bytes aan gestructureerde en ongestructureerde data gegenereerd door sensoren, camera's, mobiele apparaten, het internet en de digitale transacties die daaruit volgen. De gegevens bevatten soms zeer gedetailleerde informatie van en over consumenten. Het internet wordt gedomineerd door diensten waaraan een steeds verdere intensivering van gegevensverwerking ten grondslag ligt. Het World Economic Forum noemt persoonlijke gegevens de nieuwe olie van de economie gezien hun belang voor economische en sociale waardecreatie in alle sectoren van de economie (WEF 2010).

Door de snelle technologische ontwikkelingen verandert de aard van mogelijke privacyschendingen en wordt de uitvoering en handhaving van bestaande privacywetgeving steeds moeilijker. Niet alleen de kwantiteit van verzamelde persoonlijke gegevens verandert maar ook de kwaliteit van deze gegevens; er valt ook meer uit af te leiden. Volgens Hildebrandt (2011) is het grote verschil tussen online en offline gegevens momenteel dat er online voortdurend gegevens worden 'gelekt'. Daarnaast is sprake van verbreding van bewuste, gerichte verzameling naar onbewuste en ongerichte verzameling van gegevens van internetgebruikers. Recente discussies over Facebook, Google Street View en behavioural targeting tonen een toenemende aandacht en gevoeligheid voor privacykwesties in de maatschappij. De behoefte aan alternatieve concepten om de privacy van consumenten te waarborgen en tegelijkertijd de vruchten te plukken van alle nieuwe (internet)diensten die de datamaatschappij biedt, groeit.

Zowel aan de kant van de overheid (onder meer de Europese Commissie) als bij verschillende – voorlopende – bedrijven (ITRE 2011) is er in toenemende mate belangstelling voor aanvullende mogelijkheden om de privacy van burgers beter te beschermen. Een van die mogelijkheden is *Privacy by Design* (PbD). Hoewel een eenduidige definitie ontbreekt wordt hiermee vaak bedoeld dat al bij het ontwerpen en de toepassing van technologie in (elektronische) dienstverlening rekening wordt gehouden met de noodzaak van privacybescherming. Het gedachtegoed van PbD (zie Cavoukian, 2009) is op een aantal punten breder dan de oorspronkelijke *Privacy Enhancing Technologies*-benadering.[1] Het heeft een systemische benadering ('van wieg tot wieg') en het betrekt ook niet-technische aspecten (procesmatige/organisatorische en ruimtelijk) nadrukkelijk bij de vormgeving van nieuwe diensten. Het concept is nu opgenomen in het voorstel voor de herziening van de Europese dataprotectierichtlijn (EC, 2012).

[1] Al aan het eind van de vorige eeuw speelde de vraag naar de rol van technologie (*Privacy Enhancing Technologies*) in het versterken van de bescherming van persoonsgegevens binnen overheidsinformatiesystemen. De motie Nicolai (Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 31) bepleitte de actieve inzet van de overheid in de toepassing van PETs voor de bescherming van persoonsgegevens in overheidsinformatiesystemen. Zie Koorn R. et al. (2004).

Bij het bedrijfsleven bestaat onzekerheid en onduidelijkheid over het nut van en de mogelijkheden om persoonsgegevens met PbD systematisch en 'van wieg tot wieg' te beschermen en om gebruikers transparantie, keuze en controle te bieden in gegevensopslag en -verwerking. De onzekerheid en de onduidelijkheid komen voort uit onder andere het ontbreken van een eenduidig antwoord op de vragen naar de bedrijfseconomische consequenties van het invoeren van privacybeschermende maatregelen, wat de maatschappelijke opbrengsten hiervan zijn en waar bedrijven wettelijk verplicht toe zijn. Tegelijkertijd krijgen steeds meer bedrijven met deze vragen te maken, onder meer omdat er steeds meer mogelijkheden zijn voor bedrijfsmatige vergaring, opslag, verwerking en verspreiding van persoonsgegevens.

Bedrijven die overwegen om PbD toe te passen zullen een afweging maken tussen de bedrijfsmatige voor- en nadelen van PbD. Naast directe voor- en nadelen spelen vragen over risicobeheersing een rol. Als PbD bijdraagt aan verbetering van het maatschappelijk profiel van een bedrijf, tot een betere beheersing van bepaalde risico's en daarmee ook bijdraagt aan bedrijfseconomisch rendement zou toepassing vanPbD interessant kunnen zijn. Als toepassing van PbD vooral een kostenpost betekent met slechts een geringe opbrengst voor de organisatie, dan zal de behoefte om te investeren in PbD geringer zijn.

1.2 Doel en onderzoeksvraag

Privacy en Identity management vormt eén van de domeinen waar TNO kennis over opbouwt. TNO richt zich op het realiseren van betere maatschappelijke diensten voor burgers (overheidsdiensten) en consumenten (dienstverlening door bedrijven). Privacybescherming en identiteitsmanagement spelen soms een rol bij de verbetering van deze dienstverlening. TNO onderzoekt of en zo ja hoe deze diensten verbeterd kunnen worden. In dit onderzoek gaat het daarbij om zicht te krijgen op stimulerende en remmende factoren rond de toepassing van *Privacy by Design* door het Nederlandse bedrijfsleven. In deze studie onderzoeken we de motivaties van het Nederlandse bedrijfsleven om wel of niet te investeren in het toepassen van *Privacy by Design*. Onderzoeksvragen zijn:

1. Wat zijn de overwegingen van bedrijven om *Privacy by Design* toe te passen dan wel juist niet toe te passen en wat zijn drijvende en belemmerende factoren hierbij?
2. Welke positie neemt Nederland met betrekking tot de invoering van *Privacy by Design* in internationaal perspectief en welke succesvolle voorbeelden van PbD zijn er te vinden?
3. Welke rol kan de overheid vervullen om de toepassing van *Privacy by Design* te bevorderen?

1.3 Aanpak

De studie is uitgevoerd tussen april 2011 en april 2012. In deze periode zijn de volgende activiteiten uitgevoerd:

- *Opzet conceptueel kader en empirisch onderzoek*. Omtrent het begrip '*Privacy by Design*' bestaat nog veel onduidelijkheid. Er bestaat geen door iedereen geaccepteerde definitie. Het conceptueel kader dat wij hanteren (Lieshout et al. 2011) onderscheidt verschillende dimensies van PbD, zoals technische en organisatorische elementen. Om zicht te krijgen op de stimulerende en

remmende factoren rond de toepassing van *Privacy by Design* wordt PbD in dit onderzoek beschouwd als een innovatie. We maken gebruik van bestaande inzichten in de innovatieliteratuur over adoptie en diffusies van innovaties om stimulerende en belemmerende factoren te identificeren.

- *Uitvoering empirisch onderzoek*. Er zijn negentien interviews gehouden met diverse Nederlandse organisaties die een vorm van PbD in de bedrijfsvoering hebben toepast. Het gaat met name om bedrijven en organisaties die op systematische en gestructureerde wijze maatregelen in de omgang met persoonsgegevens in hun bedrijfsprocessen hebben ingevoerd. De motivering voor deze keuze is de volgende: i) we veronderstellen dat deze bedrijven een beter zicht hebben op wat zich in de 'markt' van privacygerichte maatregelen afspeelt dan bedrijven die geen ervaring met PbD hebben, ii) we veronderstellen dat deze bedrijven meer ervaring hebben met de gevolgen van het invoeren van privacygerichte maatregelen voor de bedrijfsvoering dan andere bedrijven en iii) we veronderstellen dat deze bedrijven een beter beeld hebben van de veranderende omgeving in relatie tot eisen ten aanzien van het omgaan met persoonsgegevens dan andere bedrijven. Deze bedrijven zijn geïdentificeerd via de leden van de klankbordgroep en brancheorganisaties. De interviews zijn gehouden met personen binnen deze organisaties die verantwoordelijk zijn voor de omgang met persoonsgegevens. Dit geeft mogelijk een bias in de beantwoording (gerichtheid op voldoen aan wettelijke vereisten). Dit zullen we bij de resultaten moeten meewegen. Het overzicht van de geïnterviewde organisaties is te vinden in Appendix 5 Overzicht geïnterviewde organisaties'. Er is gestreefd naar een verdeling tussen diverse bedrijfstakken, data-intensieve bedrijven en dataverwerkers en aanbieders van privacybeschermende maatregelen.
- *Internationale vergelijking:* via desk research en interviews is de stand van zaken in diverse landen verkend. Onderzochte landen zijn: Duitsland, Verenigd Koninkrijk, Canada en de Verenigde Staten. Deze verkenning maakt het mogelijk gedeelde ervaringen, problemen én eventuele oplossingsrichtingen in kaart te brengen. Daarnaast biedt deze verkenning ook de mogelijkheid om na te gaan waar de situatie in Nederland duidelijk afwijkt van deze landen en welke factoren daar aanleiding toe geven.
- *Rol van de overheid:* op basis van de voorgaande activiteiten en de analyse van huidige drijvende en belemmerende factoren ten aanzien van de toepassing van *Privacy by Design*, is gekeken naar mogelijke rollen van de overheid om bepaalde barrières mee te helpen oplossen en bepaalde stimulansen eventueel verder te versterken.

Het onderzoek heeft een exploratief karakter. Het onderzoek heeft geen representatief beeld ten aanzien van de invoering van *Privacy by Design* in het Nederlandse bedrijfsleven opgeleverd. Het onderzoek richt zich op de perceptie van het bedrijfsleven over stimulerende en remmende factoren van toepassing van *Privacy by Design*. De oorspronkelijke opzet van het empirisch onderzoek bestond uit een representatieve online survey uitgezet onder het Nederlandse bedrijfsleven, aangevuld met een aantal expertinterviews. De testfase van de survey heeft uitgewezen dat de survey op dit moment geen goed instrument is voor het onderzoeken van stimulerende en remmende krachten op benutting van PbD. In de pilotfase bleek de weerstand bij representanten van bedrijfstakken tegen een survey te groot om een succesvolle respons (en daarmee representatief beeld) te verkrijgen. De weerstand had vooral te maken met de perceptie dat het onderzoek

toch ook een beeld op zou leveren over de mate waarin het Nederlandse bedrijfsleven zich zou houden aan wettelijke voorschriften (*compliance*). De meegeleverde opzet van het onderzoek en de gepresenteerde onderzoeksdoelen bleken niet voldoende om deze weerstand weg te nemen. Daarom is gekozen voor interviews die zich richten op de percepties van een aantal voorlopende organisaties ten aanzien van stimulerende en remmende factoren bij de toepassing van PbD. Het begrip 'voorloper' is afkomstig uit de innovatietheorie. Hoewel dit begrip suggereert dat er een volgtijdelijkheid is in de aanvaarding van een innovatie is dit niet het uitgangspunt van deze studie. Het is net zo goed mogelijk dat de belemmerende factoren groter zijn dan de stimulerende en dat een innovatie dus niet van de grond komt. Dat kan ook voor *Privacy by Design* gelden.

1.4 Verantwoording

Het onderzoek is gefinancierd uit de kennismiddelen die TNO ter beschikking krijgt van het ministerie van Economische Zaken, Landbouw en Innovatie. Een deel van deze middelen wordt besteed in het kader van de Beleids- en Toepassingsgerichte Kennisontwikkeling (de BTK-middelen). Dit onderzoek versterkt de kennisbasis van TNO terwijl de opbrengsten een strategische waarde voor het ministerie dienen te hebben. Onderhavig onderzoek is uit deze BTK-middelen gefinancierd.

Het onderzoek is begeleid door een klankbordgroep, bestaande uit vertegenwoordigers van het ministerie van Economische Zaken, Landbouw en Innovatie, het ministerie van Veiligheid en Justitie, ICT-Office, VNO-NCW/MKB en een onafhankelijk expert (zie de bijlage voor de samenstelling). De taak van de klankbordgroep bestond uit het begeleiden van de opzet, de uitvoering en de rapportage van de studie. De verantwoordelijkheid voor het uitvoeren van de werkzaamheden voor het onderzoek en de naar buiten te brengen resultaten ligt geheel bij TNO.

1.5 Leeswijzer

In *hoofdstuk twee* presenteren we een overzicht van ontwikkelingen met betrekking tot de vergaring, bewerking en verspreiding van persoonsgegevens. Deze korte introductie toont de groei in handel van persoonsgegevens op een groot aantal uiteenlopende fronten. Het hoofdstuk is gebaseerd op een aantal actuele bronnen dat zich richt op het in kaart brengen van de economie achter de verzameling van persoonsgegevens. Het hoofdstuk maakt inzichtelijk dat deze ontwikkeling plaatsvindt en dat de omvang van deze ontwikkeling vele bedrijfstakken en vele activiteiten betreft.

In *hoofdstuk drie* introduceren we het conceptuele kader dat we voor deze studie hebben gebruikt. We starten met het aangeven van het onderscheid tussen privacy en dataprotectie. We positioneren dit in de praktijk en introduceren onze benadering van *Privacy by design*.

Hoofdstuk vier gebruiken we voor de introductie van het methodische kader dat we voor deze studie hebben gebruikt. Kern van onze aanpak is de benadering van *Privacy by Design* als een innovatie. We starten met de traditionele 'Rogeriaanse' aanpak van innovatie- en diffusiepatronen. Deze werken we uit naar een omvattender benadering die meer oog heeft voor organisatorische aspecten. Dit

verbinden we met de indicatoren die we in het empirisch deel gaan toetsen. Deze indicatoren zijn op hun beurt gerelateerd aan bepaalde constructen die iets zeggen over de innovatie, de organisatie en de externe omgeving (bij beide de faciliterende voorwaarden en de beïnvloeding vanuit een bredere context) waarin een innovatie plaatsvindt. Voor het bepalen van de rol van de overheid hanteren we een model waarin imperfecties in het functioneren van de markt en van het innovatiesysteem bij elkaar worden gebracht. We introduceren dit model.

In *hoofdstuk vijf* presenteren we de empirische bevindingen. We hanteren de in hoofdstuk vier gepresenteerde structuur en geven eerst aan wat de interviews opgeleverd hebben over de verschillende indicatoren. Vervolgens maken we een vertaalslag van deze bevindingen naar de gepresenteerde constructen om dit tot slot te analyseren vanuit de context van imperfecties in de markt en in innovatiesystemen.

Hoofdstuk zes geeft aan wat vanuit deze analyse rollen en aanpakken van de overheid zouden kunnen zijn, indien zij ervoor kiest om geconstateerde barrières te slechten en eventuele stimulansen verder te brengen.

Hoofdstuk zeven, tot slot, bevat een overzicht van gehanteerde referenties.

In de bijlagen treft de geïnteresseerde lezer een korte uiteenzetting over het *Privacy Maturity Model.* Dit model geeft een systematische indeling van de wijze waarop bedrijven om kunnen gaan met het afvangen van risico's wanneer zij met persoonsgegevens in hun bedrijfsvoering te maken hebben. Dit model is uiteindelijk niet gebruikt in het onderzoek maar het biedt een interessant handvat voor eventueel vervolgonderzoek. We geven de tabel met alle gehanteerde indicatoren, de constructen waartoe ze behoren en een korte toelichting op de achtergrond van de indicator. Vervolgens geven we een overzicht van de bedrijfstakken die in Nederland aangemerkt worden als data-intensieve bedrijfstakken. We categoriseren deze bedrijfstakken aan de hand van enkele kenmerken. We presenteren het voorstel voor een Europese verordening op het gebied van gegevensbescherming op een aantal punten. Dit voorstel is in januari 2012door de Europese Commissie publiek gemaakt. Hij werpt zijn schaduw vooruit op een aantal punten rond de privacydiscussie. Tot slot treft u een overzicht van geïnterviewde organisaties en de samenstelling van de klankbordgroep die dit onderzoek begeleid heeft.

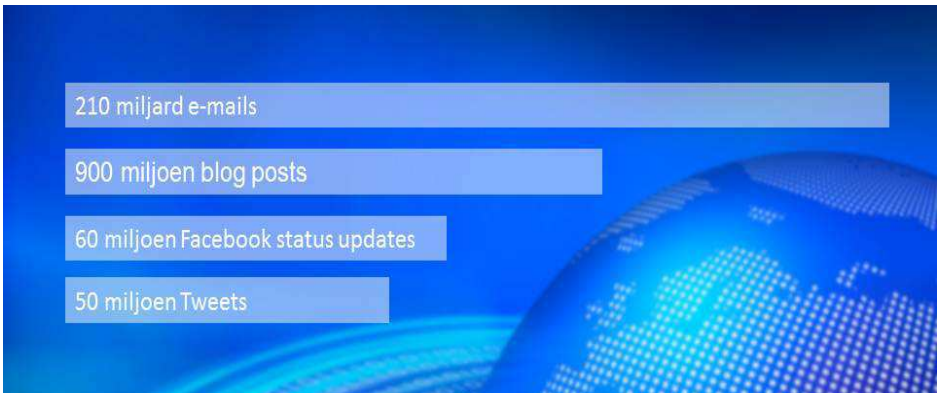
2 Trends en ontwikkelingen

2.1 De datamaatschappij

2.1.1 Big Data en persoonsgegevens als de nieuwe olie

Nieuwe technieken en diensten zoals het toenemend (mobiel) internetgebruik, de opkomst van Internet of Things en Cloud Computing zorgen voor een groeiende hoeveelheid en stroom aan digitale gegevens. Het gaat om triljoenen bytes aan gestructureerde en ongestructureerde data gegenereerd door sensoren, camera's, mobiele apparaten, het internet en de digitale transacties die daaruit volgen (zie ook **Error! Reference source not found.**). In 2020 schat men dat er meer dan 50 miljard mobiele apparaten met het internet verbonden zullen zijn (WEF 2010). Het digitale universum zal naar verwachting groeien van 1,8 zettabytes aan gegevens in 2011 naar 40.000 exabytes in 2020 (IDC 2011). De wereld heeft nu al elke twee dagen vijf miljard gigabyte opslagruimte nodig (Pariser 2011). Deze enorme hoeveelheid gegevens wordt ook wel aangeduid als 'Big Data', refererend aan datasets die te groot zijn om te beheren, op te slaan en te analyseren met reguliere database software tools (McKinsey 2012; Wikibon 2011). De term datamaatschappij wordt steeds vaker gebruikt om aan te geven dat de samenleving beweegt naar een volgende fase in de informatiemaatschappij waarin de groeiende gegevensstroom een centrale en essentiële economische grondstof en innovatiebron is voor de 21e eeuw. Ze biedt nieuwe kansen voor economische en sociale waardecreatie voor bedrijven, overheden en consumenten in alle sectoren van de economie (WEF 2010; McKinsey 2011).

Figuur 2: Per dag wordt de volgende informatie gedeeld (bron Pariser 2010)

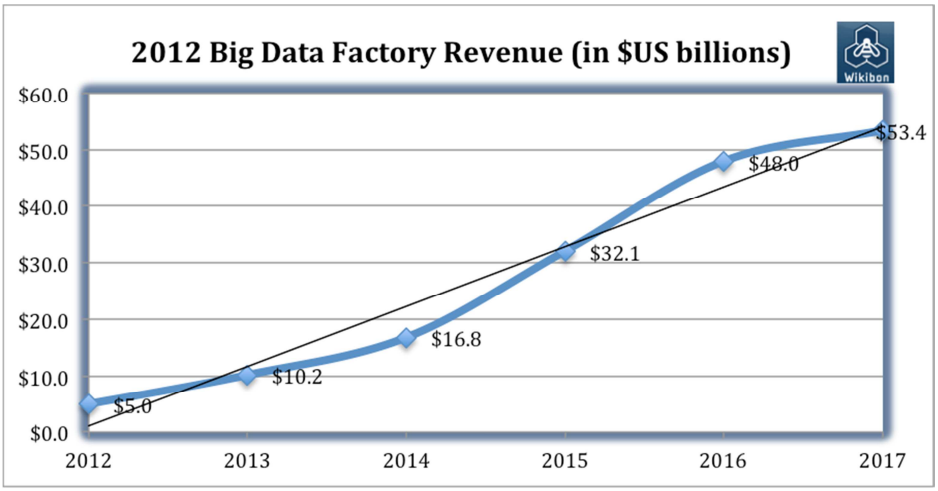


Technologiebedrijven investeren steeds meer geld in de ontwikkeling van nieuwe technieken, architecturen en algoritmes om de grote hoeveelheden van gegevens(verkeer) te doorzoeken, relevante informatie te extraheren en hier economische waarde uit te halen.[2] De investeringen betreffen opslag- en servertechnologie die het verwerken van deze gegevensstromen kunnen ondersteunen, datamining software tot aan visualisatietools die gevonden verbanden en patronen inzichtelijk maken. Marktanalisten verwachten dat de markt in 'Big Data' de komende jaren snel zal groeien naar meer dan $50 miljard wereldwijd in 2017 (zie Figuur 3). Volgens de jaarlijkse voorspellingen van IDC over

[2] http://bits.blogs.nytimes.com/2012/02/15/i-b-m-big-data-bigger-patterns/

de omvang van het digitale universum zal het aantal servers (virtueel en fysiek) wereldwijd een factor 10 groeien. IBM heeft in het kader van haar Big Data programma in de afgelopen vijf jaar in totaal $14 miljard aan software-analyse-bedrijven aangekocht.[3]

Figuur 3: Verwachte groei in Big Data opbrengsten 2012-2017 (in miljarden dollar)



Bron: Wikibon

De gegevens bevatten in toenemende mate ook gedetailleerde informatie van en over consumenten. Het World Economic Forum noemt persoonlijke gegevens dan ook niet voor niets de nieuwe olie van de economie (WEF 2010). Ze worden verzameld, geaggregeerd, geïntegreerd, verwerkt en uitgewisseld door een veelvoud van gefragmenteerde en gedecentraliseerde systemen, apparaten en dienstaanbieders. Het gaat om identiteitgerelateerde gegevens (e-mail, namen, adressen, telefoonnummers), relaties (mensen en organisaties), activiteiten en gedrag (zoekgedrag, browsergeschiedenis, muisklikken), locatiegebaseerde data (GPS, WiFi), communicatiedata en gegevens over het communicatieverkeer (logs van sms-berichten, telefoongesprekken, IP-adressen, sociale netwerk posts, data van navigatiesystemen e.d), multimedia (video, audio, foto's), financiële data (transacties, bankrekeningen, saldi), medische gegevens (variërend van onze medische geschiedenis tot aan apparaten die onze hartslag op continue basis monitoren) en institutionele gegevens (overheids- en werkgeversgegevens). De data kunnen vrijwillig door consumenten worden gedeeld, 'geobserveerd' worden door anderen (zoals het opslaan van locatiegegevens als de mobiele telefoon wordt gebruikt) of worden afgeleid op basis van de verwerking en analyse van andere gegevens.

Er ontstaan grootschalige platformen waarin persoonlijke gegevens van vele consumenten worden gecentraliseerd. Voorbeelden zijn de netwerken en gegevensverzameling door Facebook, Google, Amazon en Apple. Los van deze grote spelers ontstaan er steeds grotere en gedetailleerde databases met persoonsgegevens bij allerlei soorten bedrijven, inclusief het Midden en Kleinbedrijf. Een survey uit 2008 onder Europese bedrijven liet zien dat meer dan 50% van de grote bedrijven persoonsgegevens verhandelt. Circa 20% van de databases met

[3] idem

persoonlijke gegevens bevat meer dan 10.000 records met vaak gedetailleerde persoonlijke gegevens van klanten (LE 2010).

2.1.2 Complexiteit en grip op datastromen

Met deze toenemende intensivering van gegevensverwerking nemen ook de risico's op privacyschendingen toe. Niet alleen de kwantiteit van verzamelde persoonlijke gegevens neemt toe maar ook de kwaliteit van deze gegevens; er valt meer uit af te leiden. Volgens Hildebrandt (2011) is het grote verschil tussen online en offline gegevens momenteel dat online voortdurend gegevens worden 'gelekt' en is sprake van de verbreding van bewuste, gerichte verzameling naar onbewuste en ongerichte verzameling van gegevens van internetgebruikers. Daarnaast worden de technologieën die gebruikt worden op het internet steeds complexer. Bij de online advertentiemarkt zijn bijvoorbeeld vele spelers en technieken betrokken. Website-eigenaren, adverteerders, uitgevers, advertentienetwerken, media- en reclamebureaus, *affiliate* netwerken en leveranciers van webstatistieken en andere tracking technieken plaatsen (zelf, voor en door anderen) cookies op computers van internetgebruikers. De advertentienetwerken maken gebruik van geaggregeerde data van verschillende websites op basis van complexe afrekenmodellen die over vele lagen en partijen gaan. Het is daarom voor website-eigenaars en consumenten steeds moeilijker te achterhalen of getoonde advertenties tot stand zijn gekomen door gerichte reclame of via een andere methode.

De toenemende complexiteit en convergentie van gebruikte technologieën maakt het voor dienstaanbieders en consumenten steeds moeilijker en onduidelijker om grip te krijgen op deze datastromen, welke regelgeving van toepassing is en voor consumenten om zicht te krijgen op welke gegevens worden verzameld, door wie en waarom. Gegevens kunnen worden verzameld zonder dat consumenten dit weten of hier bewust toestemming toe geven. Box 1 geeft een aantal illustraties hiervan weer. Eenmaal rondzwervend, zijn de gegevens voor de consument bijzonder moeilijk, zo niet onmogelijk, te traceren of te verwijderen.

Voor bedrijven betekent de groeiende hoeveelheid data ook toenemende aandacht voor privacybescherming en beveiliging van deze gegevens. Datalekken worden in toenemende mate geregistreerd en geven de kwetsbaarheid weer van de onderliggende technische infrastructuur. Zo waren er in 2011 in de Verenigde Staten volgens het Privacy Rights Clearinghouse 535 bekende datalekken waarbij 30,4 miljoen gevoelige gegevens betrokken waren.[4] De ondergang van Diginotar toont enerzijds de risico's van onvoldoende zorgvuldigheid bij de inrichting en beveiliging van informatiesystemen en anderzijds de complexiteit die de beveiliging van informatiesystemen vereist.

[4] Privacy Clearing House (2011) Data breaches: a year in review. 16 December 2011, http://www.privacyrights.org/data-breach-year-review-2011 and Chronology of data breaches, http://www.privacyrights.org/data-breach/new

Box 1 Voorbeelden on(op)gemerkt gebruik van persoonlijke gegevens

Advertentiemaatschappijen volgen iPhone gebruikers
In februari 2012 ontstond er ophef over advertentiemaatschappijen, zoals Double Click van Google, die het surfgedrag van vele iPhone-gebruikers konden volgen terwijl dit door de standaardblokkade in de software niet mogelijk zou moeten zijn. Google maakt gebruikt van een webformulier dat verborgen zit in een online advertentie met een +1 knop. Wanneer de gebruiker op de knop klikt, vertelt Google de Safari-browser dat dit formulier is ingevuld. De Safari-browser staat het plaatsen van cookies toe als een gebruiker op een site is geweest voor 12 tot 24 uur. Op deze manier kon Google's Double Click ook cookies plaatsen en het surfgedrag van gebruikers volgen zonder dat zij dit wisten. Volgens Google gebeurde dit onbedoeld en werd gebruik gemaakt van bekende functionaliteiten in de Safari-browser. Het bedrijf verwijdert nu de cookies van de Safari. Het plaatsen van cookies via deze omweg lijkt al langer bekend bij Apple. Het bedrijf heeft nu besloten deze omweg onmogelijk te maken.[5]

Mobiele applicaties slaan adresboek op
In februari 2012 ontstond er discussie over mobiele applicaties die zonder medeweten van de gebruiker het complete adresboek kopiëren en op servers van de applicatie-aanbieder opslaan. Twitter bewaart deze gegevens achttien maanden. De directeur van het privacyvriendelijke sociale netwerk Path zorgde voor veel ophef door dit gebruik als *'best practice'* in de industrie te benoemen.[6]

Like-knop van Facebook
Eind november 2010 werd bekend dat de like-knop van Facebook cookies plaatst op de apparatuur van gebruikers zonder dat zij op deze knop hadden geklikt. Dit stelde Facebook in staat het surfgedrag van vele gebruikers, ook zonder Facebook-account, te volgen (Roosendaal, 2010). Volgens Facebook was dit een fout in de software waardoor deze cookies onbedoeld werden geplaatst en is deze fout inmiddels verholpen. Het plaatst geen cookies meer via de knop bij internetgebruikers die geen lid van Facebook zijn. In de Duitse deelstaat Schleswig-Holstein mogen Duitse websites de like-knop niet meer gebruiken.[7]

De inzet van gezichtsherkenningsoftware
Het Carnegie Mellon instituut in de Verenigde Staten toonde in augustus 2011 met verschillende experimenten aan dat onbekenden geïdentificeerd kunnen worden en informatie over hen opgehaald kan worden (inclusief hun *social security number*) via gezichtsherkenningssoftware en profielinformatie van sociale media. In het eerste experiment werden personen geïdentificeerd die lid waren van een datingsite en hun identiteit afschermden via pseudoniemen. In een ander experiment werden studenten op de universiteitscampus geïdentificeerd op basis van hun Facebookprofiel. In het derde experiment werden de persoonlijke interesses van studenten, en in sommige gevallen hun *social security* nummer, op basis van hun foto achterhaald.[8]

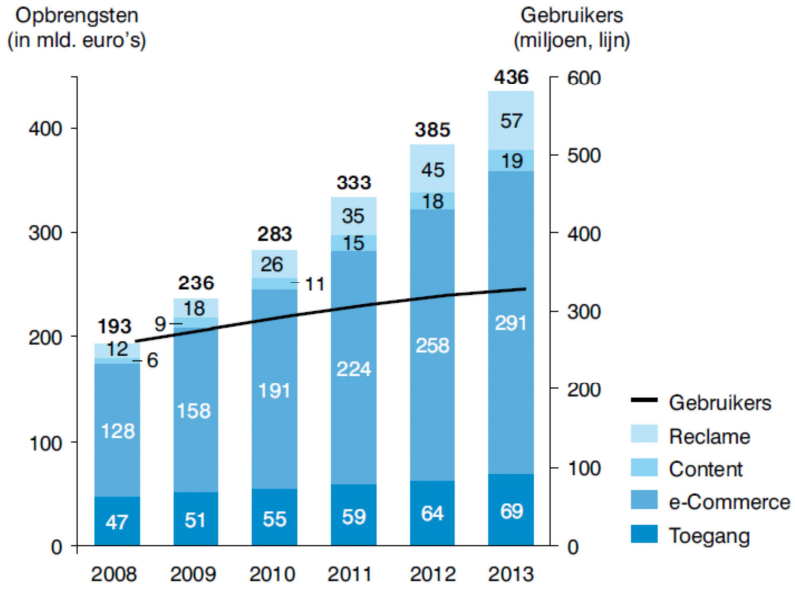
[5] Angwin, J. en Valentino-DeVries, J. (2012) Google's iPhone tracking. The Wall Street Journal, 17 februari 2012, online beschikbaar op: http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-lMyQjAxMTAyMDEwNjExNDYyWj.html, zie ook: http://www.techzine.nl/extern-nieuws/31040/google-accused-of-illicit-iphone-tracking.html en http://www.pcworld.com/article/250213/googles_safari_tracking_debacle_reality_check.html
[6] http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/ en http://bits.blogs.nytimes.com/2012/02/12/disruptions-so-many-apologies-so-much-data-mining/
[7] http://bits.blogs.nytimes.com/2011/09/27/as-like-buttons-spread-so-do-facebooks-tentacles/ http://www.adwise.nl/blog/facebook-like-illegaal-deelstaat-duitsland.html
[8] http://www.cmu.edu/homepage/society/2011/summer/facial-recognition.shtml http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/

2.2 De economische waarde van gegevens

De beschreven ontwikkelingen maken duidelijk dat er steeds meer persoonlijke gegevens verzameld worden en dat deze in toenemende mate ook een economische waarde vertegenwoordigen. Het internet wordt gedomineerd door diensten waaraan een steeds verdere intensivering van gegevensverwerking ten grondslag ligt. Voorbeelden zijn locatiegebaseerde diensten, cloud computing, RFID, biometrische diensten en online *behavioural targeting* (zie ITRE 2011). Zij breiden het type persoonlijke gegevens dat verzameld en geëxploiteerd kan worden steeds verder uit. Veel verdienmodellen van internetbedrijven zijn gebaseerd op gerichte en gepersonaliseerde reclame, die op hun beurt zijn gebaseerd op gegevens die de consument achterlaat en het verkeer dat hij/zij genereert. De consument kan op deze manier vaak gratis, of voor een klein bedrag, gebruik maken van online diensten en mobiele applicaties. Figuur 4 laat de geschatte groei van online reclame zien in Europa.

Exacte cijfers over de omvang van de totale markt van online reclame zijn schaars en lopen zeer uiteen. Schattingen variëren van $750 miljoen in 2008 tot $4.4 miljard in 2012. Andere bronnen geven aan dat de online *behavioural targeting* markt ongeveer 5% tot 9% van het totale bedrag voor (online) advertenties uitmaakt in de Verenigde Staten (ITRE 2011).

Figuur 4: Online opbrengsten en gebruikers in de EU



Noot: Europa inclusief EU-26, Noorwegen en Zwitserland
Bron: Forrester e-Commerce Forecast, Bedrijfsrapportage Apple, Bedrijfsrapportage Google, EU TV and Broadband Forecast Model, Booz & Company analyse

Bron: Booz en Company 2008

De (komende) beursgang van verschillende internetbedrijven in 2011 en 2012 geeft een eerste inzicht in wat persoonlijke gegevens in de datamaatschappij waard zijn. Het zakelijke sociale netwerk LinkedIn (100 miljoen gebruikers) maakte in mei 2011 een succesvolle gang naar de beurs: de eerste dag werd afgesloten met 109% winst. Het netwerk haalde daarmee 350 miljoen dollar op, de waarde van het bedrijf kwam op 10 miljard dollar (7 miljard euro).[9] Binnenkort zal ook Facebook de gang naar de beurs maken. De waarde van het bedrijf wordt inmiddels geschat op $75 miljard tot $100 miljard en is gebaseerd op de persoonlijke gegevens die het inmiddels van meer dan 800 miljoen gebruikers heeft verzameld. Dit zou een waarde van $94 tot $125 per Facebookgebruiker betekenen. Volgens ComScore is Facebook inmiddels het grootste online platform voor advertenties geworden in de Verenigde Staten: meer dan 28% van alle online advertenties worden getoond op Facebook, gevolgd door Yahoo met minder dan de helft daarvan.

Het bedrijf Reputation dat de online reputatie van internetgebruikers (tegen betaling) “opschoont”, schat in dat persoonlijke informatie tussen $50 en $5000 per persoon per jaar waard is voor adverteerders en marktonderzoekbureaus, afhankelijk van hoeveel de persoon uitgeeft en hoe waardevol de informatie is voor derde partijen.[10] Inmiddels zijn er diverse kleine startende ondernemingen die op deze waarde inspelen en internetgebruikers controle proberen te geven over hun persoonlijke gegevens. Ze bewaren de gegevens in digitale kluizen en laten gebruikers de gegevens verhandelen met internetbedrijven. De ondernemingen verdienen geld door een percentage van het overeengekomen verkoopbedrag te innen.[11] Google maakte begin februari 2011 bekend dat het internetgebruikers $25 per jaar wil betalen voor het volgen van hun surfgedrag. Dit in het kader van de ontwikkeling van een nieuw softwareprogramma door het bedrijf. De internetgebruikers worden lid van een testpanel en kunnen een speciale extensie in de Google browser Chrome downloaden. Deelname aan het testpanel blijkt populair onder internetgebruikers. Google heeft inmiddels een tijdelijke stop voor het aantal aanmeldingen aangekondigd.[12]

2.2.1 De kosten van privacyschendingen

Een andere bron van informatie over de waarde van persoonlijke gegevens zijn privacy- en beveiligingsincidenten en de verliezen die daar mee gepaard gaan. Met de toenemende verwerking van persoonlijke gegevens, neemt ook de kans toe dat ze op straat komen te liggen en worden misbruikt. Een studie uit 2010 gebaseerd op bijna 1000 incidenten laat zien dat sinds 2005 de kans op het verlies van persoonlijke gegevens snel toeneemt (Maillart en Sornette 2010). Tot nu toe ontbreken betrouwbare en volledige kwantificeringen van de kosten van het verlies van data en lopen de cijfers zeer uiteen. De incidenten kunnen het imago van de betrokken organisatie schaden. Aan de andere kant zijn er aanwijzingen dat de beurswaarde van een organisatie na een privacy-incident slechts gering daalt en ook slechts voor korte tijd; Acquisti et. al. (2006) vonden een cumulatieve daling in prijzen van aandelen per privacy-incident van circa 0,6% op de dag na de gebeurtenis. Dit is gelijk aan een gemiddeld verlies van circa € 7.4 miljoen ($10 miljoen) in marktwaarde.

[9] http://nos.nl/artikel/241843-spectaculair-beursdebuut-linkedin.html
[10] http://blogs.smartmoney.com/advice/2012/01/25/who-would-pay-5000-to-use-google-you/
[11] http://www.pcpro.co.uk/news/372706/google-pays-25-for-browsing-data
[12] http://www.pcpro.co.uk/news/372706/google-pays-25-for-browsing-data

Ook zijn er pogingen gedaan om de economische verliezen voor consumenten te kwantificeren. Ook hier geldt dat er geen betrouwbare cijfers voorhanden zijn. London Economics heeft een schatting gemaakt door gebruik te maken van de prijzen die voor gestolen persoonlijke gegevens gehanteerd worden (zie Tabel 4), waarbij wordt aangenomen dat de zwarte markt voldoende concurrerend is en dat de prijzen gelijk zijn aan de directe verliezen van consumenten.

Tabel 4 Prijzen voor persoonlijke data verkocht op de zwarte markt (2008)

Plaats	Item	Percentage incidenten	Prijs range
1	Creditcard informatie	49,2%	$0,06-$30
2	Bankrekening credentials	29,2%	$10-$1000
3	E-mail account	7,7%	$0,10-$100
4	E-mail adressen	7,7%	$0,33/Mb - $100/Mb
5	Volledige identiteiten	6,2%	$0,70-$60

Bron: Symantec Global Internet Security Threat Report, Volume XIV (2009) in LE 2010

Ook de economische schade van *phishing* en/of online identiteitsfraude is onbekend. Wat bekend is, is vooral gebaseerd op schattingen. De statistieken van verschillende organisaties lopen wijd uiteen (OECD 2009). Dit heeft o.a. te maken met de definities van wat precies gemeten wordt en de daarvoor gebruikte indicatoren. De opgestelde statistieken zijn daarom moeilijk onderling te vergelijken (TNO 2009). De schattingen lopen uiteen van miljoen tot miljarden euro's. In het Verenigd Koninkrijk worden de kosten voor de Britse economie van online identiteitsfraude bijvoorbeeld geschat op GBP 1.7 miljard (OECD 2009). APACS, de Britse betalingsorganisatie, schatte de kosten voor de Britse industrie op GBP 22,5 miljoen. Gartner (2007) schatte de financiële schade in de Verenigde Staten in 2007 op $3,2 miljard (tegenover $2,8 miljard in 2006). Volgens Gartner verloren Amerikaanse consumenten in 2009 in totaal 5 miljoen dollar (een stijging van bijna 40% ten opzichte van 2008). Voor Nederland zijn geen actuele openbare gegevens bekend. Zo is bijvoorbeeld niet openbaar hoeveel fraude plaatsvindt bij online bankieren en internetaankopen en wat de schade is van *phishing* aanvallen. De banken zelf beschikken vaak wel over deze informatie (TNO 2009).

Meerdere incidenten bij verschillende organisaties kunnen het algemene vertrouwen van consumenten in het internet en online transacties ondermijnen. Een rapport van Booz en Company berekende dat – als het lukt om consumentenvertrouwen in online omgevingen te doen stijgen – de economische winst uit digitale omgevingen op kan lopen tot 11% extra groei (of € 46 miljard) in de Europese Unie, boven op de huidige omzet uit digitale omgevingen van € 436 miljard. Als het consumentenvertrouwen in online omgevingen verslechtert, dan kan er 18% (of € 78 miljard) economische groei verloren gaan. Dit betekent dat het vertrouwen een marktvolume van ongeveer 1% van het BBP voor de EU-27 kan beïnvloeden.

2.3 De privacyparadox

Perceptie-onderzoek laat zien dat de zorg om privacy bij consumenten toeneemt (TNS-NIPO, 2011). Zo is 70% van de Europeanen bezorgd dat persoonlijke gegevens opgeslagen bij partijen voor anderen doeleinden worden gebruikt dan ze oorspronkelijk zijn verzameld. Ook nemen de zorgen van Europeanen toe dat hun gedrag via betaalpassen (54% tegenover 38% in 2008), mobiele telefoons (49% tegenover 43%) en mobiel internet (40% tegenover 35%) wordt opgeslagen. Tegelijkertijd beschouwt 74% van de Europeanen het vrijgeven van persoonlijke informatie als een groeiend onderdeel van het moderne leven. Ook deelt een groeiend aantal internetgebruikers vrijwillig persoonlijke informatie op sociale netwerksites als Hyves, Facebook en Twitter. De zorg om privacy lijkt zich dus niet rechtstreeks te uiten in het gedrag van consumenten. Achterliggende redenen van deze welbekende privacyparadox zijn zaken als te weinig bewustzijn van mogelijke gevolgen, te weinig controle- en keuzemogelijkheden, gebrek aan transparantie over dataverzameling door dienstaanbieders, maar ook de spanning tussen opbrengsten op korte termijn (gratis toegang tot een dienst, korting, e.d.) en onduidelijke eventuele verliezen op lange termijn (zoals mogelijke reputatieschade of de kans op identiteitsfraude) en de relatieve waarde van privacy ten opzichte van andere waarden en belangen (ITRE 2011).

Onderzoek over deze achterliggende factoren van de privacyparadox laten conflicterende resultaten zien. Aan de ene kant lijken consumenten bereid te zijn (meer) te betalen voor privacybescherming indien privacy-informatie zeer duidelijk aanwezig is op websites of applicaties (Tsai et al 2011). Aan de andere kant komt een beeld naar voren dat consumenten geneigd zijn persoonlijke gegevens te delen als daar (economisch) gewin tegenover staat (Acquisti 2010; Spiekermann 2001). Acquisti, John en Loewenstein (2010) laten in verschillende experimenten zien dat de waardebepaling van privacy en de keuze die de consument maakt zeer contextgevoelig is en afhangt van de ‘framing’ en het menselijk beslisgedrag. De experimenten laten zien dat er verschil is in de mate van bereidheid van consumenten om geld te betalen om hun privacy te beschermen *(‘willingness to pay’*) en de mate van bereidheid van consumenten om geld te ontvangen om privacybescherming op te geven (‘*willingness to accept’*). Het blijkt dat de ‘prijs’ die mensen toekennen om een stukje informatie te beschermen verschillend is van de prijs die mensen toekennen om een stukje informatie te verkopen (zie Box 2). Daarnaast hangt de waardering van consumenten van privacy af van een aantal menselijke vooronderstellingen in het maken van beslissingen en het inschatten van kansen, zoals de volgorde waarin opties worden gepresenteerd of de recente confrontatie met een bepaald incident (als een incident kort geleden is opgetreden of bekend is via tv, vrienden en dergelijke wordt de kans op optreden hoger geschat).

De resultaten van deze gedragsexperimenten stellen vraagtekens bij de gedachte dat consumenten op een ‘rationale’ en consistente manier privacy waarderen of kunnen waarderen (bijvoorbeeld door het lezen van *privacy policies* van verschillende diensten, een vergelijking maken en op basis daarvan een dienst uitkiezen). Consumenten nemen besluiten op basis van vuistregels waaraan verschillende voorkeuren of beslismodellen ten grondslag liggen. Het huidig wettelijk kader leunt echter sterk op een rationale keuze op basis van inzage en toestemming voor datagebruik door het individu. Acquisti pleit daarom voor

'*nudging privacy*'; het inbouwen en presenteren van keuzes op een manier die rekening houdt met de preferenties van consumenten om hen zo beter bewust te maken van mogelijke negatieve gevolgen. De bedoeling is niet een keuze voor consumenten te maken door het systeem, of deze via het systeem af te dwingen; *nudging* is bedoeld om privacybeslissingen en overwegingen beter te adresseren bij de consument.

Box 2 Voorbeeld gedragseconomie consumentenwaardering privacy

Gedragexperiment

Acquisti, John en Loewenstein voerden in 2010 een serie experimenten om te onderzoeken hoe consumenten hun privacy waarderen. In een serie experimenten werd proefpersonen twee soorten cadeaubonnen aangeboden in ruil voor het afnemen van een enquête (de enquête was niet echt en was alleen bedoeld als reden om een cadeaubon uit te kunnen delen). Proefpersonen konden kiezen tussen een anonieme cadeaubon van $10 en een bon op naam van $12. De volgende condities werden getest:

1. Ontvang de $10 anonieme bon of wissel deze, indien gewenst, in voor een $12 bon op naam
2. Ontvang de $12 bon op naam of wissel deze, indien gewenst, in voor de $10 anonieme bon
3. Kies tussen een anonieme $10 bon (verschijnt eerst) en een $12 bon op naam
4. Kies tussen een $12 bon op naam (verschijnt eerst) en een $10 anonieme bon

Ter controle werden de bedragen in één experiment omgedraaid: $10 bon op naam en een $12 anonieme cadeaubon. Het experiment werd uitgevoerd met 349 proefpersonen. In deze controleconditie koos elke proefpersoon voor de $12 anonieme bon.

De meerderheid van de proefpersonen in condities één en twee waren meer geneigd de ontvangen bon te behouden. Maar van de proefpersonen in conditie twee was 90,3% meer geneigd de aangeboden $12 bon op naam te houden, tegenover de bereidheid van 52,1% van de proefpersonen in conditie 1 om de $10 bon te houden. Met andere woorden, 52,1% van de proefpersonen was niet bereid geld te ontvangen ('*willingness to accept*') voor minder privacy. Aan de andere kant was slecht 9,7% bereid $2 te betalen ('*willingness to pay*') voor meer privacy door de $12 bon op naam in te wisselen voor de $10 anonieme bon.

In condities drie en vier, waar het ging om keuze en volgorde, bleek dat proefpersonen meer geneigd zijn te kiezen wat het eerste wordt gepresenteerd.

Bron: Acquisti. John & Loewenstein 2010.

Hoewel inzicht in hoe individuele consumenten afwegingen maken ten aanzien van privacy en het gebruik van online diensten kan bijdragen aan een betere privacybescherming door consumenten zelf, moeten we niet uit het oog verliezen dat privacy niet alleen een individueel recht is (zoals vastgelegd in de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties), maar dat privacy ook een sociale en publieke waarde heeft die verder reikt dan dat van het individu. Alle individuen in een (Westerse) maatschappij hebben een gedeeld belang in privacy, gereflecteerd in de gedeelde opvattingen over wanneer privacy onder druk komt te staan – zelfs als individuele opvattingen kunnen verschillen over de aard en waardering van privacy. De publieke waarde van privacy wijst naar het instrumentele belang in het ondersteunen van democratische instituties en praktijken, onder andere door de ondersteuning van vrijheid van meningsuiting en beperking van de macht van de overheid ten opzichte van het individu (Regan, 1995). De privacyparadox laat ook een mismatch zien tussen de korte-termijn

opbrengsten van een bepaald gedrag (directe beloning voor het prijsgeven van persoonlijke informatie) en de lange-termijn individuele en maatschappelijke impact van dat gedrag.

2.4 Noodzaak van betere afscherming van persoonsgegevens

De ontwikkelingen geschetst in dit hoofdstuk maken duidelijk dat er steeds meer persoonsgegevens worden verzameld en dat persoonsgegevens in toenemende mate een economische waarde vertegenwoordigen. De ontwikkelingen rondom Big Data zullen dit naar verwachting verder versterken. Hierdoor wordt ook duidelijk dat de *incentives* voor bedrijven om persoonlijke gegevens te exploiteren momenteel veel groter zijn dan de *incentives* voor organisaties om voorzichtig en terughoudend om te gaan met het gebruik van persoonsgegevens of het realiseren van voldoende waarborgen om de gebruikte gegevens op adequate wijze te beschermen (ITRE 2011; LE 2010). Het World Economic Forum concludeert dan ook dat als de maatschappij de volledige vruchten wil plukken van de waardecreatie door het gebruik van persoonlijke gegevens, zaken als privacybescherming, vertrouwen, controle en transparantie eerst geadresseerd zullen moeten worden (WEF 2010). Het volgende hoofdstuk biedt inzicht in de mogelijkheden voor privacygerichte online diensten en de ontwikkelingen rondom het wettelijk kader voor privacy en dataprotectie.

3 Privacy by Design

3.1 Inleiding

De trends die in het vorige hoofdstuk zijn geschetst maken duidelijk dat de spelregels rond het omgaan met persoonsgegevens in de datasamenleving aan het veranderen zijn. De digitalisering van de leefwereld leidt tot een explosieve toename van beschikbare persoonsgegevens. Eén van de conclusies van het vorige hoofdstuk was dat er maar weinig domeinen zijn die niet op een of andere wijze te digitaliseren zijn en dat daar steeds vaker en steeds meer persoonsgegevens in het geding zijn. Aan de ene kant leidt personalisering van dienstverlening tot een groei van het dienstenaanbod en het voldoen aan de vraag vanuit consumenten aan op de persoon afgestemde diensten, aan de andere kant wordt daardoor het belang om na te denken over de omgang met de verzamelde gegevens groter. Dit wil niet automatisch zeggen dat privacyoverwegingen dienen te leiden tot het afzien van bepaalde diensten. Zeker waar de consument daardoor aanvullende waarde verkrijgt (want betere op de persoonlijke situatie toegesneden diensten) zal deze bereid zijn daar persoonlijke gegevens voor af te staan. Voor bedrijven is het de vraag hoe de balans rond de omgang met persoonsgegevens eruitziet. Als consumenten er niet om vragen en privacy-incidenten betrekkelijk weinig repercussies op de reputatie van de onderneming hebben, is het verleidelijk om minder strenge voorwaarden aan verzameling, verwerking en benutting van persoonsgegevens te stellen. Tegelijkertijd lijkt het maatschappelijke klimaat van ondernemingen een verantwoorde opstelling te vragen, ook zonder consumentendrang. Dit wordt mede gevoed door incidenten die in de regel op de nodige media-aandacht mogen rekenen. *Privacy by Design* kan bedrijven mogelijk een handvat bieden om op een gestructureerde en systematische manier met persoonsgegevens om te gaan.
Het vorige hoofdstuk liet al zien dat de groeiende hoeveelheid persoonsgegevens consequenties heeft voor de manier waarop die gegevens worden opgeslagen en vervolgens worden beschermd. Nieuwe infrastructuren en diensten zoals *cloud computing* roepen ook nieuwe vragen op over bescherming van persoonsgegevens en het beleggen van verantwoordelijkheden tussen verschillende betrokken partijen. Er komt meer aandacht voor de gevolgen van datalekken.[13] Soms is sprake van het vrijkomen van omvangrijke bestanden met persoonsgegevens. Dit kan ten koste gaan van consumentenvertrouwen.

Op dit speelveld profileren sommige organisaties zich met het aanbieden en/of implementeren van oplossingen die helpen om de privacyrisico's beheersbaar te houden, hetzij door technische oplossingen, hetzij door organisatorische benaderingen, hetzij door een combinatie van verschillende aanpakken. In deze studie richten we ons op deze alternatieve concepten en de stimulerende en remmende factoren voor bedrijven om deze concepten te gebruiken.

In het navolgende staan we eerst stil bij wat we verstaan onder privacy. Privacy en gegevensbescherming worden soms in één adem genoemd. Dat is niet altijd correct. We positioneren beide begrippen ten opzichte van elkaar. We gaan dan verder met de vraag hoe de privacy van personen adequaat beschermd kan

[13] Zie http://webwereld.nl/nieuws/108052/lektober--iedere-dag-een-privacylek-op-webwereld.html

worden. We introduceren het begrip *Privacy by Design* en lichten toe hoe wij dit begrip in het kader van het uitgevoerde onderzoek gebruiken. Dit werken we verder uit in een conceptualisering van *Privacy by Design* en bij een verkenning van wat dit in de praktijk van het onderzoek inhoudt.

3.2 Privacy of bescherming van persoonsgegevens?

In het voorgaande zijn de begrippen (bescherming van) persoonsgegevens (oftewel dataprotectie) en privacy door elkaar gebruikt. Dit suggereert dat beide begrippen uitwisselbaar zijn. Dat is niet het geval. Er zijn enkele cruciale verschillen tussen beide begrippen aan te geven. Het begrip privacy is de lastigste van de twee. Er zijn vele boeken geschreven over wat het begrip privacy inhoudt. Etymologisch komt het begrip 'privacy' van het Latijnse *privare* wat zoveel als beroven betekent. In de Romeinse (en Griekse) tijd was het hebben van publieke functies dé manier om maatschappelijk aanzien te verwerven. Indien iemand beroofd was van deze publieke functies dan daalde zijn maatschappelijke status (vrouwen en slaven kwamen sowieso niet in aanmerking voor publieke functies). 'Privare' heeft daarmee een negatieve klank: beroofd zijn van de mogelijkheid om publiek aanzien te verwerven. Tegenwoordig verwijst het begrip 'privacy' naar de persoonlijke levenssfeer en naar het vermogen om deze levenssfeer in te mogen richten zonder bemoeienis van buitenaf. Dat is een omkering van de oorspronkelijke betekenis. Over de precieze betekenis van het begrip privacy is minder overeenstemming. Er zijn vele dimensies in te onderkennen. Bij wijze van voorbeeld presenteren we de opdeling die Solove hanteert. Hij onderscheidt zes verschillende benaderingen van het begrip privacy (Solove 2008, pp 15 ev):

- het recht om alleen gelaten te worden;
- het kunnen beperken van toegang tot je eigen ik;
- het geheim kunnen houden van bepaalde zaken ('*secrecy*');
- controle uit kunnen oefenen over persoonlijke informatie;
- het mogen beschikken over een eigen persoonlijkheid;
- de mogelijkheid tot intimiteit.

Of deze zes perspectieven een gemeenschappelijke kern hebben, laat Solove in het midden. Afhankelijk van tijd en plaats zal de invulling van deze dimensies verschillen. Wat iemand toelaat en wat niet, zal sterk afhangen van de context, de cultuur, de in gebruik zijnde normen en de persoonlijke ervaringen. Dat maakt het moeilijk om tot een algemeen aanvaarde invulling van het begrip 'privacy' te komen. Dit blijkt onder meer uit de aanpak van de European Court of Justice die in afzonderlijke gevallen bekijkt hoe het begrip privacy gewogen moet worden in de situaties die het voorgelegd krijgt (Gutwirth et al 2011).

Naast deze perspectieven wordt vaak onderscheid gemaakt tussen verschillende dimensies van privacy. Een veel gehanteerd onderscheid is de informationele dimensie van privacy, de ruimtelijke en de lichamelijke. De relationele dimensie die ook genoemd wordt, staat haaks op deze dimensies (Burgoon et al 1989, Westin 1967). De informationele dimensie betreft de gegevens die over een persoon rond gaan, de ruimtelijke dimensie heeft te maken met de privacy van plaats, de lichamelijke dimensie heeft van doen met lichamelijke integriteit. De relationele dimensie betreft de vrije keuze in omgang met derden. Door de toenemende digitalisering wordt de werkingssfeer van de informationele dimensie steeds groter. Een voorbeeld betreft de toenemende verspreiding van ruimtelijke informatie, dat

wil zeggen data over waar je je bevindt. Aanvullende dimensies betreffen de *privacy of action*, waarbij ook de privacy van handelingen beschermd worden (ITRE 2011) en de privacy van gedachten (Finn et al. forthcoming). De basis voor het recht op privacy is onder meer te vinden in het Handvest van de Grondrechten van de Europese Unie (artikel 7) (EG 2000) en de Universele Verklaring van de Rechten van de Mens (artikel 12) (VN 1948).

Waar het begrip 'privacy' naar een inhoudelijk discours verwijst over de verschillende dimensies van privacy (hoe vullen we het recht om alleen gelaten te worden in? hoe wegen we dat ten opzichte van andere rechten?) gaat het bij de bescherming van persoonsgegevens om regels en procedures die duidelijk maken hoe een goede bescherming eruitziet. Dat houdt bijvoorbeeld in dat de verwerker van persoonsgegevens duidelijk aangeeft wat het doel van de verwerking is, hoe invulling wordt gegeven aan de rechten van personen over wie gegevens worden verzameld, dat duidelijk wordt hoe de verwerker het gebruik van de gegevens door derde partijen bijhoudt en dat de verwerker bepaalde kwaliteitsmaatstaven hanteert om de juistheid, compleetheid en actualiteit van de gegevens te garanderen. Bescherming van persoonsgegevens krijgt daarmee een sterk *procedureel* karakter, tegenover het *substantieve* of inhoudelijke karakter van de bescherming van privacy (Gutwirth et al 2010). De basis voor de bescherming van persoonsgegevens is te vinden in de Europese richtlijn EU/95/46 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens' (EC 1995). Deze richtlijn dateert uit 1995. De richtlijn is in Nederland in de Wet Bescherming Persoonsgegevens vertaald. Inmiddels is er een voorstel voor herziening van deze richtlijn (EC 2012). Dit voorstel zet de huidige richtlijn om in een verordening en doet daarnaast verschillende voorstellen voor aanscherping van de bestaande richtlijn. De uitgangspunten voor de bescherming van persoonsgegevens zijn (artikel 5 van de voorgestelde verordening, EC 2012):

1. Wettelijke, eerlijke en transparante manier van verwerking in relatie tot de persoon (het datasubject);
2. voor een gespecificeerd, expliciet en gelegitimeerd doel;
3. met adequate, relevante en tot een minimum beperkte gegevens in relatie tot het doel;
4. die accuraat en up-to-date zijn;
5. die niet langer gehouden worden dan strikt noodzakelijk;
6. onder verantwoordelijkheid van de bewerker en de controller die toeziet op invulling van de juiste rechten voor de datasubjecten.

Deze uitgangspunten voeren nog steeds terug op de *Fair Information Principles* die begin jaren '80 van de vorige eeuw door de OECD zijn vastgesteld (OECD 1980). Ze hebben keuzevrijheid, instemmingsrecht, controle en transparantie als belangrijke uitgangspunten voor iedere gegevensverwerking. Daarmee bieden ze procedurele waarborgen en geen inhoudelijke. Zo kan het doel van een gegevensverwerking zo ruim geformuleerd zijn dat er nog steeds aantasting van de privacy plaatsvindt, en andersom kan de privacy beschermd worden doordat bijvoorbeeld niet voldaan is aan het criterium van accurate, betrouwbare en volledige gegevens.

De begrippen 'privacy' en 'bescherming van persoonsgegevens' staan dus voor twee verschillende benaderingen. Niet alle dimensies van privacy (de mogelijkheid

op intimiteit, bijvoorbeeld) is te vertalen in persoonsgegevens en niet alle aspecten van de bescherming van persoonsgegevens (data-integriteit bijvoorbeeld) zijn van belang voor privacy (onjuiste gegevens zouden de privacy van een individu wel eens beter kunnen beschermen).

3.3 De aanpak van privacybescherming in de praktijk

Verschillende overheidsorganisaties hebben zich uitgesproken over het belang van een goede privacybescherming in de huidige complexe informatiesystemen. De Amerikaanse *Federal Trade Commission* (FTC) stelt in zijn rapport 'Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers' dat bedrijven de privacy van consumenten zouden moeten bevorderen door de gehele organisatie heen en op ieder moment van de ontwikkeling van nieuwe producten en diensten (FTC 2010). De Europese Commissie stelt in de recente Communicatie waarin hij zijn plannen ontvouwt voor de herziening van de databeschermingsrichtlijn uit 1995 in gelijke bewoordingen dat gegevensbescherming ingebouwd moet worden in de gehele levenscyclus van technologieën en procedures, van de vroege ontwerpfase tot aan uitrol en gebruik. (EC 2010). In Nederland is al in een vroegtijdig stadium politieke aandacht geweest voor de verantwoordelijkheid van de overheid in de bescherming van persoonsgegevens die in overheidsinformatiesystemen zijn opgeslagen (motie Nicolai, Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 31).

De invulling van de bescherming gebeurt in de regel langs de volgende twee lijnen:

1. Een bescherming die gericht is op het vergroten van de transparantie van de gegevensverwerking.
2. Een bescherming die gericht is op het tegengaan van misbruik van gegevens.

De eerste vorm staat bekend als privacy management (Gürses et al 2011; door ons vanaf nu aangeduid als *privacy governance*) of *privacy by policy*, (Spiekermann en Cranor 2009). De tweede als privacybescherming (Gürses et al 2011) of *privacy by architecture* (Spiekermann en Cranor 2009).

Er zijn eveneens twee aangrijpingspunten voor de te realiseren bescherming:

1. Via organisatorische maatregelen
2. Via technische maatregelen

Organisatorische maatregelen richten zich op de wijze waarop er binnen een organisatie omgegaan wordt met de verzameling, opslag, verrijking, aggregatie, bewerking en verspreiding van persoonsgegevens. Dit betreft uiteenlopende maatregelen, van het aanstellen van *Privacy Officers* met een specifieke verantwoordelijkheid ten aanzien van de gegevensverwerking, het organiseren van campagnes voor werknemers om een bewuste houding ten aanzien van de omgang met persoonsgegevens te creëren, het expliciet regelen van toegangs- en bewerkingsrechten, tot het houden van audits en het certificeren van bepaalde processen. Technische maatregelen zijn gericht op het verminderen van de hoeveelheid gegevens die verzameld worden (dataminimalisatie), het verhinderen van onbevoegde inzage en bewerking (via toepassing van encryptie), het verminderen van het risico op inbreuken van buitenaf door de bewerkingsprocessen aan de kant van het datasubject te plaatsen, het toepassen van anonimisering, etc. De combinatie van deze twee dimensies levert een matrix op met vier velden (zie Tabel 5).

Tabel 5 Overzicht van maatregelen ter bescherming van privacy

	Transparantie Privacygovernance 'Privacy by policy'	Afscherming Privacybescherming 'Privacy by Architecture'
Organisatorisch	Audits Privacy officers …	Toegang via pseudoniemen Access management …
Technologisch	Log files Data base audit interfaces Transparantietools …	Anonimisering Zero knowledge proofs Client side gegevensverwerking …

Gürses et al (2011) maken zich sterk voor dataminimalisatie als leidend principe. Zij halen Peter Schaar aan, de federale toezichthouder voor gegevensbescherming en vrijheid van informatie in Duitsland, die pleit voor een scherpe focus op het beperken van de te verzamelen en te bewerken gegevens, zo vroeg mogelijk in het proces. Dit sluit aan op het adagium 'Select before you collect' van de Article 29 Working Party (Buttarelli, 2010): gegevens die je niet verzamelt kun je ook niet misbruiken. Het principe van dataminimalisatie is terug te vinden in de Europese richtlijn en de voorgestelde verordening waarin sprake is van "adequate, relevante en niet excessieve gegevensverzameling" (Voorstel voor verordening 2012, preambule 30, p. 22). Gürses et al wijzen er tevens op dat we in de digitale wereld minder gegevens nodig kunnen hebben om een specifieke taak uit te voeren dan in de fysieke wereld. De neiging om juist meer te verzamelen dan strikt nodig is, onder meer omdat de kosten van opslag geen rol van betekenis spelen en "je nooit kunt weten waar je het nog voor kunt gebruiken", is begrijpelijk maar gaat voorbij aan het principe om alleen datgene te verzamelen dat strikt noodzakelijk is voor het – welomschreven en vooraf bepaalde – doel.

Dataminimalisatie als principe vraagt een grote mate van zelfbeheersing aan de kant van de gegevensverzamelende organisaties. Waar persoonsgegevens een steeds belangrijkere rol gaan spelen in het dienstenpakket van dienstenaanbieders is de verleiding groot om meer gegevens te verzamelen dan strikt noodzakelijk is (wederom: "je weet maar nooit") en om ze ook langer te bewaren dan strikt noodzakelijk. Toegesneden technische en organisatorische maatregelen kunnen helpen om dit principe praktische waarde te geven. Toepassing van dataminimalisatie dwingt af dat organisaties zich in een vroeg stadium afvragen hoe ze hun gegevensverzameling in willen richten. Daarmee kan gebruik van gegevens in een andere context ('function creep) ingeperkt worden.

Voor bedrijven zullen in de regel maatregelen voor een goede omgang met persoonsgegevens in de bedrijfsvoering en de te verlenen diensten van belang zijn. Bij de start van het proces, waarin nagedacht wordt over het type dienst dat ontwikkeld gaat worden, het effect dat dit heeft op de positionering van de organisatie, en het strategisch doel dat wordt nagestreefd zal een breder pakket aan belangen de revue passeren. In dat pakket kan ook sprake zijn van een benadering van de privacy van de personen over wie gegevens worden geregistreerd ten behoeve van de dienstverlening of als onderdeel van de dienstverlening. In het belang van de verlening van een dienst zal het soms (steeds vaker) noodzakelijk zijn om persoonsgegevens te verzamelen en te bewerken. De vraag of en zo ja in welke mate dit een ongewenste, bovenmatige of

onrechtvaardige inbreuk op de privacy van de dienstenafnemers betekent is niet in zijn algemeenheid te beantwoorden. Daarvoor is het begrip privacy te complex. *Privacy by Design* kan een handvat bieden om hier op een gestructureerde en systematische manier een antwoord op te vinden. Hoe dat er dan uit ziet, is onderwerp van de volgende paragraaf.

3.4 Privacy by Design: van principe tot methode

De Information and Privacy Commissioner van Ontario, Ann Cavoukian, komt de eer toe het begrip *Privacy by Design* nadrukkelijk op de politieke agenda te hebben geplaatst. De verzamelde toezichthouders hebben op een recente bijeenkomst in Jeruzalem hun fiat gegeven *aan Privacy by Design* als leidend principe bij de bescherming van persoonsgegevens.[14] De daarin genoemde principes zijn overgenomen van het werk van Ann Cavoukian (2009):

1. Proactief en niet reactief; preventie en niet herstel
2. Privacy als default
3. Privacy ingebed in het ontwerp
4. Behoud van volledige functionaliteit; positieve som in plaats van een nulsom
5. *End-to-end* beveiliging – *lifecycle* bescherming
6. Zichtbaarheid en transparantie
7. Respect voor de privacy van de gebruiker

Verschillende principes zijn in het voorgaande aan de orde gekomen. Een aantal verdient nadere toelichting. De proactieve benadering komt in verschillende recente beleidsdocumenten naar voren. Het houdt in dat een organisatie zich vragen stelt over potentiele privacy-implicaties aan de start van het ontwerp van een nieuwe dienst, dat wil zeggen aan de start van de organisatie van het business proces rond deze dienst. Het is als gemeenschappelijk te beschouwen met het tweede en derde principe, waarin privacy als vanzelfsprekend uitgangspunt wordt benoemd en waarin privacy van meet af aan bij het systeemontwerp wordt betrokken. Behoud van volledige functionaliteit wijst erop dat op voorhand goed is nagedacht over systeemfunctionaliteiten en dat dit heeft geleid tot duidelijke keuzes over welke gegevens voor welk doel verzameld worden. Inclusief een goede bescherming van de privacy levert dit geheel een positief resultaat op: de organisatie kan doen wat het wil doen en het individu over wie gegevens verzameld worden weet zijn privacy beschermd. Met name de exclusieve vastlegging van welke gegevens voor welk doel verzameld worden, zal een verandering van de huidige praktijk vergen. De *lifecycle* bescherming voegt het element van de verwijdering/vernietiging van gegevens toe. Hier kan een spanning ontstaan tussen de levenscyclus van de aangeboden dienst en de gegevens die voor de dienst noodzakelijk zijn. Uitbreiding van een dienst met extra functionaliteiten (bijvoorbeeld op basis van nieuwe technologische mogelijkheden) kan tot een conflict leiden met het beleid rond gegevensverzameling en -gebruik. Zichtbaarheid en transparantie zijn al voldoende aan de orde geweest. De betrokkenheid van het datasubject en het expliciteren van respect voor de privacy van het datasubject zijn onderdelen vande rechten die individuen hebben maar dat is slechts één aspect van het respect. Betrokkenheid van het individu bij de systeemontwikkeling, zodat opvattingen van individuen over wie gegevens verzameld worden ook een rol gaat spelen, komt nog weinig voor.

[14] Resolutie over Privacy by Design, aangenomen door de 32nd International Conference of Data Protection and Privacy Commissioners, Jeruzalem 27-29 Oktober 2010.

Het leidt tot ontwerppraktijken die bekend staan als *participatory design* (Steen 2011).

Belangrijke vraag blijft of de principes betrekking hebben op het – vagere – begrip privacy of op de bescherming van persoonsgegevens. In de Amerikaanse en Canadese traditie heeft het begrip privacy een vergelijkbare inhoud als het begrip bescherming van persoonsgegeven in de Europese traditie. Zoals eerder gesteld zijn beide begrippen niet zonder meer uitwisselbaar maar waar Cavoukian spreekt over inbedding van privacy in het ontwerp is het de vraag of zij verwijst naar het begrip privacy of dat het vooral gaat om het begrip persoonsgegeven (en de bescherming daarvan). We veronderstellen dat het maatschappelijk belang van goede waarborgen voor de privacy breder is dan alleen de garantie van een zorgvuldige omgang met verzamelde persoonsgegevens. Dat houdt in dat we een benadering voorstaan die recht doet aan dat belang en privacy in al zijn verschillende dimensies meeweegt. Tegelijkertijd is het voor bedrijven moeilijk om het bredere privacybelang in hun bedrijfsvoering mee te wegen, aangezien zich dit belang soms buiten het blikveld van de dienstverlening bevindt. Wel kunnen bedrijven invloed uitoefenen op de wijze waarop ze met persoonsgegevens omgaan. De vraag in hoeverre er sprake is van een mogelijke inbreuk op de persoonlijke levenssfeer (op de privacy) is voor bedrijven in eerste instantie relevant vanuit de vraag wat met de nieuwe dienst beoogd wordt en wat de potentiele privacy-implicaties van de te verzamelen en bewerken persoonsgegevens zijn. Die risico's zijn niet eenduidig en kunnen ook verschillend van aard en omvang zijn.. Door de verbreding van het gebruik van persoonsgegevens komen andere dimensies van de privacy, zoals ruimtelijke dimensie van privacy (informatie over waar we ons bevinden), de lijfelijke dimensie (integriteit van en zeggenschap over ons lijf) en de handelingsdimensie (wat doen we daar?) steeds meer in het bereik van de informationele dimensie van privacy (de gegevens die over plaats, lijf en handeling verzameld worden). Daarmee krijgt de verzameling, bewerking en verspreiding van persoonsgegevens een grotere lading. Nog steeds kan het dan overigens zijn dat bepaalde privacy-implicaties optreden die niet direct aan deze verzameling, bewerking en verspreiding van persoonsgegevens gekoppeld zijn, bijvoorbeeld wanneer een bepaald beeld van een persoon ontstaat dat geen recht doet aan deze persoon maar wel consequenties heeft die nadelig zijn voor deze persoon.

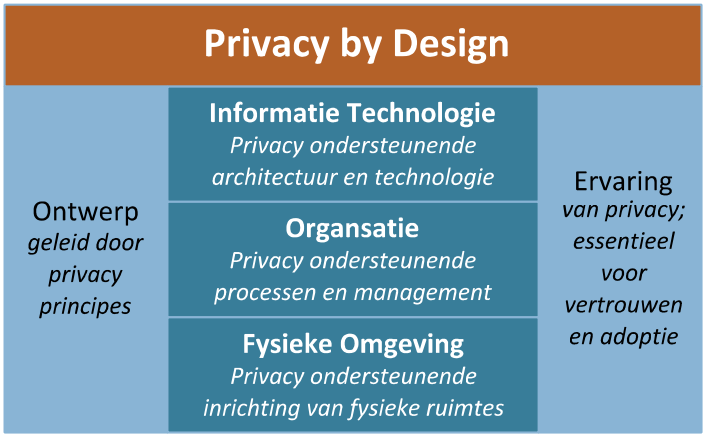
TNO heeft in de afgelopen jaren verder gewerkt aan een concretisering van het concept *Privacy by Design*. Dat heeft geleid tot het identificeren van vijf bouwstenen die een zekere mate van onafhankelijkheid hebben maar die alle vijf nodig zijn om tot een goede invulling *van Privacy by Design* te komen.

Privacy wordt in de Universele Verklaring van de Rechten van de Mens als fundamenteel recht beschouwd. Dit betekent dat privacy tot op zekere hoogte niet uitwisselbaar is met andere rechten (bijvoorbeeld het recht van de pers op vrije nieuwsgaring). De toevoeging 'tot op zekere hoogte' is hier van groot belang. Privacy zal – ook als fundamenteel recht – altijd gewogen worden tegen andere – eveneens fundamentele – rechten. De verandering die we constateren is dat de relatieve positie van privacy op de schaal van fundamentele rechten aan het veranderen is. De bezorgdheid om schending van de privacy blijft onverminderd hoog onder Europese burgers (zie TNS-NIPO 2011), waarbij we de aantekening maken dat het hier gaat om de uitgesproken bezorgdheid. Er is veel gaande in het

onderzoek naar hoe mensen in de praktijk hun privacy waarderen. Dat levert soms het beeld op dat het mensen niet veel uitmaakt wie op welke wijze gebruik maakt van hun persoonsgegevens. Hier is dan weer tegen in te brengen dat aantasting van privacy meer in de toekomst ligt, onverwachts kan zijn en zich moeilijk laat verenigen met een concreet voordeel dat op korte termijn te boeken is (door bijvoorbeeld persoonsgegevens af te staan). We laten deze discussie voor dit moment voor wat die is (zie de uitwerking van de privacyparadox in het tweede hoofdstuk), en concentreren ons op stimulerende en remmende factoren voor de invoering van *Privacy by Design*.

Privacy by Design als methode
We onderscheiden vijf bouwblokken (zie **Error! Reference source not found.**). Ieder van de bouwblokken is te kenmerken op basis van een aantal specifieke tools en methoden.

Figuur 5: Bouwstenen van *Privacy by Design*



3.4.1 *Designfase*

In de designfase komen twee vragen bij elkaar: wat moet het systeem technisch kunnen en wat zijn de risico's op privacy-/identiteitsgebied voor het betreffende systeem? Het ontwerpen van een informatiesysteem verloopt als een strak gestructureerd proces waarin verschillende methoden gevolgd kunnen worden. Doel is om vanuit vastgestelde uitgangspunten (wat moet het systeem kunnen) te werken aan functionele specificaties, deze door te vertalen naar technische specificaties en via prototyping te komen tot een systeemontwerp dat in de praktijk beproefd kan worden.[15] In dit ontwerpproces moet ruimte ingeruimd worden voor vragen met betrekking tot de verzameling, verwerking en verspreiding van persoonsgegevens. Naast het beoordelen van het strategisch belang van de ontwikkeling (de nieuwe dienst bijvoorbeeld) voor de onderneming en de ermee gepaard gaande risico's en kansen, ook met betrekking tot de consequenties voor de privacy van eventuele afnemers, gaat het hier om het eenduidig vaststellen van het doel van de gegevensverzameling en de daarvoor benodigde gegevens. We gaan er dan vanuit dat de eerste beoordeling een 'go' voor de nieuw te ontwikkelen dienst heeft opgeleverd. Die eerste beoordeling – waarin de de privacyrisico's die er

[15] International Council on Systems Engineering, http://www.incose.org/practice/fellowsconsensus.aspx

aan het verzamelen, verwerken en verspreiden van persoonsgegevens vastzit, worden beoordeeld, kan aan de hand van het uitvoeren van een *Privacy Impact Assessment* (PIA) gebeuren.

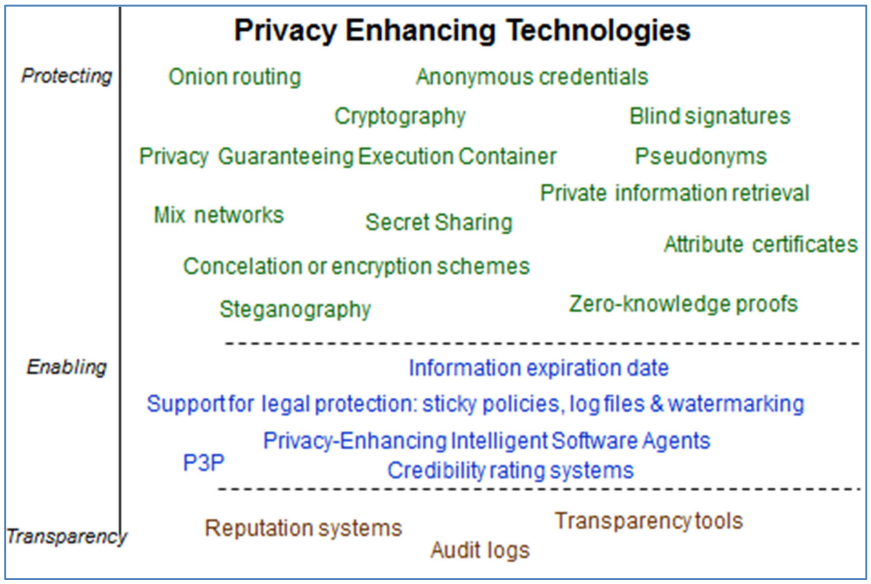
Een PIA is een methode die op een systematische en gestructureerde manier helpt om privacyrisico's inzichtelijk te maken. Er zijn verschillende vormen van PIA's in omloop. Verschillende landen, waaronder de UK, Canada en Australië hebben inmiddels een redelijke expertise op dit gebied opgebouwd (Wright & De Hert 2012). Binnen Europa is er voor RFID een specifieke PIA opgesteld die in principe door bedrijven en organisaties die RFID toepassen in hun bedrijfsprocessen moet worden toegepast. Het bepalen van de privacyrisico's is geen eenvoudige zaak. In Nederland is de Nederlandse Organisatie van Register Accountants betrokken bij het promoten van een PIA standaard. Binnen TNO is meegewerkt aan de realisatie van het raamwerk voor een RFID PIA door de internationale standaardiseringsorganisaties ETSI/CEN en is ervaring opgedaan met de toepassing van PIA in een aantal domeinen.

Het resultaat van de Designfase is een voorstel voor een ontwerp waarin aangegeven is welke privacy- en dataprotectierisico's te verwachten zijn, welk belang de nieuwe dienst voor de organisatie heeft, hoe dit belang gewogen wordt tegen de eventuele privacy-implicaties en welke maatregelen genomen worden om die risico's af te vangen dan wel te verminderen. De maatregelen kunnen zowel technisch als organisatorisch van aard zijn.

3.4.2 Informatietechnologie

De vertaling van de ontwerpparameters naar een technisch systeem vraagt om een vaststelling van de IT-architectuur en van de inzet van technologische middelen om bepaalde privacy- en dataprotectiemaatregelen te implementeren. De vaststelling van de IT-architectuur is sterk contextafhankelijk. De ervaring met de ontwikkeling van privacy-respecterende architecturen is nog beperkt. In de academische literatuur zijn voorbeelden te vinden van specifieke toepassingen van een IT-architectuur, bijvoorbeeld voor het realiseren van een systeem om op elektronische wijze stemmen voor een petitie te verzamelen en voor een systeem dat geschikt is voor rekeningrijden (Gürses et al 2011). Het gaat dan om elementen als dataminimalisatie, anonimisering van persoonsgegevens en het uitvoeren van bewerkingen aan de klantzijde en niet in een centraal systeem. Daarnaast zijn er technieken en methoden die bij kunnen dragen aan het creëren van een grotere transparantie in het systeem. Dat kan door instrumenten aan te bieden die het mogelijk maken bij te houden welke gegevens bewerkt worden, wanneer en door wie. In geven we een overzicht van de verschillende technieken en methoden die te gebruiken zijn.

Figuur 6: Overzicht van technische tools en maatregelen om privacy te beschermen



De *'privacy protecting tools and measures'* helpen bij het afschermen van persoonsgegevens. De *'privacy enabling tools and measures'* helpen bij het reduceren van privacyrisico's, bijvoorbeeld doordat een datum wordt meegestuurd die vastlegt wanneer de persoonsgegevens vernietigd worden. De *'transparency tools and measures'* dragen bij aan het vergroten van de doorzichtigheid van de verzameling, bewerking en verspreiding van de persoonsgegevens.

3.4.3 *Organisatorische maatregelen*

De organisatorische maatregelen betreffen maatregelen die een organisatie treft om een goede naleving van afspraken over het omgaan met persoonsgegevens te realiseren. Daar zijn verschillende instrumenten voor beschikbaar, zoals het aanstellen van een onafhankelijke *Privacy Officer* binnen een organisatie die betrokken is bij de ontwikkeling van nieuwe systemen, toeziet op een goede naleving van privacy- en gegevensbeschermingsregels en daarover rapporteert aan het hogere management, het organiseren van cursussen en campagnes om de bewustheid bij het personeel over privacy en gegevensbescherming te verbeteren, het organiseren van audits om de naleving van privacy- en gegevensbeschermingsregels te controleren en zo nodig voorstellen te doen voor verbetering, en het maken van concrete afspraken rond afhandeling van verzoeken tot informatie, rectificatie en klachten over procedures.

3.4.4 *Ruimtelijke dimensie*

De ruimtelijke dimensie van een gegevensverwerkend systeem is niet in alle gevallen van belang. We doelen hier op het functioneren van een gegevensverwerkend systeem in een bepaalde ruimtelijke omgeving waarbij de opzet en inrichting van het systeem consequenties heeft voor de privacy van individuen. Bij de inrichting van wachtkamers in ziekenhuizen wordt rekening gehouden met deze dimensie. De streep die in vele banken, betaalautomaten en overheidsinstellingen te vinden is en die aangeeft waar de volgende klant/cliënt zich dient op te houden is een ander voorbeeld. Daar waar IT-systemen ook een werkelijk ruimtelijke component hebben wordt het belangrijk om de

privacykenmerken van de ruimtelijke inrichting mee te wegen in het totaalontwerp. Een voorbeeld dat Cavoukian geeft is de *body scan* (tegenwoordig aangeduid als '*security scan*'). Een ruimtelijke scheiding tussen de plek waar de apparatuur staat en waar de informatie wordt uitgelezen vermijdt een directe koppeling tussen het beeld dat gegenereerd wordt en het individu waar dit beeld van afkomstig is. Een andere aanpak voor de bescherming van de privacy is het gebruik van een scanner die alleen vage contouren van het menselijk lichaam geeft waardoor eveneens afstand gecreëerd wordt tussen het individu en zijn beeld. Een ander voorbeeld is de terechtwijzing van Google toen deze met standaardcamera's opnames maakte in Japanse steden voor Google Street View. Door de andere hoogte van hekken in Japanse dorpen en steden maakte Google opnames waarin ook de tuinen te zien waren. Na een terechtwijzing heeft Google de hoogte van zijn camera's aangepast. Dit voorbeeld geeft aan dat met de toename van waarnemingscamera's in de openbare ruimte de fysieke dimensie van de inrichting van deze systemen belangrijker zal worden.

3.4.5 Ervaringen en percepties van personen van wie gegevens geregistreerd worden

De laatste bouwsteen, tot slot, wordt gevormd door de individuen over wie gegevens verzameld worden. Vaak zijn de personen over wie gegevens worden geregistreerd in het geheel niet betrokken bij de ontwikkeling van nieuwe systemen. Er zijn verschillende voorbeelden te geven van problemen in de dienstenontwikkeling omdat er onvoldoende rekening is gehouden met de opvattingen en houdingen van de personen over wie gegevens verzameld en bewerkt wordenf. Facebook is meerdere malen geconfronteerd met protesten van Facebookers over onaangekondigde veranderingen van privacy-instellingen of de lancering van diensten die een inbreuk vormden op de privacy van hun gebruikers.[16] En ook Google heeft aanvullende bescherming moeten bieden toen de Street View dienst onder vuur kwam te liggen in landen als Duitsland en Zwitserland.[17] In Nederland liep de invoering van slimme meters vertraging op door weerstand bij de politiek omtrent de privacyaspecten van deze meter. Die weerstanden zijn in ieder geval ten dele weggenomen, onder meer door gebruikers de mogelijkheid te bieden uit de aangeboden dienst te stappen (*opt-out*). Hoewel het nooit met zekerheid is vast te stellen gaan we ervanuit dat wanneer de datasubjecten van meet af aan betrokken worden bij het ontwerpen van systemen die consequenties kunnen hebben voor hun privacy dit tot systemen en diensten leidt die sneller door consumenten worden benut. Er is nog betrekkelijk weinig ervaring met het betrekken van individuen bij het systeemontwerp. En hoewel het soms lastig kan zijn – bijvoorbeeld bij de bewaking van de openbare ruimte die gericht is op het identificeren van vandalen – kan het een goede zaak zijn om met een groep representatieve individuen na te gaan waar privacyknelpunten zitten.

3.4.6 Conclusie

In dit hoofdstuk hebben we de gedachte achter Privacy by Design geïntroduceerd. We hebben aangegeven dat er een fundamenteel onderscheid is tussen bescherming van persoonsgegevens en privacy. Tegelijkertijd hebben we geconstateerd dat – vanwege de doorgaande digitalisering van steeds meer aspecten van het alledaagse leven – steeds meer dimensies van privacy door

[16] Zie http://ftc.gov/opa/2011/11/privacysettlement.shtm voor een overzicht van acht klachten die de Amerikaanse Federal Trade Commission heeft opgesteld tegen Facebook.
[17] Zie ITRE (2011). 'Does it help or hinder – Promotion of Innovation on the Internet and citizen's Right to Privacy'. Studie uitgevoerd door RAND en TNO voor het Europees parlement. Pp 42 ev.

persoonsgegevens bestreken worden. Bedrijven hebben in eerste instantie te maken met de verwerking van persoonsgegevens. Ook de instrumenten die we geïntroduceerd hebben, en die ofwel gericht zijn op het vergroten van transparantie in het verwerkingsproces ofwel in het vergroten van de afscherming van informatie over een individu, zijn gericht op persoonsgegevens. Inbreuk op de privacy kan de uitkomst zijn. Het instrument ligt in de aanpak van de omgang met persoonsgegevens. Dit instrument hebben wij uiteengelegd in een vijftal bouwblokken die tezamen het concept *Privacy by Design* vormen. Zoals het begrip aangeeft, ligt er een groot accent op de ontwerpfase, wanneer er nagedacht wordt over nieuwe diensten. Dan moet ook nagegaan worden welke technische en organisatorische maatregelen kunnen worden ingezet. Het datasubject speelt tot op heden een bescheiden rol bij dit ontwerpen en handhaven. Ervaringen en percepties van de personen van wie gegevens worden geregistreerd spelen in onze benadering evenwel ook een rol. De ruimtelijke dimensie speelt soms een rol. Dan gaat het over de digitale equivalent van de streep in de wachtkamer. De borging van privacy en bescherming van persoonsgegevens in de Universele Verklaring van de Rechten van de Mens maakt dat deze rechten niet makkelijk opzij gezet kunnen worden. Wel zal altijd sprake zijn van weging van uiteenlopende rechten en mogelijkheden voor organisaties voor uitbreiding van hun dienstenaanbod.

4 Privacy by Design: meten van diffusie en adoptie

4.1 Inleiding

In het vorige hoofdstuk hebben we de gedachten achter *Privacy by Design* uiteengezet. Uit die uiteenzetting kwam naar voren dat het concept *Privacy by Design* door verschillende instanties omarmd wordt als manier om privacy van personen van wie gegevens worden geregistreerd te beschermen. Vanuit de optiek van het bedrijfsleven zal dit belang van een goede privacybescherming worden gewogen tegen andere belangen. Privacy is één van de factoren waar bedrijven mee te maken hebben bij de vormgeving van hun bedrijfsprocessen. Naarmate de bescherming van privacy nauwer aansluit op andere bedrijfsdoelstellingen en ook eenvoudiger te realiseren is, zal de keus voor invoering van privacybeschermende processen en technologieën eerder gemaakt worden dan wanneer dit veel moeite kost, de opbrengsten gering zijn en het ook niet duidelijk is wat er precies moet gebeuren. Personalisering van dienstverlening vraagt om beheer en bewerking van persoonsgegevens. Als consumenten om privacybescherming vragen en dit zwaar mee laten wegen in de keuze voor een dienstenaanbieder geeft dit een duidelijk signaal af. En andersom. De omgeving waarbinnen bedrijven opereren en waarin privacy een rol speelt, is een complexe. Het in kaart brengen van remmende en stimulerende factoren voor invoering van *Privacy by Design* verduidelijkt het speelveld waarop bedrijven acteren. We benaderen *Privacy by Design* als een innovatie, als een vernieuwing die bedrijven al dan niet overnemen. De motivering om een innovatie in de bedrijfsvoering op te nemen zal van verschillende factoren afhangen. Als een vernieuwing een duidelijk voordeel lijkt te bieden zal deze eerder worden opgenomen dan wanneer de voordelen onduidelijk zijn. Zijn er vooral remmende factoren dan is het zeer de vraag of bedrijven de vernieuwing overnemen. In dit hoofdstuk zetten we het methodisch raamwerk uiteen dat we hebben gebruikt om de remmende en stimulerende factoren rond *Privacy by Design* in kaart te brengen.[18]

4.2 Diffusie van innovaties

Een innovatie is “een idee, een praktijk of een object dat als nieuw wordt ervaren door een individu of een andere eenheid van adoptie.” (Rogers 2003). Een adoptie is “een beslissing om volledig gebruik te maken van een innovatie op de best mogelijke manier.” (Rogers 2003). Een innovatie kan allerlei zaken betreffen en is – volgens de definitie – breder dan alleen maar de ontwikkeling van een nieuw product. Zolang een individu, een groep, een organisatie, een samenleving het idee, de praktijk, de dienst of het product als nieuw beschouwt, is deze aan te duiden als een innovatie. Freeman en Perez maken onderscheid in typen innovatie en spreken over incrementele en radicale innovaties (Freeman en Perez 1988). Een incrementele innovatie is een innovatie die iets toevoegt aan een al bestaand product of dienst (of praktijk of idee) terwijl een radicale innovatie fundamenteel vernieuwender is. Zij plaatsen hun innovatietheorie in het perspectief van nieuwe maatschappelijke ordeningen die met enige regelmaat zichtbaar worden en die te

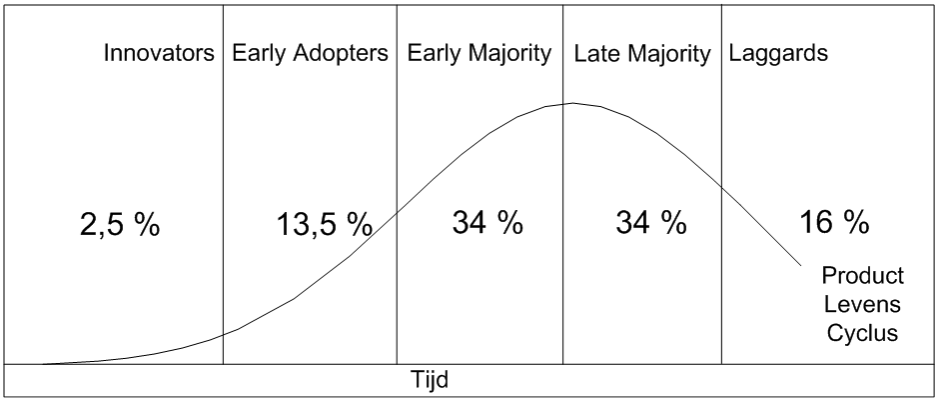
[18] De aanpak die we hieronder presenteren is in grote lijnen vergelijkbaar met de aanpak die John Borking in zijn proefschrift presenteert. Wij voegen er de analyse in termen van imperfecties inde markt en in innovatiesystemen aan toe (zie Borking 2010, met name hoofdstuk 7).

relateren zijn aan de fundamentele kenmerken van een sleuteltechnologie (Freeman & Perez 1988, Perez 2001). Voor de huidige periode is de chip (formeel: het *integrated circuit*) de sleuteltechnologie. In hun benadering komt een innovatie nooit alleen maar is sprake van een grotere omwenteling van elkaar beïnvloedende economische, technische en institutionele factoren. Deze techno-economische benadering van innovatie is bijvoorbeeld herkenbaar in de ontwikkelingen die we in het eerste hoofdstuk hebben geschetst over een nieuw systeem van diensten die gebruik maken van persoonsgegevens.

De benadering die Rogers voorstaat is praktischer van aard dan de benadering van Freeman en Perez en voor ons doel beter te gebruiken. Het conceptuele kader dat Rogers over een aantal decennia heeft opgebouwd en waarvan de oorsprong in de jaren zestig van de vorige eeuw ligt, geeft een aantal factoren dat van invloed is op de diffusie en de adoptie van een innovatie. Een diffusie is “het proces waardoor een innovatie gecommuniceerd wordt langs bepaalde kanalen gedurende een bepaalde tijd onder leden van een sociaal systeem.” (Rogers 2003). We geven deze definities zo precies weer omdat ze aangeven dat het innovatie-diffusiesysteem van Rogers gebaseerd is op een solide conceptueel raamwerk rond innovatie- en diffusieprocessen.

Privacy by Design kan in de optiek van Rogers beschouwd worden als een innovatie. Het betreft een combinatie van ideeën, nieuwe praktijken en nieuwe objecten die door een individu of een organisatie als nieuw ervaren wordt. Rogers maakt onderscheid tussen verschillende dimensies aan een innovatie. Hierboven is al gesproken van de innovatie zelf, de kanalen waarlangs de innovatie verspreid wordt en het adoptieproces. Daarnaast heeft Rogers verschillende categorieën van personen, groepen of organisaties die een innovatie adopteren onderscheiden. Van hem is ook de bekende adoptiecurve afkomstig die aangeeft dat een innovatie na een langzame start (adoptie door ‘voorlopers’) plotsklaps omarmd wordt door een grote groep ‘volgers’ waarna een innovatie een verzadiging bereikt waarin ‘achterlopers’ aansluiting vinden of definitief afzien van adoptie. Er is in de benadering van Rogers geen sprake van een noodzaak tot adoptie. De terminologie is in zekere zin ongelukkig gekozen omdat bijvoorbeeld de aanduiding ‘achterlopers’ suggereert dat dit een groep is die de voordelen van de innovatie nog niet ziet en dus nog ‘achterloopt’. Als je nog niet begrijpt dat een innovatie goed voor je is, moet je maar wachten tot je ‘het licht ziet’. Een dergelijke normatieve insteek kiest Rogers niet, hoewel de terminologie wel die indruk wekt.

Figuur 7 Adoptiecurve (Rogers 2003)



Vanuit andere perspectieven is het proces van adoptie verder bestudeerd (Punie 2000; Silverstone & Haddon 1996, Frissen & Van Lieshout 2006). De adoptie van een technisch artefact wordt door deze wetenschappers beschouwd als een proces van 'domesticatie' ofwel het opnemen van een nieuw element in het geheel van dagelijkse routines en handelingspraktijken van een individu of organisatie. Die domesticatie doorloopt verschillende stadia, aangeduid als 'commodificatie', 'appropriatie' en uiteindelijk 'conversie' (Silverstone & Haddon 1996). In deze benadering wordt verondersteld dat de betekenis van nieuwe producten, diensten, ideeën, etc. verandert gedurende een adoptieproces. De 'commodificatie' gebeurt in het ontwerpproces waarin ontwerpers een betekenis meegeven aan een nieuw product of dienst. In de appropriatiefase eigent een individu of een organisatie zich een innovatie toe. In de conversiefase is de innovatie zodanig ingeburgerd dat hij tot het gewone handelingspatroon van individu of de organisatie is gaan behoren. Dit laatste stadium is bij *Privacy by Design* vermoedelijk nog maar sporadisch aan de orde. Daarvoor is PbD nog een te nieuw concept. Het gaat momenteel vooral om het proces van de toe-eigening. Hoe gaat dat? Welke stimulerende en remmende factoren zijn in dit proces te onderkennen?

4.2.1 Productkenmerken

Volgens Rogers zijn de volgende vijf productkenmerken van belang voor het al dan niet slagen van een innovatie:

1. Relatieve voordeel: biedt acceptatie van de innovatie een voordeel dat voldoende groot is ten opzichte van de bestaande praktijk om opname van de innovatie te billijken?
2. Inpasbaarheid: Sluit de innovatie goed aan op bestaande systemen, procedures en routines?
3. Complexiteit: Is de innovatie lastig en ingewikkeld of eenvoudig en simpel in te voeren?
4. Uittesten: kan de innovatie/kunnen onderdelen van de innovatie uitgetest worden alvorens hem op te nemen of is dat niet mogelijk?
5. Zichtbaarheid: is invoering van de innovatie zichtbaar voor de organisatie en voor anderen buiten de organisatie? Met andere woorden: kan een organisatie zich via de innovatie beter profileren dan voorheen?

Dit zijn allemaal kenmerken die iets zeggen over de innovatie zelf. Niet altijd zullen deze productkenmerken eenduidig en op voorhand vast te stellen zijn. Het gaat bij deze kenmerken dan ook niet om objectief vast te stellen kenmerken maar om de *gepercipieerde* productkenmerken: heeft een organisatie de indruk dat invoering van *Privacy by Design* voordelen biedt, dat invoering van *Privacy by Design* eenvoudig te realiseren is in de bestaande structuren en dat het goed aansluit op al bestaande procedures, routines en processen. Het kunnen uittesten van (onderdelen van) *Privacy by Design* is een kenmerk van een innovatie die bijvoorbeeld door systeemleveranciers geboden kan worden, maar zal ook afhankelijk zijn van bestaande systemen, processen en procedures. Zichtbaarheid van een innovatie is niet altijd duidelijk. Een nieuwe i-Pad kun je aan je vrienden laten zien maar een programmaatje dat cookies verwijdert, kun je niet zo makkelijk tonen.

4.2.2 Innovatieprocessen bij organisaties

Naast productkenmerken spelen houdingen, opvattingen, kennis en sociaal-economische achtergronden een rol. Via het *Technology Acceptance Model* (Davis 1993; Davis & Venkatesh 1996; Chuttur 2009) wordt voortgebouwd op het model

van Rogers en is ook een vertaalslag te maken naar organisaties als eenheden die innovaties adopteren. Voor onze studie naar de stimulerende en belemmerende factoren voor de adoptie van *Privacy by Design* is de organisatie als analyse-eenheid voor de hand liggender dan de adoptie door individuen binnen een organisatie. Dat neemt niet weg dat bijvoorbeeld de rol van het hoger management en leiderschap gewicht in de schaal legt en ook onderzocht moet worden. We komen daar op terug.

Bij een organisatie wordt het beslismodel voor adoptie van een innovatie in twee fasen onderscheiden: initiatie en implementatie (Schurink 2006, p 184). Bij de initiatiefase spelen percepties over de te verwachten karakteristieken van de innovatie een belangrijke rol. In de implementatiefase wordt de innovatie daadwerkelijk geïmplementeerd en vindt een terugkoppeling naar de oorspronkelijke percepties plaats: voldoet de innovatie aan de verwachtingen, moeten verwachtingen worden bijgesteld, is de innovatie inpasbaar in de organisatorische routines, welke onvoorziene consequenties heeft de implementatie, etc. De daadwerkelijke adoptie vindt plaats tussen initiatie- en implementatiefase, aldus Schurink. De initiatie- en implementatiefase vertonen een overeenkomst met de appropriatie- en conversiefase die we eerder hebben geschetst.

Het model dat Rogers heeft opgesteld en de aanvullingen daarop die we hierboven besproken hebben toch vooral oog voor de interne en sociale karakteristieken van het innovatieproces (percepties van individuen en organisaties, gepercipieerde voordelen binnen bestaande processen) en hebben minder oog voor de omgeving waarbinnen organisaties moeten opereren. Sommige auteurs stellen voor om de externe omgeving explicieter mee te nemen als verklarende factor waarom bepaalde innovaties wel en andere niet geadopteerd worden. Schurink verwijst naar het *Technology-Organisation-Environment* model dat door Tornatzky en Fleischer is opgesteld (Schurink 2006, p. 187). De technologische context betreft de al aanwezige systemen en technologische kennis binnen de organisatie en zegt iets over de mate van radicaliteit van mogelijke vernieuwingen. Ze sluiten daarmee aan op de benadering van Freeman en Perez. De organisatorische context betreft zowel objectieve als subjectieve factoren. Naast objectief vaststelbare factoren zoals bedrijfsgrootte, arbeidsdeling binnen een organisatie en mate van formalisering van bedrijfsprocessen, spelen ook subjectievere factoren zoals aard van het leiderschap (openstaand voor vernieuwing of juist afhoudend), aard en kwaliteit van het personeel (kennisniveau, vernieuwingsbereidheid, loyaliteit) en interne communicatiekanalen (open of gesloten, formeel of informeel) een rol. De omgeving heeft betrekking op de bedrijfstak waarbinnen de organisatie functioneert, de competitie die de organisatie ondervindt en de rol van de overheid. Voor de houding tegenover innovatie zijn twee factoren van belang: de marktomgeving met factoren als de competitiviteit van de markt, de relatie met toeleveranciers, de maturiteit van de bedrijfstak en de mate van onzekerheid van de bedrijfsomgeving; daarnaast de aanwezigheid van een infrastructuur voor technologische ondersteuning, bestaande uit onder meer het kennisniveau van de werknemers, de regulerende rol van de overheid en de arbeidskosten (Schurink 2006, p. 188).

De verschillende modellen rond diffusie en adoptie van innovatie zijn in verschillende studies empirisch getoetst. Schurink heeft in een overzichtsartikel de resultaten van de verschillende empirische studies op een rij gezet. Het betrof hier

studies die zich richtten op de verspreiding en adoptie van EDI (*Electronic Data Interchange*, ofwel Elektronisch Berichtenverkeer). De aard en het belang van deze innovatie zijn anders dan die voor *Privacy by Design*, maar de resultaten geven wel een interessant beeld over factoren die van belang zijn voor adoptie en over een verklaring voor het belang van deze factoren.
Er worden drie categorieën van factoren onderscheiden:

- Kenmerken van de innovatie
- Kenmerken van de organisatie
- Kenmerken van de omgeving

Met betrekking tot de innovatie is de conclusie dat de factoren die Rogers aangeeft van belang blijken te zijn. Gepercipieerd voordeel speelt een positieve rol, evenals compatibiliteit. Naarmate een innovatie als complexer gezien wordt, is ook de innovatiebereidheid minder.

Met betrekking tot de organisatie is de conclusie dat *organisational readiness*, de mate waarin een organisatie klaar staat om een innovatie te ontvangen, een belangrijke verklarende factor voor de innovatiebereidheid is. *Organisational readiness* hangt onder meer af van de wijze waarop het management de vernieuwing percipieert en deze al dan niet ondersteunt, van de kennis en vaardigheden van de mensen die te maken krijgen met de consequenties van invoering van een nieuw systeem of proces, en van het gemak waarmee enn vernieuwing in de bestaande processen en systemen is in te voeren. *Organisational readiness* is belangrijker dan de gepercipieerde voordelen van een innovatie. Organisatiefactoren als bedrijfsgrootte zijn eveneens van belang: uit de literatuur volgt dat een groter bedrijf eerder in staat is om een innovatie in zijn bedrijfsvoering op te nemen dan een klein bedrijf. Schaal werkt hier klaarblijkelijk positief op de mogelijkheden tot adoptie van een innovatie.

Met betrekking tot de omgevingskenmerken is de conclusie dat de omgeving een belangrijke invloed heeft op het adoptieproces. De relatie werkt twee kanten uit: wanneer handelspartners een innovatie opnemen dan groeit de druk bij anderen om dit ook te doen. Dwang tot innoveren heeft daarentegen eerder een negatief effect: wanneer kleine bedrijven onder dwang van grote bedrijven besluiten tot implementatie van een innovatie werkt dit in de regel niet gunstig uit voor het kleine bedrijf. De voordelen komen vaak ten goede van het grote bedrijf.

We geven deze conclusies in hoofdvorm weer. Twee kanttekeningen zijn op zijn plaats. Ten eerste, de verschillende empirische studies lopen nogal uiteen in hun hoofdconclusies. Wat we hierboven als hoofdlijnen presenteren kan voor de afzonderlijke studies anders liggen. Ten tweede, de relaties zijn gevonden voor een specifieke innovatie, namelijk de invoering van Elektronisch berichtenverkeer. De gevonden relaties zullen tot op zekere hoogte ook voor invoering van *Privacy by Design* gelden maar de motieven en houdingen van de verschillende partijen kunnen met betrekking tot invoering van *Privacy by Design* anders liggen dan bij EDI. Daar zullen we alert op moeten zijn.

4.3 Het gehanteerde model voor diffusie van PbD-innovaties

Het model dat wij voor deze studie zullen gebruiken bouwt in grote lijnen voort op de innovatie-diffusiemodellen die we hierboven besproken hebben. Het model

verenigt bestaande opvattingen over kenmerken van innovatieprocessen bij individuen en organisaties in zich. De basis van ons model wordt gevormd door de *Unified Theory of Acceptance & Use of Technology* (Venkatesh et al 2003). Dit model bouwt voort op het eerder besproken Technology Acceptance Model en incorporeert de inzichten uit het diffusie-innovatiewerk van Rogers. Het UTAUT-model beoogt – zoals de naam aangeeft – de bestaande opvattingen over adoptie en gebruik van nieuwe technologieën bijeen te brengen en te verenigen. Het model is gebaseerd op vier kernbegrippen:

- *Performance expectancy*: de mate waarin potentiele adopters (het management) verwachten dat de innovatie zal bijdragen aan betere prestaties van de organisatie c.q. zal bijdragen aan het realiseren van de bedrijfsdoelstellingen.
- *Effort expectancy*: de mate waarin adopters verwachten dat de innovatie makkelijker of moeilijker te gebruiken is c.q. de inspanning die geleverd moet worden om de innovatie in te voeren in de organisatie.
- *Social influence*: de mate waarin factoren uit de directe (organisatie) en bredere (samenleving) omgeving van invloed zijn op al dan niet adoptie van een innovatie
- *Facilitating conditions*: de voorwaarden in de directe (organisatie) en bredere (samenleving) omgeving die bijdragen aan de adoptie van een innovatie.

Waar het UTAUT kiest voor individuele kenmerken (gender, leeftijd, ervaring en bereidheid tot adoptie) als invloedrijke factoren hebben wij dit in ons model uitgewerkt naar organisatiekenmerken (zie hieronder). Voor onze benadering hebben we het UTAUT model aangepast en ingebed in een model waarin we vanuit drie perspectieven naar een innovatie kijken (zie ook Borking 2010):

- Innovatiekenmerken (*Performance expectancy* en *effort expectancy*)
- Organisatiekenmerken (faciliterende voorwaarden en invloedrijke omgevingsfactoren)
- Kenmerken van de externe omgeving (eveneens uitgesplitst in faciliterende voorwaarden en invloedrijke omgevingsfactoren).

Bij de organisatiekenmerken ruimen we een bijzondere plaats in voor de maturiteit van een organisatie met betrekking tot de beheersing van risico's die voortkomen uit het omgaan met persoonsgegevens.. Hierin koppelen we het Privacy Maturiteitsmodel (PMM) aan de organisatiekenmerken die in de innovatie-diffusieliteratuur worden genoemd. Het Privacy Maturiteitsmodel is een model dat is opgesteld met het van de Carnegie Mellon Universiteit afkomstige Capability Maturity Model (CMM) in het achterhoofd. Het CMM geeft inzicht in de maturiteit van een organisatie bij het invoeren van nieuwe softwaresystemen (Humphry 1989). Het Privacy Maturity Model geeft een systematische benadering voor de wijze waarop een organisatie gepercipieerde risico's in de bedrijfsvoering tracht te ondervangen. In dit geval betreft het risico's die vertaald kunnen worden naar privacy-aspecten. Maar in wezen gaat het om risicopercepties met betrekking tot processen en systemen waarin persoonsgegevens worden bewerkt.[19] In ons onderzoek hebben we hier uiteindelijk relatief weinig aandacht aan kunnen

[19] Zie http://www.cica.ca/service-and-products/privacy/gen-accepted-privacy-principles/index.aspx

besteden.[20] Omdat het PMM ook iets verduidelijkt over de adoptie van een innovatie (in organisatorische, technische, institutionele of beleidsmatige zin) en over stimulerende en remmende factoren stellen we het in dit hoofdstuk kort aan de orde.

De drie invalshoeken van UTAUT beoordelen de verschillende dimensies aan een innovatie die we in het voorgaande aan de orde hebben gesteld. In Appendix 2 Overzicht adoptiefactoren' staan de elementen van het raamwerk dat we hebben opgesteld en gebruikt in ons onderzoek vermeld. Bij de *Performance expectancy* komen de indicatoren aan de orde die Rogers heeft benoemd (relatieve voordeel, zichtbaarheid en testbaarheid; de laatste factor is buiten beschouwing gebleven in het onderzoek). Daarnaast zijn indicatoren opgenomen die verwijzen naar hoe de innovatie bij kan dragen aan het realiseren van de bedrijfsdoelstellingen). Dit betreft indicatoren zoals financiële impact, toename verkoop en toename vertrouwen klanten. Een derde categorie indicatoren betreft de efficiëntie- en effectiviteitswinst die te boeken is door de innovatie. Hier gaat het om toename in de efficiëntie in gegevensbewerking, de (gepercipieerde) effectiviteit in het bepalen en aanpakken van privacyrisico's en aansprakelijkheid. Bij *Effort expectancy* zijn indicatoren gekozen die iets zeggen over de moeite die het kost om de innovatie in de organisatie in te passen. Dit betreft indicatoren als compatibiliteit met bestaande processen, complexiteit van invoering en gepercipieerde uitvoerbaarheid van de geplande innovatie.

De faciliterende voorwaarden bij organisaties hebben als belangrijkste indicatoren houding en percepties bij medewerkers en management van de organisatie. Dit is uitgewerkt in bewustzijn bij het (top-)management voor de beschikbaarheid en het eventuele nut van privacymaatregelen, de mate van ervaring met deze maatregelen (dan wel het ontbreken daarvan), de gepercipieerde privacyrisico's (de mate waarin de kans dat het risico optreedt als hoog of laag wordt ingeschat), de mate waarin het management op de hoogte is van wetten en regels rond privacy, en het bewustzijn bij het (top-)management over de gevolgen van het introduceren van PbD binnen de organisatie. Zoals al eerder is geconstateerd zijn ook kenmerken van de organisatie van belang, zoals bedrijfsgrootte. Kleine bedrijven hebben meer moeite met het inschatten van alle risico's en gevolgen, maar kleine bedrijven kunnen aan de andere kant ook sneller en flexibeler omgaan met de introductie van nieuwe maatregelen omdat de hiërarchie geringer is en de besluitvorming sneller en effectiever kan verlopen. Naast deze bedrijfskenmerken gaat het om de complexiteit van de IT-infrastructuur en soort en omvang van de gegevens die worden verwerkt. Een factor die mee kan wegen maar die in dit onderzoek buiten beschouwing is gebleven is de aanwezigheid van sleutelpersonen binnen de organisatie, dat wil zeggen personen met een specifieke houding tegenover PbD die ook in de buitenwereld als zodanig worden herkend. De sociale beïnvloeding is gemeten aan de hand van één indicator, namelijk de mate waarin de betreffende organisaties banden hebben met toezichthouders en adviserende instellingen en organisaties over te treffen privacymaatregelen.

De faciliterende voorwaarden in de externe omgeving is in drie indicatoren vervat die met de wet- en regelgeving te maken hebben: de manier waarop de

[20] Het PMM maakt onderscheid in verschillende' stadia van maturiteit. Er bleek weinig bereidheid te zijn bij de respondenten om ook daadwerkelijk informatie aan te leveren die te interpreteren was in de context van dit Privacy Maturiteitsmodel. Zie verder Appendix 1 Het Privacy Maturiteitsmodel.

toezichthouders hun rol invullen, de (gepercipieerde) complexiteit van de wet- en regelgeving voor de organisatie, en de ervaren druk om aan wet- en regelgeving te voldoen. Daarnaast spelen de mate waarin consumenten ook om PbD-maatregelen vragen (of het gebrek aan vraagarticulatie bij consumenten) een rol en tot slot de mate waarin PbD-oplossingen te verkrijgen zijn. De sociale beïnvloeding is weer in één indicator samengevat: de mate waarin concurrenten en partners van de organisatie gebruik maken van PbD-oplossingen.

4.3.1 Relatie van indicatoren met PbD raamwerk

De indicatoren die in de voorgaande paragraaf zijn benoemd, geven een overzicht van de remmende en stimulerende factoren waar organisaties mee te maken hebben als zij maatregelen in de omgang met persoonsgegevens in willen voeren. In dit onderzoek zijn deze maatregelen samengebracht onder de noemer *Privacy by Design* (PbD). In hoofdstuk 2 is aangegeven wat wij hieronder verstaan, en uit welke bouwstenen PbD in onze benadering is opgebouwd. PbD als concept is nog in ontwikkeling; er is geen vaststaande omschrijving of definitie van voorhanden. De benadering die wij voorstaan onderscheidt verschillende bouwstenen die ieder voor zich weer bestaan uit methoden, technieken en tools. Onze onderverdeling op hoofdlijnen maakt onderscheid tussen methoden, technieken en tools

- die ingezet kunnen worden bij de ontwerpfase van een nieuw systeem (de keuze voor een nieuwe dienst en de bijbehorende ontwikkeling van de IT-architectuur),
- die gebruikt kunnen worden voor de beveiliging van gegevens binnen een systeem (de privacytools),
- die de organisatorische veranderingen die nodig zijn begeleiden
- die oog hebben voor de ruimtelijke dimensie van privacy
- waarmee ervaringen, houdingen en percepties van de personen van wie gegevens worden geregistreerd worden betrokken bij systeemontwerp, -ontwikkeling en gebruik.

Waar de ruimtelijke dimensie van privacy een apart fenomeen is dat we voorlopig buiten beschouwing laten, zijn de andere vier bouwstenen herkenbaar in de innovatieprocesbenadering die we in dit hoofdstuk hebben uitgewerkt. De drie hoofddimensies: innovatiekenmerken, organisatiekenmerken en kenmerken van de externe omgeving, zijn te relateren aan respectievelijk de IT-architectuur en de privacytools (de eerste twee bouwstenen), de organisatie (derde bouwsteen) en de personen van wie gegevens worden geregistreerd (vijfde bouwsteen). De laatste dimensie hebben wij niet op directe wijze bestudeerd maar hebben we indirect via percepties en attitudes van werknemers en leiding/(top)management meegenomen in de indicatoren van het raamwerk. In het onderzoek hebben we *Privacy by Design* als een op zich staand concept benaderd waarbij we een werkdefinitie hebben gehanteerd die de elementen van PbD als innovatief concept benoemt. Via de benadering van *Privacy by Design* als integrerend concept hebben we tevens onderzocht of er specifieke stimulerende en remmende factoren te vinden zijn voor ieder van de afzonderlijke componenten. Waar van toepassing zullen we de resultaten voor de afzonderlijke dimensies aan de orde stellen.

4.3.2 Stimulerende en belemmerende factoren in invoering van Privacy by Design

In een omvangrijke studie, uitgevoerd in 2010 voor de Europese Commissie, heeft London Economics (LE) onderzocht welke stimulerende en belemmerende krachten te onderscheiden zijn bij de innovatie en adoptie van Privacy Enhancing Technologies (PETs) (London Economics 2010). In ons raamwerk van Privacy by

Design vallen PETs onder de technische oplossingen. Doel van PETs is in de regel het versleutelen van persoonlijke gegevens, het anonimiseren en/of pseudonimiseren van persoonsgegevens, en het verheimelijken van routes die persoonsgegevens afleggen. Dit is wat wij *Privacy by Architecture* hebben genoemd. Daarnaast worden PETs ontwikkeld die bijdragen aan vergroting van transparantie en die toestemmingsmechanismen ondersteunen. Dit hebben we *Privacy by Policy* oplossingen genoemd (zie Hoofdstuk 3). In zijn onderzoek, gebaseerd op desk research, interviews en uitgezette questionnaires komt LE tot een lijst van stimulerende en belemmerende factoren voor de introductie van PETs (zie Tabel 6).

Tabel 6 Overzicht stimulerende en remmende factoren invoering van PET (bron: LE 2010)

Stimulerende factoren	Remmende factoren
Vraag vanuit consumentenzijde	Gebrek aan politieke noodzaak
Noodzaak vanuit wet- en regelgevende kaders	Weigering van consumenten om te betalen voor PETs
Onderscheidend vermogen door gebruik van PETs	Acceptatie door consumenten van huidige privacy en gegevensbeschermings risico's
Vermindering van risico op ongewenste gegevensverspreiding	Verondersteld gebrek aan economisch voordeel voor ondernemingen
Aantoonbare compliance met wet- en regelgeving	Beperkt begrip bij ondernemingen van PETs
Vermindering kosten compliance	Veronderstelde noodzaak voor training en het inhuren van nieuwe expertise
Vermindering kosten van herstel door schending van privacy/gegevensbescherming	De 'value for money' die met invoering van PET wordt geassocieerd
	Complexiteit van de technologie
	Gebrek aan informatie hoe om te gaan met de invoering van PETs
	Beperkte toepasbaarheid van PETs voor verschillende soorten ondernemingen
	Grootte van de onderneming
	Onbekendheid van organisaties met PET
	Noodzaak van hernieuwde investeringen door onderhoud/upgrading van PETs
	Vaste kosten voor de invoering van PETs

Uit Tabel 6 komt naar voren dat veel stimulerende factoren te maken hebben met winsten die op termijn ingeboekt kunnen worden maar waarvan de opbrengsten onzeker zijn (zowel in omvang als in mate van zekerheid dat de opbrengst ook op zal treden). Bij de remmende factoren speelt eveneens de perceptie met betrekking tot eventuele kosten in de toekomst een belangrijke rol. Daarnaast zijn verschillende remmende factoren gerelateerd aan de situatie zoals die nu is, en zoals die nu wordt verondersteld te zijn. Bij een deel van de eerste soort remmende factoren (voorbeeld 'gebrek aan informatie') is sprake van informatieachterstand of gebrek aan gerichte informatie. Dit soort remmende factoren kan weggenomen worden door aanbod van gerichte informatie. Uit de tabel volgt dat sommige factoren voor kleinere bedrijven belangrijker zullen zijn dan voor grote. Informatieachterstand is voor sommige bedrijven op te lossen door inhuur van de

juiste expertise maar kleinere bedrijven zullen hier door gebrek aan noodzakelijke middelen eerder in problemen kunnen geraken dan grote.

De stimulerende en remmende factoren die uit het LE-onderzoek naar voren komen, liggen in het verlengde van de factoren die adoptie bevorderen dan wel afremmen. In het volgende hoofdstuk zullen we de overeenkomsten en de verschillen van ons eigen onderzoek met het LE-onderzoek aangeven..

4.4 Imperfecties in markten en in innovatiesystemen

De resultaten van het empirisch onderzoek (interviews) zullen we duiden met behulp van een raamwerk voor dat imperfecties van markten en innovatiesystemen benoemd. Dit raamwerk vindt veel toepassing in een beleidscontext (Poel en Kool 2009; Poel, Kool en van der Giessen 2009) . De imperfecties in de markt zijn afgeleid uit de neo-klassieke economie (Gustafsson en Autio 2006) en verwijzen naar imperfecties bij het ontstaan of het functioneren van een markt, dat wil zeggen een plaats waar vraag en aanbod van diensten en producten bij elkaar komt. Deze imperfecties kunnen optreden bij het realiseren van een efficiënte allocatie van hulpbronnen door marktmacht, informatie-asymmetrie of externaliteiten. De achterliggende gedachte is dat de overheid niet intervenieert in de markt als dat niet nodig is. Imperfecties in innovatiesystemen zijn afgeleid uit de literatuur over nationale systemen van innovatie en evolutionaire economie (Nelson, 1993; Edquist, 1997). Hier is de veronderstelling dat er relaties en interacties tussen actoren en instituties van verschillende gedaanten zijn die soms goed werken maar soms ook niet. Het gaat dan om factoren als samenwerking tussen actoren in het innovatiesysteem, aan kansen om sterke regio's en sectoren verder te stimuleren en aan de randvoorwaarden voor innovatie (infrastructuur maar ook de rol van formele en informele instituties). In bepaalde situaties bieden gesignaleerde imperfecties in innovatiesystemen een rationale voor beleidsinterventie. Er bestaat overlap tussen beide concepten (Gustafsson en Autio 2006). In Tabel 7 presenteren we de verschillende elementen van imperfecties in markten en innovatiesystemen (Poel en Kool 2009):

Tabel 7 Imperfecties in markten en innovatiesystemen (Poel en Kool 2009)

Imperrfecties in markten	Imperfecties in innovatiesystemen
Positieve externaliteiten (spill-overs)	Belemmeringen in infrastructurele voorzieningen en investeringen
Publieke goederen en toe-eigening	*Lock-in* en padafhankelijkheid
Informatie-asymetrie	Institutionele belemmeringen
Niet-effectieve marktwerking	Falende interacties
	Onvoldoende vaardigheden en kennis

Positieve externaliteiten (spill-overs): Deze imperfectie is aan de orde wanneer een deel van de positieve opbrengsten van een innovatie niet toevalt aan de innoverende organisatie maar aan andere actoren in het innovatiesysteem. Hierdoor innoveert een individuele organisatie (bijvoorbeeld een bedrijf) minder

intensief, minder vaak of minder riskant, dan mogelijk zou zijn vanuit het bredere en soms ook publieke belang van de betreffende innovatie (het macroperspectief).

Publieke goederen en toe-eigening verwijst naar de situatie dat het vaak moeilijk is om een innovatie exclusief te houden en anderen te laten betalen voor gebruik van de innovatie. Dit betreft kennis die niet te beschermen is of geen marktvoorsprong geeft en die wordt gebruikt in producten en diensten waarbij het niet mogelijk is een exclusief gebruik van de innovatie af te dwingen

Informatie-asymmetrie betekent dat sommige partijen een beter beeld hebben over wat er gaande is rond een innovatie dan andere partijen. Het gebrek aan informatie kan ertoe leiden dat bepaalde partijen niet in staat zijn het voordeel van een innovatie te herkennen voor de eigen bedrijfsvoering. Het gaat hier om asymmetrie tussen partijen die een verschillende rol in de waardeketen spelen, zoals een toeleverend en een afnemend bedrijf, of een bedrijf die een dienst aanbiedt en een consument die de dienst afneemt.

Niet-effectieve marktwerking: de aanwezigheid van een dominant bedrijf, in combinatie met bijvoorbeeld hoge toetredingsdrempels en overstapkosten, kan leiden tot minder prikkels om te innoveren. Dit is in de eerste plaats een onderwerp voor mededingingsbeleid, maar het kan ook meespelen in innovatiebeleid. Voorbeelden zijn het stimuleren van open standaarden en open source, of van mogelijkheden tot radicale innovatie waarin een dominant bedrijf niet investeert omdat het daar geen direct belang bij heeft.

Aan de kant van imperfecties in innovatiesystemen kunnen we de volgende vijf elementen onderscheiden:

Belemmeringen in infrastructurele voorzieningen en investeringen betekent dat er een gebrek is aan voorzieningen die voor alle partijen van belang zijn (bijvoorbeeld een goede telecommunicatie-infrastructuur) die in de regel door de overheid moet worden geregeld (hoewel dit niet noodzakelijk zo is). De infrastructurele voorzieningen kunnen naast fysieke netwerken ook bestaan uit de kennisinfrastructuur: zaken als onderzoeksprogramma's en onderzoeks- en testfaciliteiten.

Van *lock-in* of padafhankelijkheid is sprake wanneer partijen zich min of meer gedwongen voelen op een bestaand pad door te gaan, omdat de kosten van verandering erg hoog zijn. Dit kan te maken hebben met de mate van standaardisering, interoperabiliteit tussen platforms en diensten en marktdominantie. De lock in/padafhankelijkheid die door MS Office in de PC-wereld is ontstaan, is een passend voorbeeld. Leiderschap en coördinatie zijn van groot belang om een organisatie op het nieuwe pad te krijgen. Niet iedere partij heeft belang bij een overstap, heeft de middelen om andere partijen mee te krijgen, of de kennis en middelen om te volgen.

Institutionele belemmeringen zijn te onderscheiden in harde institutionele belemmeringen (zoals ontoereikende of ontbrekende wetten en regels) en zachte institutionele belemmeringen (zoals een politieke cultuur die niet gericht is op stimulering van innovatie, een gebrek aan vertrouwen of een gebrek aan ondernemerszin).

Falende interacties verwijzen naar problemen in de interactie tussen actoren in het innovatiesysteem. Hier maken we onderscheid in twee vormen van falen: te veel interactie tussen een te kleine groep actoren (met als risico's een interne oriëntatie, groepsdenken een beperkte blik op kansen en mogelijkheden tot kartelvorming) en te weinig interactie tussen actoren die complementair zijn in termen van technologieën, partijen, vaardigheden en know how en die met en voor elkaar nieuwe diensten zouden kunnen ontwikkelen.

Een gebrek aan vaardigheden en kennis verwijst naar onvoldoende of afwezig leervermogen bij de betrokken partijen, te weinig of een verkeerde verzameling van competenties, te weinig capaciteit en human resources of onvoldoende flexibiliteit die de overgang naar een ander socio-technisch regiem belemmert.

In de analyse van de empirische bevindingen zullen we voor de verschillende soorten imperfecties nagaan in hoeverre deze zichtbaar zijn in het geval van de introductie van *Privacy by Design*.

4.5 Aanpak empirisch onderzoek

Het aanvankelijke doel van de studie was om via een representatieve survey onder bedrijven in Nederland die te maken hebben met de – massale – verwerking van persoonsgegevens een beeld te schetsen van de aangetroffen stimulerende en remmende factoren rond de adoptie van *Privacy by Design*. De survey is opgezet op basis van het theoretische en conceptuele kader dat we in het voorgaande hebben geschetst. Bij de *pilot* van de survey bleken twee problemen op te treden die ons noopten een andere onderzoeksaanpak te kiezen:

- Om een goed beeld van de stimulerende en remmende factoren te verkrijgen is een zekere mate van maturiteit ten opzichte van een systematische aanpak van risicobeheersing noodzakelijk. Gegeven de fase waarin de invoering van *Privacy by Design* verkeert, zullen vele bedrijven nog niet toe zijn aan een systematische en gestructureerde benadering van het belang dat *Privacy by Design* voor hen zou kunnen betekenen, Dat impliceert dat deze bedrijven vermoedelijk ook een beperkt beeld van de stimulerende dan wel remmende factoren rond adoptie van *Privacy by Design* hebben.
- Er heerste een zekere huiver bij de pilotgroep dat het beeld dat uit de survey naar voren zou komen, toch vooral iets zou zeggen over de mate waarin het Nederlandse bedrijfsleven voldeed aan de wettelijke vereisten. De pilotgroep gaf aan huiverig te staan tegenover deelname. Dit leidde bij de projectgroep tot de inschatting dat mogelijk veel respondenten niet zouden meewerken aan de survey.

De eerste factor leidde tot de constatering dat een survey mogelijk niet de gewenste rijkheid aan antwoorden zou genereren over stimulerende en remmende factoren in de praktijk van vandaag de dag. De tweede factor leidde tot de constatering dat de survey vermoedelijk verre van representatief zou worden en dus weinig daadwerkelijke inzichten zou bieden. Hoewel we nadrukkelijk – ook in het begeleidend schrijven – stelden dat het onderzoek niet gericht was op het meten van *compliance* bleek dit in de pilot niet overtuigend genoeg te zijn om deelname te garanderen van de intermediaire organisaties die we hiervoor

benaderd hadden (de brancheorganisaties die hoorden bij de selectie van de bedrijfssectoren met informatie-intensieve bedrijvigheid; zie Appendix 3 Dataverwerkend Nederland' voor een overzicht). In zekere zin kwam deze survey dus te vroeg om de situatie in Nederland op een grondige manier in beeld te brengen.

Op basis van een afweging van noodzakelijke investeringen, beschikbare tijd en te verwachten medewerking hebben we vervolgens gekozen voor een minder ambitieuze opzet. Beide problemen die hiervoor zijn geschetst, zijn te vermijden door te kiezen voor een doorsnee van bedrijven die te betitelen zijn als 'voorlopers'[21] met betrekking tot de adoptie en invoering van *Privacy by Design*. Deze bedrijven hebben in de praktijk stimulansen en belemmeringen ervaren met invoering van privacygerichtee maatregelen en zijn dus in staat om feedback te geven op de vooronderstellingen die uit ons conceptueel model naar voren komen. Daarnaast staan deze bedrijven in de regel minder huiverig tegenover de vraag in hoeverre ze ook handelen in overeenstemming met het wettelijk kader omdat deze bedrijven dit kader ook als richtsnoer voor hun aanpak kiezen. Overigens blijft ook met deze keuze staan dat het onderzoek niet gericht is op het onderzoeken van de mate van *compliance* in het Nederlandse bedrijfsleven met het wettelijk kader. Het onderzoek blijft uitsluitend gericht op het in kaart brengen van stimulerende en remmende factoren die bedrijven tegenkomen als ze besluiten (onderdelen van) *Privacy by design* in de bedrijfsvoering op te nemen.

Met deze keuze is de vragenlijst aangepast zodat deze geschikt was voor telefonische of *face to face* bevraging van de interviewpartners. In totaal zijn 35 organisaties benaderd die door de leden van de klankbordgroep zijn geïdentificeerd als voorlopende bedrijven. Negentien organisaties zijn geïnterviewd (zie Appendix 5 Overzicht geïnterviewde organisaties'). Het criterium 'voorlopend' is heuristisch gebruikt. De ervaringen en inzichten van de leden van de klankbordgroep met betrekking tot bedrijven die privacygerichte strategieën en middelen in hun bedrijfsvoering inzetten hebben we gebruikt om een bedrijven te selecteren voor het empirisch onderzoek. Uit de verkenning voor de survey bleek het belang van een nader onderscheid tussen bedrijven die persoonsgegevens bewerken voor of als onderdeel van hun dienstverlening (dataverwerkers) en bedrijven die oplossingen aanbieden of systeempakketten beheren (systeemleveranciers). In de presentatie van de bevindingen maken we duidelijk hoe dataverwerkers en systeemleveranciers over bepaalde vragen denken (zie hoofdstuk 5). Met de inperking tot een beperkt aantal respondenten is het onderzoek duidelijk exploratief van karakter geworden, en is er geen poging meer om tot een representatief beeld te komen. Door de blik van de respondenten pogen we een beter begrip te krijgen van stimulerende en remmende factoren waar ook andere organisaties dan de voorlopers mee te maken (kunnen) krijgen.

[21] De term 'voorlopers' suggereert dat de rest noodzakelijk moet volgen. Dit is een gevolg van de Rogeriaanse benadering die we hanteren. We gebruiken de term hier neutraler, dat wil zeggen dat we niet veronderstellen dat er een logische volgorde is of dat er sprake is van een wetmatigheid. Het onderzoek is alleen gericht op de vraag wat ervaren wordt als stimulerende en als remmende factoren. Het onderzoek richt zich niet op de vraag of *Privacy by Design* wenselijk dan wel noodzakelijk is.

4.5.1 *Internationale verkenning*

Naast de interviews met voorlopende bedrijven in Nederland hebben we in vier landen nader bekeken hoe *Privacy by Design* in overheid- en bedrijfsstrategie is ingebed. Deze vier landen zijn na een korte inventarisatie uitgekozen omdat er reden is om aan te nemen dat *Privacy by Design* een andere plaats inneemt in de bedrijfscultuur en de politieke omgeving in deze landen dan in Nederland. Daarmee kunnen deze landen een interessante spiegel vormen voor de Nederlandse situatie. De volgende vier landen zijn uitgekozen:

- Duitsland is Nederlands belangrijkste handelspartner en is in cultureel opzicht opmerkelijk privacybewust.
- De Verenigde Staten kent in tegenstelling tot Nederland geen horizontale privacywetgeving, maar wel een uitgebreide jurisprudentie op dit gebied. Daarnaast is het thuisbasis van veel internationale internetbedrijven die ook actief zijn in de EU en Nederland.
- Binnen Canada vinden we een toezichthouder die één van de grondleggers van de gedachte en theorie rond *Privacy by Design* is (de Office of the Information and Privacy Commissioner of Ontario).
- Het Verenigd Koninkrijk heeft een zeer lange traditie op het gebied van privacybescherming.

Deze beperkte landenstudie geeft een eerste indruk over wat Nederland kan leren van de aanpak in andere landen (door bedrijven en door overheden) en in hoeverre verschillen in politieke- en bedrijfscultuur hun weerslag hebben op diffusie en adoptie van *Privacy by Design.*

Voor elk van deze landen, inclusief Nederland zelf, is een literatuuronderzoek uitgevoerd waarbij de rol van de overheid (inclusief wetgeving en toezichthouder), bedrijfspraktijken, cultuur en perceptie en de daaruit voortvloeiende stimulerende en remmende factoren geïnventariseerd zijn. Deze inventarisatie is aangevuld en gevalideerd in tien interviews met internationale privacyexperts, *privacy officers* van bedrijven en toezichthouders (zie ook annex 5). Uiteraard zijn deze 10 interviews niet genoeg om een gedetailleerd en representatief beeld te geven, maar de combinatie van literatuuronderzoek met expertinterviews geeft een afdoende duidelijk beeld om de verschillen met de Nederlandse situatie te schetsen.

De inventarisatie is ingestoken vanuit een aantal perspectieven, die noodzakelijkerwijs een hoger abstractieniveau hebben (het gaat hier immers over een vergelijking tussen landen, niet tussen organisaties). Deze perspectieven zijn de rol van de overheid, wetgeving en toezichthouder, aspecten van de cultuur en hoe privacy in de media aandacht kreeg, de rol van het bedrijfsleven, en de stimulerende en remmende factoren die daaruit naar voren komen.

Privacy – cultuur' is een lastig begrip om in een analyse mee te nemen. Niettemin is er – onder andere door ogenschijnlijk grote verschillen op dit gebied met Duitsland – reden om hier nader naar te kijken. Een uitgangspunt wat we hierbij gebruikt hebben om snel landen met elkaar te kunnen vergelijken op cultureel gebied zijn de cultuurdimensies van Hofstede.[22] Deze dimensies zijn *power distance (PDI), individualism (IDV), masculinity (MAS), uncertainty avoidance (UAI) en long-term*

[22] Zie http://www.geerthofstede.nl/dimensions-of-national-cultures

oriëntation (LTO). Een belangrijke kanttekening daarbij is dat de betrouwbaarheid van methoden om “cultuurdimensies” te meten beperkt’is; het gaat hier om gemiddelden waardoor de diversiteit die binnen een land aanwezig is uit beeld verdwijnt. Deze dimensies nemen daarom geen belangrijke rol in de internationale vergelijking in.

In Hoofdstuk 5 worden de resultaten van deze landenstudie gepresenteerd.

5 Resultaten

In dit hoofdstuk geven we de resultaten van de empirische resultaten weer. We beginnen met een weergave van de nationale interviews, gevolgd door de internationale verkenning. Allereerst geven we weer in welke mate de geïnterviewde organisaties bekend zijn met het concept *Privacy by Design* en op welke manier zij dit in hun organisatie hebben vormgegeven. Daarna volgt een analyse vanuit de drie perspectieven zoals die omschreven zijn in het vorige hoofdstuk: de innovatiekenmerken, de interne organisatiekenmerken en de kenmerken van de externe omgeving. Het hoofdstuk sluit af met een beschouwing vanuit beleidsperspectief, met een analyse in termen van imperfecties in de markt en in het innovatiesysteem.

We maken in deze analyse onderscheid tussen organisaties die beschouwd kunnen worden als de verantwoordelijke voor de verwerking van persoonlijke gegevens (de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens) en organisaties die aanbieders zijn van technologie, IT-diensten (waaronder systeemleveranciers, system-integrators, clouddiensten, beveiliging en testen), en organisatorisch en juridisch advies. De verantwoordelijke organisaties hebben vaak persoonsgegevens van consumenten verzameld en opgeslagen en nodig om diensten te leveren of de persoonsgegevens vormen de kern van hun verdienmodel. De aanbieders zijn in sommige gevallen ook bewerker van persoonsgegevens in de zin van de Wet bescherming persoonsgegevens. Zij leveren bijvoorbeeld een IT-dienst en bewerken data (bijvoorbeeld door testen uit te voeren) in opdracht van de eigenaar van de gegevens. Een overzicht van de geïnterviewde organisaties is te vinden in Annex 4 (nationaal en internationaal). Een overzicht van het interviewprotocol is te vinden in Annex 5.

5.1 Privacy by Design

In hoofdstuk twee werd duidelijk dat er in de wetenschappelijke literatuur nog geen eenduidige definitie van *Privacy by Design* bestaat. Ook uit de interviews komt naar voren dat organisaties verschillende definities en betekenissen toekennen aan het begrip *Privacy by Design*. Alle partijen benadrukken het belang van de combinatie tussen technische en organisatorische maatregelen om persoonlijke gegevens op een adequate manier te beschermen (zoals geïllustreerd wordt door onderstaande citaten). Het gedachtegoed van PbD (zie Cavoukian, 2009) – dat breder is dan de oorspronkelijke *Privacy Enhancing Technologies*-benadering – wordt daarmee breed gedragen. Drie partijen noemen gegevensminimalisatie als een belangrijk onderdeel van *Privacy by Design*.

“Alles wat je moet doen om op technisch en organisatorisch gebied privacy te waarborgen en ook meetbaar te maken.” [verantwoordelijke]

“Het pakket aan technische en organisatorische maatregelen die voorkomen dat er onregelmatigheden zijn op het gebied van het beschermen van persoonsgegevens.” [verantwoordelijke]

“Ik ben blij verrast om te zien dat de toelichting [in het interviewprotocol, red] zich ook richt op organisatorische aspecten.” [aanbieder]

"Stap één bij Privacy by Design is data limitation, ofwel zo veel mogelijk voorkomen dat gegevens in de systemen terechtkomen." [aanbieder]

Toch zijn er wel degelijk verschillen te ontdekken tussen de omschrijvingen die geïnterviewde partijen geven voor PbD. Enkele organisaties benoemen bijvoorbeeld expliciet het belang omprivacy als ontwerpfactor mee te nemen bij aanvang van het ontwerpproces. Voor een aantal organisaties geldt dat zij de term en het concept PbD wel kennen, maar dat dit in hun organisatie niet zo genoemd wordt. PbD wordt dan meer als een visie beschouwd; de gebruikte term voor privacymaatregelen is dan dataprotectie of privacybescherming. Veel organisaties maken bewust onderscheid tussen deze beide begrippen (zie ook hoofdstuk twee voor een toelichting op beide begrippen) en geven aan zich te richten op dataprotectie. De nadruk ligt voor hen op het naleven van de dataprotectiewetgeving (de Wet bescherming persoonsgegevens), met andere woorden, onder welke voorwaarden mag de organisatie persoonlijke gegevens verwerken en welke criteria gelden er dan? Anderen wijzen erop dat als PbD alleen door de organisatie wordt ingevoerd om de wet na te leven, dit in de praktijk niet zal leiden tot een succesvolle adoptie van PbD.

"Privacy gaat helemaal niet over de 'Big Brother' aspecten. Het gaat om bescherming van persoonsgegevens, de wet. Het is een balanswet waarin je kijkt naar enerzijds de bescherming van de persoonsgegevens (individuele belangen) en anderzijds het vrije gebruik ervan (bedrijfsbelangen)." [verantwoordelijke]

"PbD is het waarborgen van het gehele proces, volgens de spelregels van de Wbp. Dus anonimiseren en minimaliseren waar nodig. Maar voor je het weet ben je bezig met het zoeken naar een specifieke oplossing voor een processtap, terwijl het vooral gaat om het geheel van processtappen." [verantwoordelijke]

"Als je de wet gewoon volgt, dan pas je PbD toe." [verantwoordelijke]

"De drijfveer moet zijn om de algemene organisatie te verbeteren. Bij een organisatie die PbD alleen toepast vanuit het oogpunt van compliance, krijg je nooit mensen die het ook echt willen. (…) [aanbieder]

Anderen leggen meer de nadruk op informatiebeveiliging en accessmanagement. Sommige partijen lijken opeenvolgende fases of niveaus van PbD te onderscheiden, beginnend bij informatiebeveiliging en accessmanagement en uitbreidend naar dataminimalisatie en een meer pro-actieve benadering van het adresseren van mogelijke privacykwesties door de organisatie.

"PbD is gewoon informatiebeveiliging en dit kan ook al worden toegepast in de Design-fase." [aanbieder]

"Het belangrijkste voordeel van PbD is het systeem-technisch ondervangen dat alleen bevoegde personen toegang hebben tot bepaalde informatie." [verantwoordelijke]

"Nu wordt er veelal detectief [reactief, red] gewerkt en door het toepassen van PbD kan worden omgeschakeld naar een pro-actieve manier van werken. Daar zouden we nog wel stappen kunnen maken." [verantwoordelijke]

5.2 De praktijk

De verschillen in de definitie van *Privacy by Design* hebben ook zijn weerslag op de manier waarop *Privacy by Design* in de praktijk is toegepast. Elke geïnterviewde organisatie heeft een andere combinatie van technische en organisatorische maatregelen geïnstalleerd. De maatregelen variëren van organisatorische maatregelen zoals het aanstellen van een of meerdere *Privacy Officers* of een Functionaris voor de Gegevensbescherming, training van personeel en bewustzijn van het personeel verhogen tot aan technische maatregelen zoals het anonimiseren en pseudonimiseren van gegevens, versleutelen van gegevens, autorisatiemanagement, informatiebeveiliging en het toepassen van gescheiden databases. Een enkele organisatie heeft creatieve methoden toegepast en heeft bijvoorbeeld een 'ethische hacker' laten zoeken naar privacy- en beveiligingslekken.

5.2.1 Privacy Officers

Veel geïnterviewde organisaties hebben één of meerdere *Privacy Officers* (PO) aangesteld. Organisaties maken een bewuste keuze om een *Privacy Officer* (PO) of een Gegevensfunctionaris (FG) aan te stellen. In sommige gevallen wordt voor beide functies gekozen. De Gegevensfunctionaris (FG) is aangemeld bij het College Bescherming Persoonsgegevens. De FG is niet verantwoordelijk voor het beleid ten aanzien van privacy door de organisatie, maar houdt onafhankelijk toezicht op de bescherming van persoonsgegevens door de organisatie. De *Privacy Officer* is direct betrokken bij het te voeren beleid binnen een organisatie en adviseert over het realiseren van privacybescherming in concrete projecten en toepassingen.

Er bestaat variatie in de opzet, functie en plek van de PO binnen de organisatie en organisatiestructuur. Sommige organisaties kiezen er bijvoorbeeld bewust voor om de PO's niet aan een afdeling of divisie te laten rapporteren maar direct aan de Raad van Bestuur (RvB). Op deze manier heeft de PO een onafhankelijke positie en wordt de belangenafweging door het hoger management van de organisatie gemaakt. Ook geeft het de PO meer gezag en autoriteit. Deze constructie geldt niet voor alle geïnterviewde partijen. Soms vormen de *Privacy Officers* samen met *Security Officers* een gezamenlijke afdeling en rapporteren de PO's aan de *Centrale Security Officer* (CSO) die verantwoordelijk is voor informatiebeveiliging. Voor sommige organisaties is de aanstelling van een *Privacy Officer* een manier om ook naar buiten toe te laten zien dat privacy serieus wordt genomen door de organisatie.

"Bij externe processen, bijvoorbeeld wanneer klanten een marketingomgeving willen opzetten met verschillende uitingen, dan zal de projectmanager de IT-afdeling, data-afdeling en privacy en security afdeling erbij betrekken om gezamenlijk te brainstormen over de belangrijkste aspecten die moeten worden ingebouwd. De privacy officer is van het begin betrokken bij het proces. Dit is een luxe positie. Vaak komt de privacy officer en de juridisch adviseur van de klant er ook bij. Dat is een extra voordeel omdat zij veel meer weten over het proces en behoefte bij de klant. Veel privacy officers in andere bedrijven worden te laat ingeschakeld of moeten achteraf kunnen herleiden welke keuzes er zijn gemaakt."
[verantwoordelijke]

5.2.2 Privacy en dataprotectie Impact Assessments

Veel geïnterviewde organisaties werken met een (verplichte) gestandaardiseerde vragenlijst die medewerkers inzicht geeft bij de start van een nieuw project of er gewerkt wordt met persoonsgegevens, of de *Privacy Officer* moet worden ingeschakeld en welke criteria moeten worden nageleefd. De vragenlijsten zijn een (beknopte versie) van een *Privacy* of *Data Protection Impact Assessment* die nauw zijn afgestemd op het bedrijfsproces. In vrijwel alle gevallen ligt de nadruk op dataprotectie en minder op privacy (zie hoofdstuk twee). Een quick-scan geeft aan of er wel of niet sprake is van persoonsgegevens. Deze wordt gevolgd door een uitgebreide vragenlijst of een beoordeling van de PO over (de vorm van) diens betrokkenheid. Dit kan variëren van een eenmalig advies tot aan een vast lid van het projectteam als dat noodzakelijk is. In een aantal organisaties is het bepalen van de privacyrisico's opgenomen in een bredere '*Business Impact Assessment*' waar ook andere zaken en risico's (zoals confidentialiteit) worden meegenomen.

"Wij werken met een privacymonitor. Deze bestaat uit een simpele verkorte vragenlijst om mee te kunnen draaien in de organisatieprocessen." [verantwoordelijke]

"Wij voeren nu PIA's [Privacy Impact Assessments, red] uit. Deze worden op dit moment herzien omdat ze iets te generiek zijn voor de gewenste standaard, de zogenaamde Binding Corporate Rules." [verantwoordelijke]

"Het uitvoeren van een PIA is een normale verplichting: informatiebeveiliging begint met risicoanalyse. De PIA zou als norm kunnen worden uitgewerkt in de ISO-27002 om enig handvat te bieden." [aanbieder]

5.2.3 Techniek

Naast diverse organisatorische maatregelen wordt er ook een veelvoud aan technische maatregelen toegepast. Dit is vaak een combinatie van pseudonimiseren en anonimiseren van gegevens, versleutelen van gegevens, autorisatiemanagement, informatiebeveiliging en het toepassen van gescheiden databases. Ook worden zogenaamde "Chinese muren" tussen afdelingen, personeel en databases gecreëerd. Sommige organisaties geven aan persoonsgegevens in te delen in verschillende risicoklasses waar verschillende waarborgen aan verbonden zijn. Partijen geven aan dat PbD in de praktijk bijna altijd maatwerk betekent. Hierdoor krijgt PbD in elke organisatie en in elk project een ander karakter.

"In onze IT-systemen zijn vormen van encryptie opgenomen (…). Standaard worden testgegevens geanonimiseerd en gescrambled daar waar het kan. Een buitenstaander kan er dan niets mee." [aanbieder]

"Tussen de verschillende afdelingen bestaan Chinese walls, dit is ook bij IT goed ingebed. Bij testen is de testdata geanonimiseerd. Ook hebben we vrij ingewikkelde matrices over wie allemaal waar bij mag. Dit is een volwassen instrument." [aanbieder]

"Wanneer er bijvoorbeeld een nieuwe website wordt gemaakt, wordt er eerst gekeken wat voor type informatie verwerkt wordt. Vanuit IT-oogpunt wordt dan gekeken wat er moet worden toegepast zoals encryptie, dataflow analyseren, waar beschermen, wachtwoord en hoe de opslag en vernietiging van data moet worden geregeld." [verantwoordelijke]

5.3 Innovatiekenmerken van Privacy by Design

5.3.1 Performance expectancy

5.3.1.1 Relatief voordeel / Unique Selling Point / Toename verkoop

De geïnterviewde partijen reageren wisselend op de vraag of *Privacy by Design* een relatief concurrentievoordeel biedt en of PbD een *Unique Selling Point* kan opleveren. Bedrijven wiens business model gebaseerd is op de verwerking van persoonsgegevens (bijvoorbeeld in de marketingsector) geven aan dat dit wel het geval kan zijn. Het actief uitdragen van adequate privacybescherming is voor hen ook noodzakelijk om zaken te kunnen doen met hun klanten. Voor bedrijven waar de verwerking van persoonsgegevens niet de kernactiviteit van de organisatie is (zoals de retail, energie of financiële sector) ligt dit anders. Zij zien *Privacy by Design* niet als een methode waarmee ze zich kunnen onderscheiden van hun concurrenten, het is meer een '*commodity*', een gegeven: het is iets dat ze moeten doen. Deze organisaties verwachten ook niet dat de invoering van PbD op korte termijn zal leiden tot een toename van de verkoop. Dit is gerelateerd aan de mate van bewustzijn over privacybescherming en het belang dat er door consumenten en bedrijven aan gehecht wordt (dit wordt in de volgende paragrafen over organisatie- en omgevingskenmerken nader toegelicht).

"Privacy wordt veel meer gezien als een commodity dan als een satisfier. Klanten verwachten dit simpelweg van ons." [verantwoordelijke]

Met het toepassen van PbD kan in onze branche geen concurrentievoordeel worden behaald. Je zou het een commodity moeten noemen. Wij zijn niet de industrie die baten verkrijgt uit persoonlijke informatie." [verantwoordelijke]

"Het hanteren van privacybeschermende maatregelen zal pas op langere termijn een concurrentievoordeel opleveren voor klanten. Er is een verandering gaande van onwetendheid dat men op de hoogte is dat er iets bestaat als privacy, naar langzaam in de richting van waar een bedrijf goed voorbereid moet zijn" .[aanbieder]

"Er kan overigens een kantelpunt [om PbD meer toe te passen, red] komen dat privacy echt belangrijk wordt gevonden door de consumenten en door bedrijven ook gerespecteerd wordt." [aanbieder]

5.3.1.2 Herkenbaarheid

Organisaties constateren als een van de problemen van PbD dat privacybescherming niet volledig meetbaar is, of in elk geval minder meetbaar dan het meten van de hoeveelheid CO2-uitstoot. Daar kan direct worden vastgesteld of men aan een bepaalde norm voldoet. Dit is dan ook herkenbaar voor de buitenwereld. Voor privacy en dataprotectie ligt dit ingewikkelder. Het versleutelen van persoonlijke gegevens kan bijvoorbeeld op vele verschillende manieren, met verschillende voor- en nadelen, maar wat is de juiste manier? Organisaties zijn van mening dat de Wet bescherming persoonsgegevens te veel ruimte voor interpretatieverschillen laat (zie paragraaf over omgevingskenmerken). Bedrijven vinden daarom een ISO-certificering een prettig instrument, omdat ten eerste duidelijk wordt aan welke norm ze exact moeten voldoen en ze vervolgens kunnen aantonen aan klanten en consumenten dát ze aan die norm voldoen. Ook *Privacy Officers* vormen een herkenbaar – en voor sommige organisaties daarmee noodzakelijk – onderdeel van *Privacy by Design*.

"De wetgeving is vrij vaag. Er is ook ruimte voor interpretatieverschillen. De auditer kan er zijn stempel opzetten, maar nog steeds is het niet voor 100% meetbaar dat de privacy is gewaarborgd. Dit is anders bij milieuwetgeving, daar heb je een duidelijke limiet van een bepaalde hoeveelheid CO2-uitstoot, bij privacy ligt dat veel ingewikkelder." [aanbieder]

"Als je je kan onderscheiden door ISO en met een PbD-certificaat, dan is het [Privacy by Design] een drijfveer." [aanbieder]

"Het is bijna niet meer mogelijk om zonder Privacy Officer in deze markt te kunnen acteren. Klanten nemen je niet meer serieus als je dit niet hebt georganiseerd. Onze grote klanten hebben allemaal prominente privacy officers" [verantwoordelijke]

5.3.1.3 Efficiëntie en effectiviteit

Organisaties verwachten dat het toepassen van *Privacy by Design* de kans op privacy-incidenten verkleint. Dit is een van de belangrijkste redenen voor organisaties om PbD te adopteren. Toch zijn organisaties zich er van bewust dat de toepassing van PbD privacy-incidenten niet altijd kan voorkomen. Aan de andere kant zien organisaties PbD niet als een innovatie waar de organisatie ook efficiënter van wordt. Een geïnterviewde geeft bijvoorbeeld aan dat PbD vertragend kan werken omdat het een extra check en controle in het proces betekent. Uit verschillende studies komt naar voren dat een vermindering van functionaliteit van diensten en IT-systemen een belemmerende factor is om PbD in te voeren. Geïnterviewde organisaties geven aan dit dat inderdaad wel eens voor komt, maar dat het in de praktijk niet als barrière wordt gezien.

"Wat we zien, is dat applicaties voor klanten die consumenten hebben dat die veel eerder dit soort concepten [PET, red] gaan adopteren, omdat zij bang zijn voor imagoschade. Als bedrijven bekend worden met dit soort concepten dan kiezen ze zeker hiervoor. Informatieverschaffing is daarvoor wel noodzakelijk." [aanbieder]

"Wanneer je PbD adequaat toepast zal het de kans op privacyschendingen verkleinen (…). Maar Privacy by Design kan privacyschendingen nooit helemaal uitsluiten." [verantwoordelijke]

"Een voordeel om PbD toe te passen is dat er duidelijke garanties zijn dat aan bepaalde voorwaarden is voldaan." [verantwoordelijke]

"Een positieve drijfveer is om de beveiliging beter op orde te hebben, beveiliging is gebaat bij aandacht voor privacy zodat persoonsgegevens goed beveiligd zijn. Andere positieve drijfveren, bijvoorbeeld dat een organisatie efficiënter zou worden, dat is niet altijd zo." [aanbieder]

"Positieve drijfveren zijn: vergroten van vertrouwen en loyaliteit, business agility, inzicht in risico's, verbetering effectiviteit door meer controle. Maar in de praktijk is men vooral bang dat persoonsgegevens op straat komen te liggen." [aanbieder]

5.3.1.4 Vertrouwen van klanten

Voor verschillende organisaties is het respecteren van de persoonsgegevens van consumenten een belangrijke reden voor het toepassen van PbD. Het imago dat de organisatie heeft is daarbij belangrijk. Organisaties voelen een morele verplichting om zorgvuldig met persoonsgegevens om te gaan.

"Betrouwbaarheid en vertrouwen uitdragen is voor ons de grootste drijfveer om mensen [werknemers, red] te leren zorgvuldig met persoonlijke informatie om te gaan." [verantwoordelijke]

"[Wij passen PbD toe, red] Om te voldoen aan datgene wat de organisatie wilt uitdragen: veiligheid en betrouwbaarheid." [verantwoordelijke]

"Het is een voorwaarde voor het waarborgen van vertrouwen. Als er lekken optreden raakt die relatie [het vertrouwen dat de klant in organisatie heeft, red] verstoord" [verantwoordelijke]

5.3.1.5 Verantwoordelijkheid en aansprakelijkheid

Verschillende partijen wijzen op het verband tussen *Privacy by Design* en *accountability*. *Accountability* wordt gezien als het vaststellen, controleren en aantonen dat de organisatie aan de (wettelijke) normen voldoet. *Privacy by Design* is dan een onderdeel van *accountability* of een manier om *accountable* te zijn: een manier om in de praktijk te realiseren dat de organisatie aan de norm voldoet en aan anderen aan te tonen dat de organisatie aan de norm voldoet. Voor veel geïnterviewden wordt de norm bepaald door het wettelijk kader (de Wet bescherming persoonsgegevens). Bedrijven spannen zich in om aan dit kader te voldoen en richten zich op naleving van deze wettelijke kaders. Eén geïnterviewde vindt dat de omschrijving van *Privacy by Design* zoals gebruikt in het interviewprotocol meer richting *accountability* gaat:

"Ik zie PbD als een specifieke term voor het ontwikkelen van nieuwe producten. De toelichting uit het interviewprotocol is te breed en gaat meer richting accountability principe van de OECD. Vooral de organisatorische maatregelen maken het te breed. PbD is maar één component van accountability. PbD kan je toepassen bij een nieuw en concreet project. Het is project-specifiek. PbD vindt dus plaats op tactisch niveau. Accountability is meer overkoepelend en op strategisch niveau". [verantwoordelijke]

In de afgelopen jaren is de aandacht voor aansprakelijkheidskwesties rondom de verwerking van persoonsgegevens bij organisaties toegenomen. Dit betreft vooral de afspraken over de verantwoordelijkheden tussen de data processor en de data controller. Partijen geven aan dat deze afspraken steeds vaker juridisch worden vastgelegd.

"Juridische vastlegging [van verantwoordelijkheden tussen dataverwerkers en databewerkers, red] neemt toe, daar komt de klant nu zelf mee." [aanbieder]

"Ook privacylekken worden contractueel (en beveiligingstechnisch) afgedicht, net als het vernietigen van data op verzoek of bij beëindiging van het contract." [aanbieder]

5.3.1.6 Financiële impact

Eerder werd al duidelijk dat PbD in iedere organisatie, en soms in ieder project, op een andere manier wordt vormgegeven. *Privacy by Design* is maatwerk geven geïnterviewde partijen aan, zeker als het gaat om het technische aspect. Dit maakt het lastig voor partijen om aan te geven in hoeverre de financiële impact van de invoering van PbD een rol speelt bij de adoptiebeslissing. Sommige geïnterviewden maken onderscheid tussen de impact van het organisatorische deel van PbD, waaronder het opstellen van het privacybeleid en de daarbij behorende organisatiestructuur (zoals het aanstellen van *Privacy Officers*, de manier van rapporteren, audits e.d.) en de impact van PbD op projectniveau, m.a.w. privacy tijdens het project als factor meenemen in het ontwerpen van een specifieke dienst of product. Het eerste heeft volgens hen een grote financiële en organisatorische impact, het tweede heeft weinig (extra) financiële impact. Sommige partijen geven aan dat het vooral om een verschuiving van kosten gaat. De systeemontwikkeling

en organisatorische maatregelen kunnen duurder zijn maar de verwachte vermindering van (de kans op) privacy-schendingen levert besparingen op. Deze verwachte baten zijn moeilijk te kwantificeren. Dit kan het voor organisaties moeilijk maken de directe extra kosten af te wegen tegen de baten.

"De impact in termen van complexiteit van ICT valt relatief gezien mee, als je dit vergelijkt met de hoeveelheid tijd en geld die nodig is voor de inrichting van organisatorische maatregelen. Dit brengt voor organisaties vaak irreële kosten met zich mee." [aanbieder]

"De financiële impact van de toepassing van PbD valt mee. De inrichting van de organisatie [privacybeleid, red] kost wel veel geld. Er zijn weinig extra kosten bij PbD, omdat het ingebouwd is in het project. Als je het achteraf moet toepassen, kost het ontbreken van PbD bakken met geld. De tijd, manpower die nodig is om na afloop van een project PbD in te bouwen kost 10-tallen, zo niet 100 malen meer dan wat het kost om het direct in te bakken. Het toepassen van PbD levert vooral geld op. Dan laat ik claims nog buiten beschouwing." [aanbieder]

"Het is een verschuiving van kosten. Als een bedrijf een risico op privacyschending loopt, dan krijg je in de toekomst te maken met kosten. Maar de inschatting van de risico's is vaak laag. Dus een bedrijf moet nu kosten maken om toekomstige kosten te voorkomen. Dat is lastig, omdat het lastig is in te schatten wat deze toekomstige kosten zijn." [aanbieder]

"Systeemontwikkeling met PbD kan duurder zijn maar vermindering van kans op schendingen levert besparingen op. Dat is de balans voor het hoger management. De vraag 'wat levert het op' is lastig te kwantificeren. Een bedrijf moet nu kosten maken om toekomstige [kosten, red] te voorkomen. Dat is lastig, omdat het lastig is in te schatten wat de toekomstige kosten zijn. Bij privacybewuste organisaties lukt dat wel." [verantwoordelijke]

"Privacy by Design toepassen is wel duurder voor de systeemontwikkeling. Maar deze investeringen leveren aan de andere kant baten op in termen van minder privacyrisico's. Overigens is het kwantificeren van deze baten erg moeilijk, waardoor het maken van een goede trade-off lastig is." [aanbieder]

Een andere overweging die bij bedrijven meespeelt in de beslissing PbD al dan niet in te voeren is de relatie met de kernactiviteit van het bedrijf. Organisaties in de zorg bijvoorbeeld hebben te maken met krimpende budgetten en een groeiend aantal klanten. Functies als *Privacy Officers* en juristen drukken op de directe functiecapaciteit en het aantal handen aan het bed. Organisaties kunnen zich goed voorstellen dat wanneer het bedrijf of de organisatie in zwaar(der) weer komt, *Privacy Officers* een functie is die bij reorganisaties onder druk komen te staan. Dit speelt ook bij kleine bedrijven, voor wie het lastiger is deze functiecapaciteit vrij te maken (zie ook paragraaf 5.4.4 Omvang en organisatiecultuur).

"Het toepassen van PbD en het accountability principe hebben natuurlijk een financiële impact. Waar data niet de kernactiviteit is van een bedrijf, dan is het goed voor te stellen dat PO's minder belangrijk zijn en als een van de eerste posities bij een reorganisatie geschrapt wordt." [verantwoordelijke]

5.3.2 Effort expectancy

5.3.2.1 Compatibiliteit en complexiteit

De al aanwezige IT-structuur binnen organisatie, met name de aanwezigheid van verouderde systemen, bemoeilijkt vaak de invoering en realisatie van PbD in de IT-systemen van de organisatie. Het toepassen van privacymaatregelen in deze

zogenaamde legacysystemen wordt als zeer lastig, zo niet onmogelijk, ervaren. Een aanbieder van privacyvriendelijke technologie geeft aan dat organisaties die werken met webgebaseerde systemen eenvoudiger kunnen overstappen.

"Vaak is het geen green field maar heb je te maken met een erfenis van oude systemen, soms staan gegevens nog in de mainframe. De uitdaging is om daar PbD toe te passen". [aanbieder]

De bestaande infrastructuur in een organisatie is een barrière. Als je bijvoorbeeld echt vanaf het begin gescheiden databases wilt hanteren, is dit echt heel erg lastig." [aanbieder]

"Het is een grote uitdaging om bij al lopende projecten nog privacy aspecten te implementeren. Voorbeelden zijn het EPD of de OV-chipkaart. Dit is niet realistisch om naderhand te implementeren. De effectiviteit om privacy te waarborgen is zeer beperkt achteraf." [aanbieder]

"Voor nieuwe omgevingen is het evident dat privacy wordt meegenomen, maar de uitdaging zit bij de legacysystemen". [aanbieder]

"Bedrijven die recent zijn geautomatiseerd naar web-based systemen kunnen eenvoudiger overstappen naar onze infrastructuur. Die hebben het makkelijk. Legacysystemen kunnen een barrière zijn, in die zin dat het een behoorlijke investering en tijd zal vergen om de IT-systemen zodanig aan te passen." [aanbieder]

Ook de complexiteit van *Privacy by Design* en privacywetgeving is een complicerende factor voor de invoering van PbD. Er bestaat bijvoorbeeld onduidelijkheid over wat technisch gezien een goede maatregel is (zie paragraaf 5.3.2.2 over gepercipieerde uitvoerbaarheid). De complexe aard van PbD en wetgeving betekent ook dat een organisatie voldoende kennis in huis moet hebben (of moet inhuren) om privacybescherming adequaat vorm en inhoud te geven.

5.3.2.2 Gepercipieerde uitvoerbaarheid

Het realiseren van *Privacy by Design* in de organisatie is een complex en langdurig proces dat veel impact heeft op de organisatie. Alle processen en IT-systemen moeten onder de loep worden genomen, er moet een integraal privacybeleid ontwikkeld worden dat is afgestemd op het organisatieproces, in sommige gevallen zullen organisatieprocessen en IT-systemen moeten worden aangepast. Het ontwikkelen van deze structuren, evenals het ontwikkelen en gebruik van PIA's, het opleiden en trainen van personeel en de IT-systemen organiseren nemen vaak enkele jaren in beslag. *Privacy by Design* is in die zin zeker geen "plug-en-play-innovatie" die organisaties snel en eenvoudig invoeren.

"Het toepassen van PbD heeft impact op de IT binnen de organisatie. Wanneer er bijvoorbeeld een nieuwe website wordt gemaakt, dan wordt er eerst gekeken wat voor type informatie hier verwerkt wordt. Vanuit IT oogpunt wordt dan gekeken naar wat er moet worden toegepast zoals encryptie, dataflow analyseren, waar beschermen, wachtwoord, hoe moet opslag en vernietiging van data worden geregeld." [verantwoordelijke]

"Dat onze afnemers Privacy by Design meer gaan toepassen heeft ook impact op onze organisatie, met name de impact op onze informatietechnologie en bedrijfsprocessen is groot. Het gaat dan om outsourcing, het beheer regelen van systemen en databases, rekening houden met wetgeving. (...) De impact op onze bedrijfsstrategie is minder groot, die blijft waarschijnlijk ongeveer hetzelfde." [aanbieder]

Ook speelt mee dat, zoals eerder al genoemd, organisaties van mening zijn dat de wet ruimte laat voor interpretatieverschillen. Daar komt bij dat organisaties aangeven dat het niet altijd eenvoudig is vast te stellen is wat een goede privacymaatregel is op technisch gebied. Wat is nu echt een goede architectuur? Vaak kleven er voor- en nadelen aan verschillende architecturen.

"Het is maar de vraag of bepaalde oplossingen echt oplossingen zijn. Als je bijvoorbeeld het principe van gescheiden databases wilt hanteren, dan is het lastig dit in een bestaande omgeving te realiseren. Het is moeilijk vast te stellen wat goede beveiligingsmaatregelen zijn. Op alles valt wel iets af te dwingen. Stel dat je gaat encrypten, is dat dan wel safe? En hoe doe je dat dan? Er is veel discussie over wat goede technische en organisatorische maatregelen zijn." [aanbieder]

"Hoe zorgt het management ervoor dat de opgestelde maatregelen ook echt geïmplementeerd zijn? Een probleem daarbij is de vertaling van wetgeving naar concrete maatregelen, niet alleen op IT-gebied. Aan de ene kant is de wetgeving niet duidelijk en aan de andere kant zijn de genomen maatregelen niet altijd concreet genoeg om zeker te weten dat je aan de wet voldoet. Er is op dit gebied (te)veel onduidelijkheid bij klanten, en ook intern bij ons." [aanbieder]

Een aantal organisaties geeft aan dat er daarom andere redenen aanwezig moeten zijn die de organisatie doen besluiten *Privacy by Design* in te voeren, zoals privacy-incidenten, boetes van de toezichthouder, voldoen aan het wettelijk kader en dergelijke. Verder hangt de gepercipieerde uitvoerbaarheid ook af van hoe ver een organisatie al is in het implementeren van privacybeschermende maatregelen.

"De impact op de bedrijfsprocessen is redelijk groot. Mede door de druk van boetes zijn privacy officers aangesteld. Er zijn extra policies en richtlijnen aan toegevoegd." [verantwoordelijke]

"Als een organisatie op dit gebied (nog) niks doet, is het [invoering PbD, red] een echte aardverschuiving. In dat geval is het belangrijk om het aan een bredere business noodzaak op te hangen." [verantwoordelijke]

5.4 Organisatorische kenmerken

5.4.1 Bewustzijn / gebrek aan informatie/ervaring met PbD

De interviews zijn gehouden met de voorlopers op het gebied van het toepassen van privacybeschermende maatregelen. Zij geven aan dat er in Nederland over het algemeen bij het bedrijfsleven een gebrek aan kennis en bewustzijn bestaat ten aanzien van privacybescherming en de wettelijke kaders daaromtrent. Aanbieders van technologie geven aan dat hun klanten in de praktijk nog niet vragen om *Privacy by Design*. Het bewustzijn bij het grootste deel van hun klanten over het belang van privacybescherming is nog te laag voor PbD om er concurrentievoordeel uit te halen.

"Een andere barrière is onkunde / onvoldoende kennis op het gebied van techniek, organisatie en wetgeving. Dit heeft vooral te maken met het vertalen van de wet naar praktische toepassing. Dit laatste is een marktkans voor de system-integrators". [verantwoordelijke]

"Daarnaast valt op dat bedrijven technische kennis missen. Veel organisaties [dataverwerkers, red] hebben deze kennis niet meer aan boord." [dataverwerker]

"Het leeft nog niet zodanig bij onze klanten, red] dat je al kunt schermen van 'Wij hebben PbD geïmplementeerd'." [aanbieder]

"Bij organisaties in Nederland is nog steeds niet voldoende besef dat privacybescherming een vereiste is." [verantwoordelijke]

"Het zou mooi zijn als er bijvoorbeeld een web portal is, dat handvatten en richtlijnen biedt omtrent PbD. Zodat bedrijven zelf deskresearch kunnen uitvoeren. Ik denk dat het nu nog erg moeilijk is voor bedrijven om vanaf nul te beginnen." [aanbieder]

5.4.2 Gepercipieerd risico privacyschendingen

De aandacht voor privacy en het bewustzijn over privacyrisico's is in de laatste één à twee jaar duidelijk toegenomen bij zowel bedrijven als consumenten. Een belangrijke factor daarin is de media-aandacht die er in deze periode voor privacy-incidenten en beveiligingslekken is geweest. In 2011 werd dit versterkt door de affaire rond Diginotar en de aandacht voor 'Lektober'. Deze aandacht en de daaraan gerelateerde zorg voor reputatieschade hebben er toe geleid dat het waarborgen van de bescherming van persoonsgegevens hoger op de agenda staat binnen bedrijven. Organisaties beschouwen mogelijke privacyschendingen nu eerder als een risico. In contractonderhandelingen over een IT-dienst of systeem wordt privacybescherming vaker als expliciete eis meegenomen. Voor veel bedrijven is dit een belangrijke stimulerende factor om *Privacy by Design* in te voeren.

"Een driver zijn privacy-incidenten en als er gegevens op straat liggen. Dat heeft bij ons echt een 'shift' veroorzaakt, toen zijn richtlijnen opgesteld, codes of conduct, de systemen zijn doorgelicht en de beveiliging moet goed zijn. De richtlijnen zijn strikter geworden. Governance is daaraan gekoppeld, het gaat niet alleen om de ICT databases maar ook om de organisatie daaromheen. Dat is een forse implementatie." [verantwoordelijke]

Een van de geïnterviewden merkt op dat dit in feite een 'negatieve' drijfveer is. *Privacy by Design* wordt nu vaak vanuit een negatieve invalshoek ingestoken: privacy-incidenten komen veel in het nieuws, er is kans op een boete, op gehackt kunnen worden en grote reputatieschade. Dat zijn de factoren die bedrijven voornamelijk bewegen om PbD toe te passen, maar niet vanwege mogelijke positieve effecten. In de vorige paragraaf over de innovatiekenmerken van *Privacy by Design* werd al duidelijk dat PbD wel beschouwd wordt als een effectieve manier om de kans op privacyschendingen te verkleinen, maar dat organisaties het niet beschouwen als een manier om de organisatie ook efficiënter te maken.

5.4.3 Leiderschap en houding topmanagement

De mate van bewustzijn en het belang dat het topmanagement aan privacybescherming hecht komen als een van de belangrijkste drijfveren voor een succesvolle implementatie van *Privacy by Design* naar voren. Bewustzijn bij het topmanagement maakt het mogelijk dat een integraal privacybeleid wordt ontwikkeld en er bijbehorende functiecapaciteit (zoals *Privacy Officers*) wordt vrijgemaakt; zonder de wil van het topmanagement is het 'trekken aan een dood paard' volgens een van de geïnterviewde partijen. Daarnaast geeft steun van het hogere management de PO ook meer gezag. Het topmanagement beïnvloedt ook de cultuur en daarmee het bewustzijn en gedrag van individuele werknemers binnen de organisatie ten aanzien van privacybescherming. Volgens sommige organisaties is dit nog belangrijker dan de technische maatregelen en het opgesteld privacybeleid an sich.

"Belangrijkste punt is: borg dat je twee keer per jaar op de agenda van het MT en RvB het onderwerp privacyvoortgang neerzet. Zorg dat je in bestuurlijke zin en managementverantwoordelijke zin het onderwerp niet uit het oog verliest. Borg het goed en houd het bewust als bespreekpunt." [verantwoordelijke]

"Er zijn verschillende eigenschappen die maken dat een organisatie makkelijker of moeilijker Privacy by Design kan toepassen, maar de meestbepalende is de cultuur van een organisatie. De houding van het topmanagement is de belangrijkste factor om de cultuur te beïnvloeden" [verantwoordelijke]

"Als de organisatieleiding zich niet van privacyrisico's bewust is of onvoldoende, dan kan de organisatie het beter niet doen: dan is het trekken aan een dood paard. Dan kan er op papier een PO zijn aangesteld, maar als in de praktijk het mandaat of de positie ontbreekt heeft het geen zin. Het helpt mij [de PO, red]. in mijn contact met de medewerkers, dat de RvB de bescherming van persoonsgegevens heel serieus neemt. Dat geeft de PO autoriteit en gezag." [aanbieder]

"De houding van het topmanagement omtrent privacy is belangrijker dan puur het toepassen van PbD. De manier waarop management tegen PbD aankijkt is van veel grotere invloed dan bijv zoiets als dataminimalisatie. Gedrag en commitment van mensen is allerbelangrijkste. Dit laatste is ook een onderdeel van PbD" [aanbieder]

"Privacy by Design is in staat om de kans op privacyschendingen te verkleinen. Maar het gaat vooral om de stap daarvoor, namelijk de bereidheid om er überhaupt over na te denken PbD toe te passen. Organisaties die PbD gaan toepassen hebben over het algemeen meer bereidheid bij het topmanagement en organisaties die meer zijn blootgesteld aan opinies en pressiegroepen, dit veroorzaakt een groter effect." [aanbieder]

5.4.4 Omvang en organisatiecultuur

De bedrijfscultuur en de beleving van het belang van privacybescherming door de medewerkers is een belangrijk aspect van een succesvolle adoptie van PbD in een organisatie. Partijen geven bijvoorbeeld aan dat organisaties op moeten passen dat *Privacy by Design* niet alleen 'op papier' geregeld is, maar dat het zich ook daadwerkelijk vertaalt en verankert in de bedrijfsprocessen, o.a. door de beleving (en naleving) door individuele medewerkers. De verankering van PbD in de dagelijkse werkzaamheden van iedere medewerker gaat niet van vandaag op morgen. In sommige gevallen dient lokaal personeel in bijvoorbeeld India te worden opgeleid over wetgeving in Nederland. Culturen kunnen soms dusdanig verschillen dat het creëren van dit bewustzijn een lastig traject is. Het managen van deze cultuurverandering wordt door sommige organisaties als belangrijk nadeel beschouwd van PbD. Het vraagt om veel communicatie en het geven van trainingen.

"Ik denk dat het belangrijkste is dat je niet alleen kijkt naar dat op papier alles geregeld is, via mooie contracten, nette procesbeschrijvingen, audits e.d., maar dat je je als bedrijf daar niet in verliest. Uiteindelijk moet het ook door de medewerkers worden nageleefd, bijvoorbeeld door training en opleiding van medewerkers." [aanbieder]

"Het hangt niet alleen op juridische vastlegging. Het moet ook leven." [aanbieder]

"Het veranderen van de mindset van de operationele medewerkers is een langdurig (on-going/never-ending) traject" [verantwoordelijke]

"De cultuur van de organisatie heeft een grote invloed op de inbedding van het privacybeleid binnen de organisatie, het is het naar de mensen brengen van maatregelen." [verantwoordelijke]

Organisaties wijzen er ook op dat de invoering en realisatie van *Privacy by Design* een multidisciplinair probleem is waarbij verschillende expertises uit verschillende afdelingen met elkaar zullen moeten samenwerken. Dit kan lastig zijn omdat mensen elkaars taal niet spreken en de moeilijkheden versterkt kunnen worden door de organisatiecultuur, zoals onderstaand citaat weergeeft.

"Een belangrijke barrière uit de praktijk zijn de verschillende afdelingen: vaak is er een afdeling rondom compliance en een afdeling voor de dagelijkse operations. Dit zijn vaak twee ivoren torens. Juristen missen de kennis van de operations, en operations weet niet welke wetgeving van toepassing is, met als gevolg dat je privacy niet 'by design' kunt meenemen." [aanbieder]

Verder geven grote organisaties aan dat hun (grote) omvang de implementatie van PbD bemoeilijkt. Dit kan bijvoorbeeld te maken hebben met het grote aantal landen waar een organisatie actief is waardoor de organisatie te maken krijgt met grote verschillen in lokale wetgeving (bijvoorbeeld Europa, Verenigde Staten, India en Azië). Hoe groter de organisatie, hoe lastiger het is om bijvoorbeeld als *Privacy Officer* geïnformeerd te blijven over alle privacygerelateerde zaken en daar advies over te geven.

"De cultuur binnen de organisatie maakt het wel moeilijk om PbD toe te passen. De cultuur binnen onze organisatie is vrij stroperig, bureaucratisch en georganiseerd in silo's. Dit maakt het lastig om met generieke toepassingen te werken en het is lastig om de verschillende partijen te overtuigen. Het maakt ook het uitwisselen van best practices lastiger." [verantwoordelijke]

"De grootste uitdaging van onze omvang is dat je [als Privacy Officer, red] ergens heel laat van op de hoogte wordt gebracht, if at all!" [verantwoordelijke]

Ook kleinere bedrijven staan voor diverse uitdagingen als zij PbD willen implementeren. Vaak ontbreekt bij deze bedrijven specialistische kennis en de mogelijkheid om specialistisch personeel in te huren. Grote organisaties kunnen geld en functiecapaciteit vrij maken voor bijvoorbeeld het aanstellen van juristen en/of *Privacy Officers*. Dit is voor het Midden- en Kleinbedrijf lastiger. Ook geven organisaties aan dat privacybescherming extern beleggen geen optie is omdat het zo niet verankert in de cultuur van de organisatie en de werkzaamheden van individuele medewerkers.

"Als grote organisatie ben je in het voordeel omdat je in staat bent om bijvoorbeeld een jurist of FG in dienst te hebben. Kleine organisaties hebben daar geen geld voor en schrikken wel eens wanneer er een dergelijke reactie van ons komt [dat een samenwerkingsovereenkomst niet wordt ondertekend vanwege privacybezwaren, red]. Wij krijgen soms ook wel terug van kleinere organisaties in het veld: Wat zeur je nou over privacy? Er is te weinig kennis en daar hebben wij soms ook wel vaak opvoedingswerk te doen." [verantwoordelijke]

"Je hebt een aantal mensen van een behoorlijk hoog kennisniveau nodig om al die zaken adequaat vorm en inhoud te geven. Privacy is van groot belang, maar kan gemakkelijk in de verdrukking komen in de praktijk van alledag, met name bij kleine organisaties. (…) Dat is overigens geen reden om privacyborging uit te besteden. Als je het extern gaat zetten, dan loop je het risico dat privacy niet goed tussen de oren van werknemers zit." [verantwoordelijke]

Het viel buiten het bereik van dit onderzoek om de bedrijfscultuur van iedere organisatie te bepalen in termen van innovativiteit, open voor veranderingen en dergelijke.

5.4.5 Data-intensiteit / type data dat verwerkt wordt

Bedrijven waar de verwerking van persoonsgegevens niet de kernactiviteit is, geven aan dat privacybescherming voor hen meer een *commodity* is – iets dat van hen verwacht wordt, maar niet iets waar ze zich mee kunnen onderscheiden of dat tot een toename van de verkoop leidt. Voor data-intensieve bedrijven en bedrijven die hun directe baten halen uit de verwerking van persoonlijke gegevens lijkt de invoering van privacybeschermende maatregelen wel een *satisfier* te zijn. Om zaken te kunnen doen met andere bedrijven, is het voor hen belangrijk om aan hun klanten aan te tonen dat zij de protectie van persoonlijke gegevens van consumenten serieus nemen en dat hun bedrijfsprocessen hier op afgestemd zijn.

"Het is bijna niet meer mogelijk om zonder privacy officer in deze markt te kunnen acteren: 'klanten nemen je niet meer serieus als je dit niet hebt georganiseerd'. Onze grote klanten hebben allemaal prominente privacy officers" [verantwoordelijke]

5.4.6 Diversiteit gebruikte IT-systemen

Dit onderwerp is in de interviews niet aan de orde gekomen.

5.4.7 Banden met toezichthouders

Zie volgende paragraaf 5.5.1 'Rol toezichthouder'.

5.5 Externe omgeving

5.5.1 Rol toezichthouder

De huidige rol en mogelijkheden van de toezichthouder worden door geïnterviewde partijen geïdentificeerd als een van de barrières om PbD te implementeren. De partijen merken unaniem op dat het College Bescherming Persoonsgegevens middelen te kort komt om (strenger) te handhaven en partijen aan te sporen tot betere privacybescherming. Sinds het CBP zich in vooral toegelegd heeft op handhaving en toezicht, ervaren partijen de kans dat zij daadwerkelijk gecontroleerd zullen worden door het CBP en de kans op een boete als laag. Met andere woorden, op dit moment is de toezichthouder geen drijvende kracht voor bedrijven om *Privacy by Design* te (gaan) implementeren. Overigens tonen alle geïnterviewde partijen begrip voor de situatie van de toezichthouder. Een partij geeft aan dat na druk van een buitenlandse toezichthouder het bedrijf een integraal privacybeleid heeft ontwikkeld en geïmplementeerd.

"Een zorg is wel dat het CPB te maken heeft met krimpende middelen waardoor hij haar tanden niet meer kan laten zien. Voor de geloofwaardigheid van de toezichthouder is het heel belangrijk dat hij bijvoorbeeld voldoende mankracht heeft."

"De rol van de Nederlandse toezichthouder is echter zeer gering. Er heeft een verschuiving plaatsgevonden van advisering naar controlerend, dit bereikt niet altijd het beoogde doel". [aanbieder]

"We zouden vaker iets tegen het CBP willen aanhouden, bijvoorbeeld op consultancy basis. Dit helpt bij het scheppen van het een kader, waardoor het accent veel minder zal liggen op handhaving. (…) Het CBP heeft nu te weinig handhavingsinstrumenten: boetes zijn laag, weinig mensen en middelen om te handhaven. [verantwoordelijke]

"De Amerikaanse FTC heeft de organisatie destijds dringend verzocht om meer aandacht aan privacy te besteden. Mede door de druk van de FTC zijn privacy officers aangesteld." [verantwoordelijke]

Verder geven partijen unaniem aan dat zij de adviesrol van het CBP missen. Het bedrijfsleven heeft behoefte aan een partij waar ze met vragen over concreet te treffen maatregelen terecht kunnen. Dit hangt samen met de complexiteit van het privacyvraagstuk, zowel wat betreft wetgeving als wat betreft multidisciplinariteit die nodig is voor de oplossing. Organisaties zien graag dat het CBP meer richting geeft in hoe met concrete vraagstukken om te gaan, zoals is gebeurd in het traject van de kilometerheffing. Het CBP heeft ontwerprichtlijnen opgesteld en in het bestek uitgewerkt hoe persoonsgegevens moesten worden beschermd.

"De rol van de toezichthouder mag duidelijker. (…) Maar het zou nuttig zijn als het CBP een duidelijke visie naar buiten brengt en ook een adviserende rol vervult. Een meer pro-actieve rol, die waarschuwt en laat zien hoe het wel kan, is welkom." [aanbieder]
"Het CBP heeft onvoldoende resources. De overheid zou duidelijke functionele richtlijnen moeten geven hoe persoonsgegevens moeten worden opgeslagen. Een onafhankelijke partij zou moeten borgen dat de functionele eisen door de technische architecturen ook daadwerkelijk vervuld worden." [aanbieder]

5.5.2 Verkrijgbaarheid Privacy by Design oplossingen

De voorlopers op het gebied van dataprotectie en dataverwerking geven aan zelf de technische, organisatorische en juridische kennis in huis te hebben om *Privacy by Design* toe te passen. Zij ontwikkelen zelf een instrumentarium en soms ook specifieke technieken of *Privacy Enhancing Technologies*, zoals anonimisering of pseudonimisering. Externe expertise wordt op incidentele basis ingehuurd voor specialistische technische of juridische kennis. De niet-voorlopers missen echter de kennis (zowel op juridisch als technisch vlak) om *Privacy by Design* in hun organisatie vorm te geven, volgens de geinterviewden.

"Wij zijn in staat om zelf instrumenten te ontwikkelen voor PbD […] We huren wel puur voor technische kennis en ondersteuning externen in." [verantwoordelijke]

"De organisatie is in staat om circa 80% van de PbD instrumenten zelf te ontwikkelen. Er zijn een paar specifieke gebieden waarop de kennis ontbreekt, zoals webinformatietechnologie." [verantwoordelijke]

"Een aantal instrumenten heeft de organisatie zelf ontworpen, omdat 1) het vaak ontbreekt aan kennis buiten de deur en 2) het wenselijk kan zijn om snel te acteren. We hebben wel contact met een aantal externe partijen, die zorgen voor technische ondersteuning." [verantwoordelijke]

De kwaliteit van het aanbod van externe bureaus wordt wisselend beoordeeld. Sommige geïnterviewden geven aan het veld onvoldoende te overzien om daar een oordeel over te vellen, anderen waren niet tevreden over de technische kennis. Over het algemeen wordt de juridische kennis die beschikbaar is bij externe bureaus als voldoende of goed beoordeeld.

"Er zijn nu nog bijzonder weinig kwalitatief goede bureaus. […] in het verleden heeft onze organisatie een aantal bureaus ingehuurd waar we toch minder tevreden over waren. Soms bleek tijdens het project dat mijn kennis [van de Privacy Officer, red] beter was dan dat van de externe partij." [verantwoordelijke]

"Er zijn te weinig aanbieders die zich profileren als een aanbieder die dit hoog in het vaandel heeft.(…) Privacyclausules moeten op dit moment zelf worden aangevraagd door de organisatie." [verantwoordelijke]

De technologieaanbieders geven op hun beurt aan voldoende kennis in huis te hebben om technische maatregelen in te bouwen die privacybescherming kunnen waarborgen en om aan de vraag van hun klanten te voldoen. Daarmee zou er voldoende aanbod zijn. Aan de andere kant zijn de geïnterviewde dataverwerkers vaak ontevreden met de kennis die hun aangeboden wordt en over de afwachtende houding van systeemleveranciers. De aanbieders van technologie geven aan voldoende kennis in huis te hebben om ook aan de toekomstige vraag van hun klanten te voldoen.

"Een andere barrière is de onkunde of onvoldoende kennis op het gebied van techniek, organisatie en wetgeving. Dit heeft vooral te maken met het vertalen van de wet naar praktische toepassing. Aanbieders van technologie zouden een dergelijke kans kunnen verzilveren (…) maar zij hebben vooral een technische achtergrond." [aanbieder]

"PbD is niet door een business consultant of een security-expert alleen op te lossen. Het is veel meer een multidisciplinair probleem." [systeemleverancier]

"Daarnaast valt op dat bedrijven technische kennis missen. Veel organisaties hebben deze kennis niet meer aan boord. Dit biedt een mogelijke opportunity voor ons" [systeemleverancier].

5.5.3 Wettelijk kader en complexiteit

De wettelijke verplichting die bedrijven hebben om persoonlijke gegevens adequaat te beschermen blijft een belangrijke drijfveer voor bedrijven om privacymaatregelen te nemen. Sommige partijen zien strenge(re) wetgeving als de enige drijfveer voor bedrijven om PbD te implementeren, terwijl anderen aangeven dat als het naleven van de wet (*compliance*) de enige reden is om PbD toe te passen, dit in de praktijk onvoldoende zal zijn. Enkele partijen geven aan dat een hoge boete die zij in het verleden opgelegd hebben gekregen, de directe aanleiding was om het privacybeleid van de organisatie naar een hoger plan te trekken.

"Onze klanten zijn bereid om te investeren in PbD als ze daar op worden afgerekend" [aanbieder]

"Er spelen verschillende barrières bij afnemers bij het toepassen van PbD. Kennis, er is onvoldoende bekendheid en de kosten zijn te hoog. Wanneer vanuit de wetgever PbD wordt opgelegd dan zijn dit geen issues meer." [aanbieder]

"Drivers zie ik niet anders dan dat er een wettelijke verplichting zou zijn." [aanbieder]

"De drijfveer moet zijn om de algemene organisatie te verbeteren. Bij een organisatie die PbD alleen toepast vanuit het oogpunt van compliance, krijgt je nooit mensen die het ook echt willen. (…)

De komende herziening van de dataprotectierichtlijn in Europa, met onder andere de verplichte meldplicht en de mogelijkheid tot hogere boetes, is dan ook voor sommige bedrijven aanleiding om hun huidige maatregelen te controleren en waar nodig aan te scherpen. Sommige organisaties geven aan dat ze niet verwachten dat de herziening tot grote veranderingen zal leiden omdat ze nauw aansluiten bij de huidige wetgeving.

"Er komt meer aandacht (…) voor Privacy by Design. Dit is ook in verband met wetgeving (denk bijvoorbeeld aan de herziening van de EU dataprotectierichtlijn), deze dwingt klanten om stappen te nemen in de toepassing van PbD." [aanbieder]

"Data breach notification is nu nog niet van toepassing, speelt meer in de telecomsector. Maar binnen de organisatie wordt er al wel rekening mee gehouden. De vraag rijst hoe dit kan worden geïmplementeerd in het huidige Incident Management Systeem" [verantwoordelijke]

"Het hanteren van de meldplicht is een forse ingreep. Maar de scope [van de herziene richtlijn, red] is nog niet helemaal duidelijk. Contractueel gezien moet er gemeld worden, maar wij hebben geen invloed of de dataverwerker ook de betrokkenen informeert. Het kan altijd beter, de meldplicht zet wel weer even de puntjes op de i." – [aanbieder]

Hoewel de aanwezigheid van een wettelijk kader dus een drijfveer is voor organisaties om privacybescherming te realiseren, geven organisaties ook aan dat het lastig is de Wet bescherming persoonsgegevens te vertalen naar concrete maatregelen (zowel technisch als organisatorisch). Dit is ook aan de orde gekomen bij de innovatiekenmerken van Privacy by Design, o.a. bij gepercipieerde uitvoerbaarheid van Privacy by Design en herkenbaarheid.

"Privacywetgeving is complex en onduidelijk, met als gevolg dat veel organisaties niet in staat zijn om wetgeving te borgen met Privacy by Design". [aanbieder]

5.5.4 Vraag consumenten

Het merendeel van de geïnterviewde partijen geeft aan dat er weinig drijvende kracht van de houding van de consument uit gaat op dit moment. Zij verwijzen naar de consument die vrijwillig gedetailleerde persoonlijke informatie deelt met bekenden en onbekenden via sociale media en die geen kritische houding aanneemt tegenover bedrijven ten aanzien van privacybescherming. De media-aandacht die privacy-incidenten krijgen komt wel naar voren als factor van betekenis. Een enkele partij geeft aan dat de houding van de consument wel degelijk belangrijk is.

"Ik zie twee tegengestelde trendbewegingen: iedereen mag alles van mij weten enerzijds, en de roep om meer privacybescherming vanuit politiek en organisaties anderzijds. Welke trend zet door? Nu liggen er zo vaak persoonsgegevens op straat, en steeds meer mensen delen informatie op sociale media, wordt het dan op een gegeven moment minder belangrijk? Aan de andere kant zijn bedrijven nu juist door de toegenomen berichtgeving serieus en met een flink budget bezig met privacybescherming." [aanbieder]

"De belangrijkste externe factor om PbD toe te gaan passen is de houding van de consument en de houding van de markt. Dat zijn onze klanten of potentiële klanten. Er wordt meer van ons verwacht; klanten verwachten dat wij strenger omgaan met persoonsgegevens." [verantwoordelijke]

5.5.5 Concurrentie

Voor data-intensieve bedrijven is privacybescherming, en daarmee *Privacy by Design*, belangrijk in hun contact met klanten en het binnenhalen van werk. Het is, zoals eerder aan bod is gekomen, een manier om zich van concurrenten te kunnen onderscheiden.

"De toepassing van PbD is noodzakelijk voor ons business model: in ons veld moet je met PbD werken. Dat wordt gevraagd van onze klanten." [verantwoordelijke]

Dit geldt niet voor alle organisaties. Aanbieders van technologie zien *Privacy by Design* (nog) niet als iets waarmee ze concurrentievoordeel kunnen behalen. Hun kerndienst is het leveren van een bepaalde infrastructuur of IT-dienst (zoals informatiebeveiliging, het testen van data of het aanbieden van cloud-diensten) en dat bepaalt hun waarde in de markt. Het beschermen van privacy is in dat opzicht voor hun verdienmodel (en dat van hun concurrenten) secundair. Het toepassen van *Privacy by Design* kan wel impact hebben op processen of systemen van de aanbieder (bijvoorbeeld op gehanteerde standaarden in informatiebeveiliging) maar daarmee verandert de aangeboden dienst (en bijbehorende propositie) feitelijk niet.

"Het is secundair: het leveren van infrastructuur voor datacenters en cloud services is voor ons het belangrijkst, het toepassen van PbD is niet onderscheidend" [aanbieder]

"Onze propositie is informatiebeveiliging, tenzij marketingtechnisch PbD interessanter wordt (…). De marktbenadering zal wellicht anders zijn, maar in principe is 'alles onder de motorkap' aanwezig." [aanbieder]

Aanbieders vinden dat zij zich niet van hun concurrenten kunnen onderscheiden door de invoering van *Privacy by Design*. Hier speelt mee dat het bewustzijn bij het grootste deel van hun klanten over het belang van privacybescherming nog te laag is voor PbD om concurrentievoordeel uit te halen. Veel klanten vragen in de praktijk niet om *Privacy by Design*. Op langere termijn kan PbD mogelijk wel concurrentievoordelen opleveren.

"Concurrenten van huidige klanten hebben geen invloed op de toepassing van PbD. Het hanteren van privacybeschermende maatregelen zal op langere termijn concurrentievoordelen op kunnen leveren voor klanten. Er is een verandering gaande van onwetendheid dat men op de hoogte is dat er zoiets bestaat als privacy, naar langzaam in de richting van waar een bedrijf goed op voorbereid moet zijn." [aanbieder]

"Tijdens de ontwikkeling van software denk je na hoe je dat kan doen [toepassen PbD, red]. Er zijn veel voorbeelden van bedrijven die dat niet doen: hun business model is No Privacy by Design" [aanbieder]

Uit de interviews valt op dat aanbieders van technologie (system-integrators en systeemleveranciers) zich reactief opstellen als het gaat om het toepassen bij *Privacy by Design*. Deze afwachtende houding wordt door de aanbieders zelf benoemd en erkend. Ze werken volgens de wensen en eisen van de klant (de dataverwerker). Als die er specifiek om vraagt, dan wordt gekeken waar en hoe (extra) waarborgen kunnen worden aangebracht in het systeem, dienst of geleverde infrastructuur. In de afgelopen twee jaar is privacybescherming en vooral het (kunnen) aantonen hoe persoonlijke gegevens worden beschermd in de IT-systemen door aanbieders belangrijker geworden. Voor sommige klanten zijn resultaten van audits niet genoeg, zij willen vergaand inzicht in de processen en systemen van de systeemleveranciers om zeker te weten hoe gegevens worden beschermd.

"Wij moeten 100% kunnen aantonen dat privacy goed gewaarborgd is. Dat doen we door de klant vergaand inzicht te geven in hoe het systeem wordt ingericht." [aanbieder]

"Vanuit de klant is er de laatste twee jaar meer aandacht voor gekomen. Aan de vraagkant zien we dat er nu ook gevraagd wordt om dit in contracten te regelen, zodat de juiste juridische inbedding ontstaat. Aan de vraagkant worden ook de auditrechten uitgebreid; er wordt gekeken welke technische en organisatorische maatregelen die de organisatie neemt" [aanbieder]

Dit komt ook terug bij het opstellen van de contracten over databeheer en dataverwerking tussen dataverwerkers en datacontrollers (de aanbieders van technologie). De dataverwerkers (de voorlopers) zijn hier de drijvende kracht. De opdrachtgever (de dataverwerker) neemt haar eisen op in het bestek en de aanbieders geven aan hoe zij aan deze eisen tegemoet komen. De dataverwerkers ervaren het als nadelig dat zij zelf actief moeten wijzen op het belang van privacybescherming en dat zij zelf de privacymodules voor de contracten moeten aandragen, terwijl de systeemleveranciers van mening zijn dat de opdrachtgevers (de dataverwerkers) hun verantwoordelijkheid moeten nemen en privacybescherming in de bestekken / offerte-aanvragen moeten opnemen. Beide partijen kijken dus naar elkaar om het initiatief te nemen om privacybescherming op een hoger plan te krijgen.

"Privacy clausules moeten op dit moment zelf worden aangevraagd door de organisatie." [verantwoordelijke]
"Opdrachtgevers [dataverwerkers, red] moeten hun verantwoordelijkheid nemen. Opdrachtnemers kunnen niet het voortouw nemen in het beschermen van privacy wanneer dit hen géén 'competitive edge' oplevert" [aanbieder]

Ook aanbieders van alternatieve privacyvriendelijke oplossingen hebben last van de afwachtende houding van partijen.

"Wat je meestal ziet is dat [privacyvriendelijke, red] technologie pas een kans krijgt als iemand pijn krijgt. (…) We merken dat bedrijven het belang van onze dienst wel zien, maar toch zijn ze aarzelend. Ze vragen zich af 'wanneer gaat dit echt lopen, wanneer moet ik er bij zijn, moet ik er nu gas op geven of nog even wachten'. De waarde en het nut van ons alternatief wordt groter naarmate meer bedrijven zich aansluiten. Bedrijven staan in feite voor een kip-ei probleem." [aanbieder]

De afwachtende houding ligt anders voor de relatie met het MKB. Daar geven zowel de systeemleveranciers als de dataverwerkers aan dat het MKB de kennis en het bewustzijn mist van het waarborgen van persoonsgegeven en privacy van klanten. Richting het MKB zijn beide actoren pro-actiever in het benoemen van mogelijke risico's en oplossingen om deze te verkleinen. Het gaat dan om standaard- of basisoplossingen rondom de bescherming en beveiliging van persoonlijke gegevens.

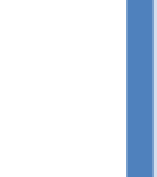
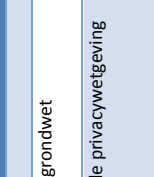
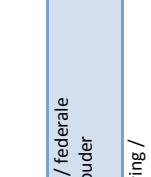
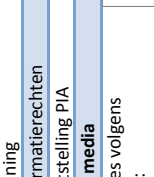
"Wij ondersteunen hier onze kleine klanten, we hebben een sjabloon waarin dit allemaal is opgenomen, dat we als opdrachtnemer hieraan voldoen. We voeden in feite zo de klant op. Dit is niet alleen best practice, maar vooral om onze privacypositie te benadrukken. Dit is commercieel interessant: wij zijn een organisatie die serieus omgaat met privacy." [verantwoordelijke]

5.6 Internationaal perspectief

Privacy en privacybescherming wordt in verschillende landen op verschillende manieren ingevuld: er zijn culturele verschillen, maar ook de rol die overheden spelen varieert sterk. Bestudering van verschillen én overeenkomsten in de omgang met privacy en privacybescherming in andere landen verrijkt het beeld over wat stimulerende en remmen de factoren zijn bij de invoering van *Privacy by Design*. Het toont welke rol overheden spelen, wat de gevolgen van deze rol zijn, welke successen er geboekt worden en welke problemen over landen heen vergelijkbaar zijn. Er zijn vier landen uitgekozen om te bestuderen. Buurland Duitsland is Nederlands belangrijkste handelspartner, en is qua cultuur opmerkelijk privacybewust. De Verenigde Staten vormen een interessante spiegel, omdat er in dit land (nog) geen horizontale privacywetgeving is, maar wel een uitgebreide jurisprudentie. Binnen Canada vinden we een toezichthouder die één van de grondleggers van de gedachte en theorie rond *Privacy by Design* is (de *Office of the Information and Privacy Commissioner of Ontario*). Onze andere buur, het Verenigd Koninkrijk, heeft een uitzonderlijk lange traditie op het gebied van privacybescherming.

5.6.1 Overzicht

Op de volgende pagina zijn deze vier landen in vogelvlucht naast Nederland geplaatst. Na de overzichtstabel volgt een bespreking van de resultaten, en wat dit zegt over Nederland en stimulerende en remmende factoren bij *Privacy by Design*.

Factor	Nederland	Duitsland	Verenigde Staten	Canada	Verenigd Koninkrijk
Overheid					
Privacy in grondwet	ja	Ja	nee (wel bij sommige staten)	indirect (enkele artikelen die er naar verwijzen)	nee (VK heeft geen grondwet)
Horizontale privacywetgeving	Wet Bescherming Persoonsgegevens (met implementatie EU Directive)	Bundesdatenschutzgesetz (met implementatie EU Directive)	Nee, wel uitgebreide jurisprudentie (case-law)	Privacy Act (overheid) & Personal Information Protection and Electronic Documents Act (private sector)	Data Protection Act (met implementatie EU Directive) & Privacy and Electronic Communications Regulations
Sectorspecifieke wetten	ja, politie, medisch, sociale zekerheid, arbeidsdeelname minderheden, burgerservicenummer	ja, specifiek per deelstaat	ja, financieel, medisch, video huur, kinderen online, telemarketing, en wetten specifiek per staat	ja, banken, verzekeringen, telemarketing, jeugdige delinquenten, en wetten specifiek per provincie	ja, medisch, kredieten, politie, rehabilitatie
Nationale / federale toezichthouder	College Bescherming Persoonsgegevens (nationaal)	BfDI (federaal), en aparte toezichthouder per staat	nee (al vervult de Federal Trade Commission deze rol deels)	OPCC (nationaal), aparte toezichthouder per provincie	Office of the Privacy Commissioner Canada (nationaal)
handhaving / ondersteuning	handhaving	beide, nadruk op handhaving	beide, nadruk op handhaving	beide, nadruk op ondersteuning	Beide, nadruk op ondersteuning
ook informatierechten	nee	Ja	-	Ja	ja
verplichtstelling PIA	nee	Nee	ja (publieke sector)	ja (publieke sector)	ja (publieke sector)
Cultuur & media					
Dimensies volgens Hofstede[1]: - Power distance (PDI) - Individualism (IDV) - Masculinity (MAS) - Uncertainty avoidance (UAI) - Long-term orientation (LTO)					
een invloedrijk incident	Elektronisch Patiënten Dossier gestopt	grote weerstand tegen Google Street View	aanslagen 11-9-2001, gevolgd door patriot act	-	News of the World telefoon afluisterschandaal

Tabel 8 Data verkregen van http://geert-hofstede.com/countries.html. Enige kanttekeningen: het gaat hier om gemiddelden, waardoor diversiteit binnen land verdwijnt; ook is de betrouwbaarheid van methoden om “cultuurdimensies” te meten beperkt. Niettemin kan met deze grafieken in één oogopslag een redelijk beeld gekregen worden van de verschillend tussen landen op cultureel gebied.

Een aantal zaken in dit overzicht is opmerkelijk. Zo is in de Verenigde Staten geen expliciete grondwettelijke bescherming van privacy, en ook geen horizontale federale privacywetgeving zoals de Wet Bescherming Persoonsgegevens. Er is echter wel degelijk een zekere mate van privacybescherming dankzij sectorale privacywetgeving, bepaalde vormen van lokale privacywetgeving en een uitgebreide jurisprudentie op dit onderwerp.

De rol van de toezichthouder (als deze er is) varieert sterk tussen landen. Waar in Nederland de nadruk ligt op handhaving, ligt die bij de toezichthouder van Ontario, Canada juist sterk op ondersteuning en het samen zoeken naar oplossingen.

When we notice a breach, we go and sit around the table with those responsible and see it as an opportunity to introduce Privacy by Design into an organization; this makes organizations very receptive. [Office of the Information and Privacy Commissioner of Ontario, Canada]

Privacy Impact Assessments zijn in een aantal landen verplicht gesteld voor publieke instanties, maar dit is niet zo in Nederland.

Qua cultuur is een opvallend gegeven dat het land wat het laagst scoort op Hofstede's 'individualisme' dimensie (Duitsland), juist een bijzonder actieve cultuur rond privacy heeft, en van tijd tot tijd van zich laat horen in het geval van diensten met een potentieel privacy-invasief karakter (zoals in de aanpak van Google Street View). Ook zien we dat het publieke debat rond privacy in landen vaak gevormd wordt door een aantal invloedrijke incidenten. Privacy is een onderwerp wat ook internationaal meestal niet proactief maar reactief behandeld wordt ("als het kalf verdronken is…").

5.6.2 Wat betekent dit voor de Nederlandse situatie

Het vergelijken van deze landen geeft met name inzicht in de kenmerken van de externe omgeving die werken als stimulerende en remmende factoren voor het toepassen van *Privacy by Design*.

5.6.2.1 Externe omgeving

Wat wetgeving rond privacy betreft, heeft Nederland evenals Duitsland en het Verenigd Koninkrijk een wet die van dezelfde Europese dataprotectierichtlijn is afgeleid. Ook kennen deze landen sectorspecifieke wetten waarin regels rond privacy vastgelegd worden.

Op het gebied van wetgeving vormt vooral de Verenigde Staten een interessante uitzondering door het (vooralsnog) ontbreken van horizontale privacywetgeving, en een sterkere nadruk op zelfregulering. In de praktijk is er wel degelijk een zekere mate van rechtelijke bescherming van privacy, dankzij sectorale wetgeving en een uitgebreide jurisprudentie op dit onderwerp. Het idee achter de aanpak in de Verenigde Staten is dat zelfregulering zou leiden tot meer flexibele richtlijnen en codes, die sneller tot stand komen dan regulering of wetgeving. Enerzijds heeft dit inderdaad geleid tot het tot stand komen van richtlijnen en *best practices*, anderzijds lijkt het ontbreken van duidelijke privacywetgeving een negatieve impact

te hebben op het bedrijfsleven. De Verenigde Staten overwegen daarom om ook privacywetgeving in te voeren, al zal de nadruk op zelfregulering blijven liggen.[23]

Een ander interessant verschil is dat in drie van de vijf bestudeerde landen een Privacy Impact Assessment (PIA) in de publieke sector verplicht gesteld is, in tegenstelling tot in Nederland. De rationale hierachter is dat een (verplichte) PIA organisaties en bedrijven aanzet tot het systematisch en bewust omgaan met privacybescherming, en bijdraagt aan een vergrote transparantie over de wijze waarop bedrijven met persoonsgegevens omgaan .

In de internationale interviews werden enkele relevante kanttekeningen geplaatst bij het van overheidswege reguleren van privacybescherming. Ten eerste dat het doel van deze regulering zou moeten zijn om bedrijven te belonen voor het nemen van de juiste maatregelen, en ten tweede dat regulering (door bedrijven) niet gezien moet worden als een obstakel, maar als een uitdrukking van de zorgen die burgers over hun privacy hebben.

The main regulatory goals would be that firms would be rewarded for having measures in place. The same issue has played out on the environmental side: regulatory systems that reward firms that have the right systems in place, even though they do not always make cost-benefit analysis that may be beneficial to the environment. [Ira Rubinstein, academische privacy expert in de Verenigde Staten]

Building consumer trust is paramount. In this context, complexity of laws and regulations should be seen primarily as an expression of specific issues of public concern rather than an insurmountable hurdle.[Collin O'Malley, chief strategy officer bij Evidon (leverancier privacy oplossingen)]

De invulling die in de verschillende landen gegeven wordt aan een toezichthouder op het gebied van privacywetgeving verschilt sterk. In de Verenigde Staten ontbreekt een federale privacytoezichthouder (mede door het ontbreken van een horizontale privacywetgeving op federaal niveau), al vervult de *Federal Trade Commission* die rol tot op zekere hoogte. Waar in Nederland het College Bescherming Persoonsgegevens alleen toeziet op het naleven van de Wet Bescherming Persoonsgegevens en de andere privacywetten, zien de toezichthouders in Duitsland, Canada en het Verenigd Koninkrijk ook toe op het handhaven van de informatierechten van burgers (in Nederland vastgelegd in de Wet Openbaarheid van Bestuur). In een breder perspectief geplaatst is dit een relevant verschil: waar een overheid steeds meer over haar burgers te weten komt (door afnemende privacy) kan deze scheve informatiebalans mogelijk gecorrigeerd worden door deze overheid transparanter te maken (door opbouwen van informatierechten).

Waar in Nederland de toezichthouder niet een stimulerende factor van betekenis lijkt te zijn voor het toepassen van privacybeschermende maatregelen door bedrijven, is dit bijvoorbeeld in het Verenigd Koninkrijk anders. Daar heeft een krachtigere handhavingsrol van de toezichthouder geleid tot een toegenomen

[23] De rationale achter het privacybeleid in de Verenigde Staten en recente ontwikkelingen daarin worden goed uitgelegd in een *green paper* uit 2010 van de Department of Commerce: http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

interesse in privacybescherming door bedrijven. De toezichthouder in Ontario, Canada, kiest nadrukkelijk voor een aanpak waarin – naast strafmaatregelen – samenwerking en ondersteuning gezocht wordt om tot een betere privacybescherming te komen. Hij noemt op haar website een reeks voorbeelden waarin deze aanpak omschreven wordt.[24] Vergeleken bij deze toezichthouders legt het Nederlandse CBP relatief weinig nadruk op ondersteuning van bedrijven, terwijl daar wel een grote behoefte aan is.

It is sometimes the success of these new ways which encourages others to adopt them as well. Therefore, when we see a privacy innovation that is successful, we shout it from the rooftops. [Office of the Information and Privacy Commissioner of Ontario, Canada]

[..] the EU would benefit from a closer co-operation between industry and the regulator. At the moment there is no such initiative. By contrast, in the US the FTC co-operates closely and successfully with the Digital Advertising Alliance. [Collin O'Malley, chief strategy officer at Evidon (privacy solutions provider)]

In de bestudeerde landen zijn, net als in Nederland, verschillende gebeurtenissen aan te wijzen die grote invloed hebben gehad op de wijze waarop met privacy en de bescherming van persoonsgegevens omgegaan wordt. De nasleep van de aanslagen op 11 september 2001 heeft met name in de Verenigde Staten, maar ook in Nederland, geleid tot wetgeving die de bevoegdheden van inlichtingendiensten en opsporingsinstanties sterk uitgebreid hebben, en die de privacyrechten van burgers ingeperkt hebben. Dergelijke incidenten vormen een krachtige barrière voor het tot stand komen van een effectieve privacybescherming.

Andere incidenten vormen juist een stimulans voor het formuleren van privacywetgeving of andere maatregelen die privacybescherming stimuleren. In Nederland heeft het (voorlopig) mislukken van het Elektronisch Patiënten Dossier een impuls gegeven aan het denken over privacy. In het Verenigd Koninkrijk is dat het geval door het grote afluisterschandaal waarbij journalisten bij de krant *The News of the World* telefoons afluisterden van bekende personen.

In vergelijking met Duitsland lijken Nederlanders zich minder zorgen te maken om hun privacy. Waar in Duitsland de introductie van de Google Street View dienst (waarbij alle straten met foto-auto's in beeld gebracht worden en op internet zichtbaar gemaakt) tot grote weerstand heeft geleid, en zelfs tot het bevriezen van deze dienst, is de invoering ervan in Nederland met vrij weinig rumoer gepaard gegaan. Aan de andere kant lijken bijvoorbeeld de burgers van het Verenigd Koninkrijk zich relatief weinig druk te maken om de uitzonderlijk grootschalige camerasurveillance die er plaatsvindt. Een naïeve aanname die gemaakt zou kunnen worden is dat culturen waarin individualisme krachtiger ontwikkeld is, de vraag om privacybescherming groter te zijn. Dit blijkt echter niet het geval te zijn, en zelfs in onze vergelijking omgekeerd te zijn: Duitsers hebben van de onderzochte landen de minst individualistische cultuur, maar zijn in de recente geschiedenis juist het meest in het nieuws geweest vanwege weerstand tegen privacyschendingen.

[24] Voorbeelden zijn privacy-vriendelijke locatie-gebaseerde diensten (http://www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf), realiseren van Privacy by Design in *smart grids* (http://www.privacybydesign.ca/content/uploads/2011/02/pbd-ont-smartgrid-casestudy.pdf) en een *proof of concept* van privacy-vriendelijke biometrische encryptie (http://www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf).

5.6.2.2 Innovatiekenmerken

Bij het wel of niet toepassen van *Privacy by Design* in de private sector is een belangrijke vraag: is het een valide propositie? Oftewel, wegen de baten tegen de kosten op? Het beeld wat door de internationale geïnterviewden geschetst wordt varieert. De toezichthouder van Ontario, Canada, geeft een volmondig “ja” op deze vraag: *Privacy by Design* betaalt zich terug. Naarmate boetes op privacyschendingen hoger worden, wetgeving meer transparantie over incidenten afdwingt en consumenten kritischer worden over de privacygerichtheid van een dienst wordt het aantrekkelijker voor bedrijven om hier werk van te maken. In de praktijk lijken consumenten echter lang niet altijd privacy als een belangrijk criterium te hanteren, en zijn ze een vrij onvoorspelbare factor. De schade en risico’s die gepaard gaan met het delen van persoonlijke informatie is niet direct waarneembaar voor consumenten.

“It’s better to have Privacy by Design than privacy by disaster
[Office of the Information and Privacy Commissioner of Ontario, Canada]

An advantage a private firm could derive from adopting Privacy by Design is building trust and reputation. In particular in markets where privacy surfaces as a key issue this could be an important benefit.[Ira Rubinstein, academische privacy expert in de Verenigde Staten]

De kosten die met het invoeren van *Privacy by Design* gepaard gaan worden door de internationaal geïnterviewden niet als zeer hoog ingeschat. Deze kosten zullen waarschijnlijk zichzelf terugverdienen door o.a. de hogere kans op het vermijden van andere uitgaven in de toekomst (bijv. in de vorm van boetes en compensatie voor het schenden van privacyregels). Er wordt echter een andere, belangrijkere overweging genoemd: bedrijven kunnen *Privacy by Design* zien als een beperking op de flexibiliteit en hun capaciteit om te innoveren en op nieuwe markten in te springen. De algemene insteek is: verzamel zoveel mogelijk data voor het geval het nuttig blijkt te zijn in de toekomst. Door voor een *Privacy by Design* aanpak te kiezen kan een bedrijf zichzelf beperkingen opleggen in toekomstige zakelijke keuzes. Waar sommige bedrijven een serieus competitief voordeel zullen proberen te behalen met een *Privacy by Design* aanpak, geldt voor veel andere bedrijven dat de potentiële kosten die privacyschendingen met zich mee brengen niet opwegen tegen de kosten of beperkingen die de aanpak met zich mee brengt:

A few companies may embrace something like competitive advantage and they may have a different approach. If the mainstream of companies would have to choose between costs versus legal requirements, then they will choose for abiding by the law. However they will try to stretch the law as far as they can. In a situation where there is no large sanction, then they actually care less for the law. They will take the risk of not implementing PbD and the costs of privacy breaches as a result. Today, privacy-breach sanctions are but pocket-money for companies.
[Prof. Dr. Sarah Spiekermann, University of Vienna]

Tot slot blijkt een belangrijk probleem te zijn dat een kosten-baten analyse moeilijk te maken is omdat bedrijven over weinig relevante data beschikken. Wat een bedrijf wil weten is welk niveau van investering passend is om de gewenste resultaten te bereiken. De aanname daarbij is dat bedrijven liever kosten willen minimaliseren en dus zo weinig mogelijk willen investeren.

Currently, there is too little data to do a good cost-benefit analysis. If someone would do a rigorous study, that would aid privacy advocates seeking to influence investment decisions within their organizations. [Ira Rubinstein, academische privacy expert in de Verenigde Staten]

5.6.2.3 Organisatiekenmerken

De internationaal geïnterviewden geven aan dat volwassen bedrijven gewoonlijk erkennen dat toezichthouders en regulering niet verdwijnen zullen, en dat ze daarmee zullen moeten leren leven. Daarbij zullen ze zoeken naar manieren om met die regulering om te gaan zodat ze in staat blijven te innoveren. Wat genoemd wordt is dat de uitdaging om *Privacy by Design* in te voeren dan ook vooral zit bij bedrijven die nog jong zijn, of zeer klein. De vraag die gesteld wordt is: hoe kan *Privacy by Design* als een *best practice* gestimuleerd worden zonder dat de innovatiekracht van met name start-ups daar onder leidt?

Tot slot is een interessant advies voor bedrijven om, als ze met *Privacy by Design* aan de slag willen gaan iemand in de eigen gelederen te zoeken die gepassioneerd over het onderwerp is en het bedrijf goed kent:

The main advice I would give to firms seeking to adopt Privacy by Design is to identify someone within its own ranks who is dedicated to this, and is really passionate about privacy. That person has to understand the firm's culture and the business and technical processes, and has to find a way to fit Privacy by Design into these processes. If it is viewed as something imposed from the outside – for example by governments, or consultants advising the CEO – engineers will see this as something to avoid, a matter of checking the boxes or filling in the paper work. The challenge is to get the staff to think of this as "just another engineering requirement". [Ira Rubinstein, academische privacy expert in de VS]

5.7 Analyse

5.7.1 Privacy by Design vanuit innovatieperspectief

Innovatie- en adoptieliteratuur beschrijven verschillende factoren die beïnvloeden of een organisatie geneigd is een innovatie toe te passen of niet. In dit hoofdstuk hebben we dit vanuit drie verschillende perspectieven bekeken: innovatiekenmerken (*performance expectancy* en *effort expectancy*), organisatiekenmerken en omgevingskenmerken.

Bij de innovatiekenmerken is de achterliggende gedachte dat naarmate een organisatie de *performance expectancy* (de mate waarin de organisatie gelooft dat de innovatie de organisatie beter zal doen presteren) hoger inschat en de *effort expectancy* (de moeite die het kost om de innovatie in te voeren in de organisatie) lager inschat, men eerder geneigd zal zijn een innovatie te adopteren. De perceptie van een hogere *performancy expectancy* en een lagere *effort expectancy* zijn daarmee in theorie stimulerende factoren voor het toepassen van *Privacy by Design*.

Uit het voorgaande wordt duidelijk dat slechts een beperkt aantal factoren bijdragen aan een hogere *performance expectancy* in de perceptie van de geïnterviewde organisaties. Dit zijn vooral de effectiviteit van PbD om privacyschendingen tegen te gaan en de relatie met *accountability* (het zichtbaar kunnen voldoen aan noodzakelijke regels). De overige factoren die *performance expectancy*

beïnvloeden, waaronder relatief voordeel en onderscheidend vermogen, herkenbaarheid, efficiëntere organisatie en financiële impact, vormen over het algemeen geen positieve prikkel. Zo lijkt *Privacy by Design* geen direct effect op de verkoop (oftewel het vergroten van de omzet) te hebben. Daar speelt mee dat PbD niet altijd even herkenbaar is voor klanten en consumenten. Bij data-intensieve bedrijven is er wel een expliciete behoefte voor PbD maar wordt het nog niet als *Unique Selling Point* beschouwd (zowel nationaal als internationaal). De organisatorische impact van de invoering van PbD op organisaties is groot. Bij verouderde systemen kan dit ook een kostbare aangelegenheid zijn. Bij nieuwe systemen is de implementatie van PbD tegen relatief geringe meerkosten te realiseren, maar is het lastig om de baten op lange termijn te kwantificeren – hoewel de perceptie is dat deze meerkosten niet opwegen tegen kosten om achteraf privacymaatregelen in te bouwen en de kosten van privacyschendingen. Ook zijn organisaties van mening dat de toepassing van PbD de organisatie niet direct efficiënter maakt. Ervaring is verder dat het verlies aan functionaliteit door toepassing van PbD wel voorkomt maar in de regel overkomelijk is. Uit de internationale interviews komt naar voren dat bedrijven PbD kunnen zien als een beperking op de flexibiliteit en hun capaciteit om op nieuwe markten in te springen.

De *effort expectancy* (de moeite die het kost om de innovatie in te voeren) wordt door de geïnterviewde organisaties als hoog ingeschat. Het realiseren van *Privacy by Design* in de organisatie is een complex en langdurig proces dat veel impact heeft op de organisatie. Dit heeft ook te maken met de aanwezigheid van de verouderde IT-systemen.

Daarnaast zijn er kernmerken van de organisatie en in de externe omgeving van de organisatie die een positieve of negatieve prikkel vormen om PbD toe te passen.
Binnen de organisatie komen leiderschap en organisatiecultuur naar voren als noodzakelijke voorwaarden om PbD toe te kunnen passen. Als het topmanagement niet achter de invoering van PbD staat is het voor een organisatie zeer lastig om PbD te realiseren. Het belang dat het topmanagement hecht aan privacybescherming is toegenomen omdat de kans op privacyschendingen – en de (negatieve) aandacht die dat met zich mee brengt – hoger wordt ingeschat dan een paar jaar geleden. Uit de internationale verkenning laat zien dat incidenten sterk sturend (of remmend) kunnen zijn in het adopteren van privacymaatregelen door organisaties.

In de externe omgeving valt de rol van de toezichthouder op. Het CBP komt middelen te kort om (strenger) te handhaven en partijen aan te sporen tot betere privacybescherming. Ook wordt een adviserende rol gemist. Uit de internationale verkenning komt de ondersteunende rol van de toezichthouder veel sterker naar voren, zoals in de VS en Canada. Verder ontbreekt de vraag van consumenten. In de London Economics studie (2010) werd dit als stimulerende factor geïdentificeerd, deze lijkt hier afwezig. Een ander belangrijk aspect in de externe omgeving is dat partijen op elkaar wachten. De aanbieders zien een te weinig gearticuleerde vraag bij het merendeel van hun klanten. De geïnterviewde dataverwerkers (voorlopers op het gebied van toepassing van privacybeschermende maatregelen) stellen een te afwachtende houding bij aanbieders vast; er wordt onvoldoende meegedacht bij het opstellen van contracten en mogelijkheden om PbD te implementeren. Het MKB heeft te weinig kennis in

huis om te weten wat PbD voor hun organisatie betekent en vaak te weinig resources beschikbaar om dit te kunnen toe passen.

Samenvattend zijn de belangrijkste stimulerende factoren voor de adoptie van PbD:

- De effectiviteit van PbD om de kans op privacyschendingen te verkleinen en een toenemend gepercipieerd risico van de kans op privacyschendingen
- De relatie met *accountability* en daarmee zichtbaar maken dat de organisatie aan de norm voldoet
- Leiderschap; de aandacht en houding van het topmanagement ten aanzien van privacybeschermende maatregelen

De belangrijkste remmende/vertragende factoren voor de toepassing van PbD zijn:

- De (organisatorische) impact op de organisatie
- De aanwezigheid van verouderde IT-systemen
- Partijen die op elkaar wachten
- Gebrek aan bewustzijn van privacybescherming en PbD (met name bij MKB)
- De beperkte rol van de toezichthouder om op te treden tegen privacyschendingen en onvoldoende mogelijkheden voor advisering
- Complexiteit wetgeving

Daarnaast zijn er factoren die geen positieve of negatieve stimulans zijn maar feitelijk 'afwezig' zijn. Voorbeelden zijn het onderscheidend vermogen van *Privacy by Design* en *Privacy by Design* als *Unique Selling Point* (USP). Wanneer PbD als USP gezien wordt, is dit een positieve drijfveer. Bij afwezigheid is het niet direct een belemmerende factor maar kan het wel bepalend zijn voor de toepassing (of de beslissing daarover) van PbD, o.a. omdat het niet bijdraagt aan een hogere *performance expectancy*.

5.7.2 Reflectie op conceptueel kader

In hoofdstuk 3 is uiteengezet wat in de literatuur verstaan wordt onder *Privacy by Design* en langs welke lijnen dit in de regel vaak wordt ingevuld: 1) een bescherming die gericht is op het vergroten van de transparantie van de gegevensverwerking (*Privacy by Policy*) en 2) een bescherming die gericht is op het tegengaan van misbruik van gegevens (*Privacy by Architecture*). Beide kunnen zowel via organisatorische als technische maatregelen worden georganiseerd. Het empirisch onderzoek laat zien dat alle combinaties in de praktijk voorkomen, hoewel de nadruk ligt op '*privacy by policy*' via zowel technische als organisatorische maatregelen. Afschermende maatregelen, zoals minimale gegevensverzameling of 'client side gegevensverwerking', komen in de praktijk minder vaak voor.

Tabel 9 Dimensies en benaderingen van privacybescherming

	Transparantie Privacy governance 'Privacy by policy'	**Afscherming Privacybescherming 'Privacy by Architecture'**
Organisatorisch	Audits Privacy officers …	Toegang via pseudoniemen Access management …
Technologisch	Log files Data base audit interfaces Transparantietools	Anonimisering Zero knowledge proofs Client side gegevensverwerking

Uit de empirische resultaten vallen verschillende fasen op te maken in de ontwikkeling die organisaties doormaken als het gaat om dataprotectie en privacybescherming. Veel bedrijven zijn begonnen met informatiebeveiliging, accessmanagement, het uitvoeren van (verkorte) PIA's en de aanstelling van *Privacy Officers* (*Privacy by Policy*) en maken vervolgens de stap naar het opstellen van een integraal privacybeleid waarbij ook gekeken wordt naar afschermende maatregelen (*Privacy by Architecture*). Organisaties geven aan dat van de implementatie van '*Privacy by Policy*' naar '*Privacy by Architecture*' een extra stap vraagt van organisaties. Het is hierbij opvallend dat organisaties tegelijkertijd aangeven dat de kosten van *Privacy by Policy* veel hoger worden ingeschat dan de kosten van *Privacy by Architecture*.

Daarnaast ligt in de regel de nadruk op dataprotectie en minder op privacybescherming. Dit kan er toe leiden dat een organisatie verschillende dataprotectiemaatregelen heeft genomen en voldoet aan de eisen rondom dataprotectie maar privacyschendingen nog steeds mogelijk zijn. In hoofdstuk drie is het verschil tussen beide begrippen toegelicht.

De rol van personen van wie gegevens worden geregistreerd in het systeemontwerp en privacyverantwoordelijkheden is niet naar voren gekomen in ons empirisch onderzoek.

Slechts een aantal organisaties geeft aan de ontwikkelingen rondom de herziening van de Europese dataprotectierichtlijn te volgen en te kijken wat dit voor gevolgen heeft voor de organisatie. Sommige organisaties zijn voorbereid op de mogelijke verplichtstelling van *Privacy Impact Assessments* en verwachten (eventueel met bijstelling) hier aan te kunnen voldoen. Een verdere standaardisering van de uitvoering van PIA's kan organisaties ook meer handvatten bieden. Een enkele organisatie geeft aan bezorgd te zijn dat voorstanders van PIA en PbD het instrument of concept mogelijk belangrijker vinden dan de uitkomst. Het 'recht om vergeten te worden' is lastiger uit te voeren, met name voor organisaties die vanuit een andere hoek te maken krijgen met retentiewetgeving. Een aantal geïnterviewde partijen vinden het 'recht om vergeten te worden' wel een goede oplossing voor sommige databases of programma's. Dataportabiliteit, de mogelijkheid tot hogere boetes en andere voorgestelde wijzigingen zijn door organisaties niet genoemd.

5.7.3 Privacy by Design vanuit beleidsperspectief

Nu we de belangrijkste bevindingen uit de empirische resultaten hebben weergegeven, zetten we in deze paragraaf een volgende stap naar het analyseren en duiden van deze resultaten. Doel van deze studie is om meer zicht te verkrijgen op stimulerende en remmende factoren voor diffusie en adoptie van *Privacy by Design*. Deze factoren hebben we gekoppeld aan een conceptuele benadering van innovatie en diffusie via een daartoe aangepast UTAUT model. We hebben meer gekeken naar factoren die van belang zijn voor organisaties dan voor individuen. Het zijn in de regel immers organisaties die een (strategisch) besluit moeten nemen of ze een bepaald systeem, methode of techniek in de bedrijfsvoering en in de te verkopen producten en/of diensten opnemen. Binnen deze organisaties zijn het wel weer individuen die een belangrijke rol spelen bij het nemen van deze besluiten maar hun verantwoordelijkheid ligt vooral bij het nemen van goede besluiten voor de organisatie.

Een subdoel van deze studie is om te kijken naar de rol van de overheid bij het bevorderen van de stimulerende factoren en het wegnemen van barrières. Door *Privacy by Design* als innovatie te benaderen gaat het om de vraag of dit een innovatie is waarvan de overheid vindt dat die de moeite waard is om via gericht beleid te stimuleren en barrières te slechten. Deze vraag beantwoorden we niet in deze studie. Voor een deel is dit een beleidsmatige vraag die afhangt van het beleidskader dat de overheid ontwikkelt met betrekking tot privacy en gegevensbescherming. Voor een deel is dit een politieke vraag naar het belang van deze bescherming. In de huidige beleidsdocumenten zijn voldoende aanwijzingen te vinden dat de overheid belang hecht aan een goede verankering van de bescherming van de privacy en een adequate benadering van gegevensbescherming (ELI, Digitale Agenda 2011). Dat is voor nu voldoende basis.

In onze analyse hanteren we een kader dat mogelijkheden biedt om beleidsopties voor de overheid te identificeren. Dit kader betreft de analyse van imperfecties in de markt en imperfecties in het innovatiesysteem (zie ook hoofdstuk 4). Analyse vanuit dit raamwerk maakt duidelijk wat succesvolle of stimulerende strategieën voor diffusie en adoptie kunnen zijn. In deze paragraaf presenteren we eerst de gevonden vormen van beide typen imperfecties. Vervolgens lopen we de verschillende vormen een voor een af en bespreken hoe deze vormen van falen tegen kunnen worden gegaan.

5.7.4 Imperfecties in de markt en in innovatiesystemen

We herhalen hier het schema dat we in hoofdstuk 3 hebben gepresenteerd en we geven er de aangetroffen vormen van imperfecties in de makrt en in innovatiesystemen bij de diffusie en adoptie van *Privacy by Design* bij.

Tabel 10 Overzicht elementen van imperfecties in markt en innovatiesystemen

Imperfecties in de markt	Imperfecties in het innovatiesysteem
Positieve externaliteiten *Weinig aandacht voor maatschappelijke voordelen. Baten zijn lastig te kwantificeren.*	**Belemmeringen in infrastructurele voorzieningen en investeringen** *Niet gevonden*
Publieke goederen en toe-eigening *Niet gevonden*	**Lock-in en padafhankelijkheid** *Groot probleem bij legacysystemen. Belemmert adoptie van privacyvriendelijke alternatieven*
Informatie-asymmetrie *Niet gevonden*	**Institutionele belemmeringen** *Gebrek aan harmonisatie; complexe wetten; toezichthouder met beperkte middelen en slagkracht*
Niet-effectieve marktwerking *Grote bedrijven zetten de toon met betrekking tot het belang van* Privacy by Design. *Dat maakt markttoetreding voor kleinere bedrijven met innovatieve aanpakken moeilijker.*	**Falende interacties** *Te weinig interactie tussen verschillende partijen. Gebrekkige informatie-uitwisseling over wensen, behoeften, oplossingen en best practices*
	Onvoldoende vaardigheden en kennis *Probleem bij volgers*

5.7.4.1 Imperfecties in de markt

Positieve externaliteiten: Deze vorm van imperfecties in de markt wijst op aanwezige voordelen van innovatie die echter te ver afstaan van de innoverende partij om deze als reëel in te boeken. Bij *Privacy by Design* is deze imperfectie zichtbaar. Ten eerste is sprake van maatschappelijke voordelen (zorgvuldiger omgang met persoonsgegevens, minder kans op schendingen of fouten) die door bedrijven niet altijd als zodanig herkenbaar zijn of als (bedrijfsmatige) voordelen (kunnen) worden ingeboekt. Zeker waar het gaat om bedrijven die hun bedrijvigheid halen uit de omgang met persoonsgegevens is een spanning waarneembaar tussen het meer generieke maatschappelijke voordeel en het directe bedrijfsbelang. Tegelijkertijd is de maatschappelijke dimensie voor deze bedrijven zonder meer van belang, omdat negatieve ervaringen hun weerslag zullen hebben op de zakelijke mogelijkheden. Ten tweede zijn de voordelen voor de bedrijfsvoering (efficiëntie van bedrijfsprocessen, effectiviteit van maatregelen die demonstreren dat het bedrijf alles op orde heeft) moeilijk te kwantificeren en soms ook pas in een verdere toekomst in te boeken. Soms vallen de voordelen aan de personen van wie gegevens worden geregistreerd toe terwijl de kosten om deze voordelen in te boeken aan de bedrijven toevallen. Dit leidt ertoe dat de *business case* voor *Privacy by Design* moeilijk is vast te stellen. Dit maakt het moeilijk om deze voordelen in de bedrijfsstrategie op waarde mee te wegen. De waarde is immers moeilijk vast te stellen. Dit zou anders worden als consumenten bereid zouden worden om te betalen voor meer privacybescherming en als PbD aantoonbaar (i.e. kwantificeerbaar) in staat is om privacyschendingen te verkleinen.

Informatie-asymmetrie: Informatie-asymmetrie speelt tussen actoren in een keten. Het gaat om de informatievoorsprong die de ene partij heeft ten opzichte van een andere partij omdat die ene partij dichter bij de bron van de informatie zit. In het geval van *Privacy by Design* hebben systeemleveranciers en de voorlopende bedrijven beide naar eigen zeggen voldoende informatie over mogelijke oplossingen en mogelijke implementatiestrategieën. Volgende partijen hebben wel een informatieachterstand maar deze wordt niet uitgebuit door systeemleveranciers. Integendeel, door het ontbreken van een vraag bij de volgende partijen stellen systeemleveranciers zich terughoudend op bij hun aanbod van PbD. Dit type imperfectie hebben we dan ook niet aangetroffen in deze studie.

Niet-effectieve marktwerking: Er is geen sprake van marktdominantie in de zin dat één speler andere spelers overvleugelt en daarmee (met een zelfde type aanbod) de markt domineert. Voor deze traditionele vorm van marktdominantie is de markt nog niet voldoende volwassen. Hooguit is sprake van een niet-effectieve marktwerking doordat vragende partijen (de dataverwerkers) meer verwachten van de aanbiedende partijen waar deze aanbieders (de systeemleveranciers) vanwege het ontbreken van voldoende (en voldoende gearticuleerde) vraag nog afwachtend zijn. Ook is sprake van een vorm van strategische oriëntatie door grote spelers met betrekking tot het belang van *Privacy by Design* waardoor met name kleine(re) en innovatieve(re) bedrijven het moeilijker hebben om de markt te betreden. Dit heeft ook te maken met lock-in en padafhankelijkheid (zie een van de volgende secties).

Van de genoemde soorten van imperfecties is alleen het probleem om positieve externaliteiten voldoende zichtbaar te krijgen en ze daardoor mee te kunnen wegen bij investeringsbeslissingen duidelijk zichtbaar. Voor de andere drie geldt dat ze niet

aangetroffen zijn of slechts in een indirecte vorm. Uit de interviews spreekt een opstartende markt waarin voorlopers met elkaar definiëren hoe deze markt eruit moet komen te zien. De aanbieders zijn nog bezig met een proces van strategische positionering, verkenning van de behoefte aan systemen, tools en methodes en een verkenning van de beste benadering van de vragende partijen. De vragende partijen op hun beurt hebben ofwel voldoende kennis in huis om tot op zekere hoogte zelf ook de benodigde systemen, tools en methodes te ontwikkelen of zijn in zekere zin nog niet toe aan het voldoende articuleren van een vraag. Hoewel vormen van informatie-asymmetrie en van marktdominantie door vragende partijen is aan te geven, is er geen sprake van bewust in stand gehouden informatie-asymmetrie uit marktoverwegingen of van een dominante speler aan de aanbodszijde die het functioneren van een normaal opererende markt belemmert.

5.7.4.2 Imperfecties in het innovatiesysteem

Hier hebben we vijf soorten van imperfecties onderscheiden:

Belemmeringen in infrastructurele voorzieningen en investeringen: In een goed functionerend innovatiesysteem is sprake van een voldoende aanbod van infrastructurele voorzieningen waarlangs de innovaties verder ontwikkeld en verspreid kunnen worden. Onder deze infrastructurele voorzieningen vallen fysieke infrastructuren zoals netwerken (bijv,. in het geval van energievoorzieningen of telecommunicatievoorzieningen) en andere voorzieningen zoals onderzoeksprogramma's en testfaciliteiten. Het zijn investeringen die de overheid kan plegen omdat ze a. niet door afzonderlijke marktpartijen zijn op te brengen of b. de opbrengsten niet aan afzonderlijke marktpartijen zijn toe te bedelen. Deze imperfectie hebben we in de studie niet aangetroffen. Er is voldoende kennis beschikbaar en deze kennis is ook voldoende toegankelijk voor de marktpartijen. Er is geen roep om testfaciliteiten of onderzoeksprogramma's. De roep om advisering over goede (juridisch juiste) oplossingen en om deling van kennis over *best practices* heeft te maken met falende interacties (zie een van de volgende secties).

Lock in en padafhankelijkheid: Een groot probleem bij de invoering van *Privacy by Design* is de toepassing ervan bij al bestaande systemen. De ervaring die uit de interviews spreekt is dat toepassing bij nieuwe systemen weinig effect hoeft te hebben op de functionaliteit van een systeem of dat sprake is van geaccepteerd verlies van een bepaalde functionaliteit in de afweging tegen een hogere opbrengst in transparantie en *accountability*. Dit ligt anders bij aanpassing van al bestaande systemen (het *legacy*probleem). Als *Privacy by Design* niet van meet af een rol heeft gespeeld bij de systeemontwikkeling blijkt het praktisch erg lastig om dit op een later moment alsnog toe te voegen zonder dat hiervoor hoge kosten gemaakt moeten worden (door een grondige systeemherziening en investeringen in de organisatie om met het nieuwe systeem en de daarbij behorende spelregels te leren omgaan). Hier dringt zich de parallel met de ontwikkelingen rond duurzame energie op, waar ook pas daadwerkelijk duurzame winst wordt geboekt wanneer overgegaan wordt van *end-of-pipe* technologie (het plaatsen van roetfilters bijvoorbeeld) naar een duurzaam systeemontwerp. In het geval van *Privacy by Design* gaat het om een geïntegreerde aanpak in een zo vroeg mogelijke fase van systeemontwerp zodat ook later aanpassingen gemaakt kunnen worden die blijven passen. Deze imperfectie is moeilijk aan te pakken bij bestaande systemen. Het gaat er vooral om dat bij nieuwe systemen *Privacy by Design* vanaf het vroegste

ontwerp wordt meegenomen, mits markt- en maatschappelijke overwegingen dit ook verkieslijk maken. Bedrijven die alternatieve business concepten rond *Privacy by Design* aanbieden hebben vanwege hun oriëntatie op nieuwe aanpakken een extra drempel te overwinnen. Ze opereren in een niche-markt en moeten zich zichtbaar maken in de huidige markt waarin PbD nog geen gemeengoed is.

Institutionele belemmeringen: Een belangrijke overweging voor marktpartijen om na te denken over hoe (onderdelen van) *Privacy by Design* toe te passen is ingegeven door het wettelijke kader en de mogelijke aanscherping van dit kader. Aan die kant zijn dus geen belemmeringen. Wel is er sprake van een harde institutionele belemmering aan de kant van de toezichthouder. Algemeen wordt benadrukt dat de toezichthouder te weinig zichtbaar is om effectief te zijn. De geinterviewden ervaren geen positieve prikkels van de toezichthouder om actief met *Privacy by design* aan de slag te gaan. Ook wordt een rol gemist van een platform waar partijen terecht kunnen voor advisering en uitleg over de (als complex ervaren) wetten waar bedrijven mee te maken hebben. Geïnterviewden constateren dat de toezichthouder niet of nauwelijks een rol speelt bij de beslissing van de organisatie om *Privacy by Design* toe te passen. Indien er vanuit de politiek meer gewicht wordt gegeven aan het belang van adequaat toezicht kan dit stimulerend werken op organisaties die zich onderscheiden door een verantwoorde en passende omgang met persoonsgegevens. Daarnaast geven geïnterviewden aan dat de wetgeving complex is (ze laat ruimte voor interpretatie) en internationaal (vooral in Europa) niet geharmoniseerd is. De voorgestelde herziening van de dataprotectierichtlijn zal een verordening zijn en adresseert dit probleem daarmee in elk geval in Europa.

Falende interacties*:* Uit de interviews kwam naar voren dat er behoefte is aan informatie-uitwisseling en kennisdeling over oplossingen en *best practices* bij zowel vragende als aanbiedende partijen. Vragende partijen (dataverwerkers) hebben behoefte aan gestandaardiseerde en indien mogelijk ook gecertificeerde oplossingen omdat ze daarmee weten waar ze aan dienen te voldoen. Aanbiedende partijen kunnen dit nog niet leveren, omdat ook zij niet weten wat de beste oplossing is. De falende interactie heeft betrekking op de complexiteit van de situatie waarin verschillende disciplinaire achtergronden (technische, organisatorische, juridische kennis) bij elkaar moeten worden gebracht. Dat is geen eenvoudige zaak. Voor de aanpak van deze systeemimperfectie zijn verschillende oplossingen denkbaar. Daar komen we in de slotparagraaf op terug.

Onvoldoende vaardigheden en kennis: Duidelijk is dat de complexiteit van toepassing van *Privacy by Design* waarin sprake is van samenhangende technologische, organisatorische en bedrijfsmaatregelen, vraagt om specifieke vaardigheden en kennis. Bij grote bedrijven wordt dit intern georganiseerd (waarbij de *Privacy Officer* een rol kan spelen), ingekocht of van externen gevraagd, maar voor kleinere bedrijven legt dit mogelijk een te groot beslag op middelen. Tegelijkertijd knelt het ontbreken van voldoende vaardigheden en kennis omdat – in combinatie met het *legacy*probleem – ook bij nieuwe systemen dan niet wordt nagedacht over de mogelijkheid om *Privacy by Design* (in welke vorm dan ook) toe te passen en er dus sprake is van onvoldoende vraagarticulatie. Zolang consumenten hier niet expliciet om vragen, aanbieders het niet noodzakelijk in hun aanbod verwerken en partijen ook niet afgerekend worden op het ontbreken van *Privacy by Design* in producten, diensten en bedrijfsvoering kan en mag niet

verwacht worden dat partijen door eigen investeringen vaardigheden en kennis op dit terrein verwerven.

De verschillende soorten van imperfecties in het innovatiesysteem die we geconstateerd hebben, hebben voor een deel te maken met een systeem in opbouw (falende interacties en ontoereikende vaardigheden en kennis) en voor een deel met kenmerken van de inrichting van het systeem (rol toezichthouder, *legacy*systemen). Een deel van deze imperfecties kan met gerichte interventies worden weggenomen, een ander deel is moeilijker aan te pakken. In het slothoofdstuk presenteren we enkele aanbevelingen om deze imperfecties aan te pakken, mocht dit vanuit politieke en beleidsmatige overwegingen gewenst zijn.

6 Conclusies en aanbevelingen

Het doel van de studie naar remmende en stimulerende factoren voor de invoering en toepassing van *Privacy by Design* was het verkrijgen van een beeld over deze remmende en stimulerende factoren vanuit de benadering van *Privacy by Design* als innovatie. Deze studie heeft het inzicht vergroot in de achtergrond van de remmende en stimulerende factoren en geeft aan hoe dit vanuit innovatietheorie begrepen kan worden.

Daarnaast hebben we de resultaten geplaatst in een kader dat inzichtelijk maakt welke imperfecties in de markt en in het innovatiesysteem zichtbaar zijn bij de hedendaagse invoering en toepassing van *Privacy by Design*. Door deze benadering wordt het ook mogelijk om de stap te zetten naar het benoemen van de interventies die gepleegd kunnen worden om de gesignaleerde kimperfecties aan te pakken. De vraag of deze interventies inderdaad gepleegd moeten worden, en zo ja, door wie, valt buiten de scope van dit onderzoek. Omdat privacy steeds vaker genoemd wordt als issue hebben we een studie uitgevoerd die ons begrip van het (maatschappelijk) krachtenveld rond de bescherming van privacy zou vergroten. De rol die de overheid zou kunnen spelen is daar geen expliciet aandachtspunt in geweest.

Bij het vaststellen van interventiestrategieën gaat het wel om de rol van de overheid. In de studie hebben we evenwel niet gekeken naar het beleid van de overheid. We hebben ook niet onderzocht in hoeverre *Privacy by Design* op de agenda van het huidige kabinet staat. De volgende overwegingen maken het evenwel aannemelijk dat de overheid haar voordeel kan doen met de geïdentificeerde interventiestrategieën:

1. Het Kabinet krijgt van tijd tot tijd verzoeken van het parlement om inzicht te geven in de wijze waarop het omgaat met privacy en de bescherming van persoonsgegevens.[25]
2. In de Digitale Agenda Nederland vormen privacy en identiteitsmanagement aandachtspunten.
3. Dit heeft tevens geleid tot opname van privacy en identiteitsmanagement in het topsectorenbeleid, met name in de topsectoren ICT en Creative Industrie.

In het navolgende koppelen we de gesignaleerde soorten van imperfecties aan mogelijke interventies door de overheid. Deze helpen de rationale van overheidsinterventie scherp te krijgen. De rationale geeft richting aan mogelijke instrumenten. Deze interventies zijn ingegeven door één van de volgende typen beleidsinstrumenten (Poel & Kool, 2009):

1. Overheidsvoorzieningen: is er behoefte aan aanvullende infrastructurele voorzieningen en faciliteiten? Is er behoefte aan testfaciliteiten die de markt niet zelf zal organiseren vanwege te beperkt belang per marktpartij?
2. Financiële instrumenten: Is er behoefte aan subsidies, aan onderzoeksprogramma's om bepaalde kennishiaten op te vullen?
3. Regulering: Is er behoefte aan bijstelling van/aanvulling op het wettelijk kader?

[25] Zoals recentelijk het verzoek zoals neergelegd in de Motie Gesthuizen/Verhoeve (Kamerstuk, 24 095, nr. 294).

4. Informatie: Is er behoefte aan meer kennis en informatie? Is er behoefte aan een bundeling van kennis/informatie?
5. Vraag door publieke organisaties: Is er behoefte aan een rol van de overheid als *launching customer* om daarmee vraagarticulatie en vraagbundeling te bevorderen?

6.1 Positieve externaliteiten/spillovers

Bij deze imperfectie speelt het probleem dat het voor marktpartijen moeilijk is om voldoende duidelijkheid te verkrijgen over de baten. Deze baten vallen soms aan derden toe (de maatschappij, individuen over wie gegevens verzameld en gebruikt worden), terwijl de eventuele baten voor de marktpartij zelf moeilijk te kwantificeren zijn en daardoor geen rol spelen bij het opstellen van een kosten-batenanalyse voor invoering/toepassing van Privacy by Design.

Deze imperrfectie kan weggenomen worden door deze externe baten wel inzichtelijk te maken en door te bestuderen hoe deze baten voor bedrijven zijn mee te nemen als onderdeel van een business case. Dit vraagt om onderzoek naar de verduidelijking van de externe baten en naar onderzoek van het opstellen van business cases. Het instellen van een platform dat verschillende belanghebbenden bij elkaar zet (consumentenorganisaties, bedrijven, aanbieders) kan het proces van kennisdeling en kennisopbouw versnellen.

6.2 Niet-effectieve marktwerking

Bij deze imperfectie speelt het probleem van een onvoldoende gearticuleerde vraag en van een strategische oriëntatie van grote spelers die het belang van *Privacy by Design* minder hoog inschatten.

Om deze imperfectie weg te nemen is ondersteuning van de vraagarticulatie nodig. Dit kan door de organisatie van voorlichting die gericht is op het verduidelijken van vragen waar (kleinere) spelers mee zitten: wat is er beschikbaar aan privacytools en methoden, hoe is dit in bestaande diensten/processen in te passen, hoe is dit in nieuwe diensten/processen in te passen, welke voordelen/nadelen zitten er aan de verschillende opties? Een voorlichtingscampagne kan ook tot doel hebben om bekendheid te geven aan het vraagstuk. Geïnteresseerde brancheorganisaties zouden in samenwerking met de overheid zich achter deze voorlichting kunnen scharen. De aankomende herziening van de huidige dataprotectierichtlijn kan een extra motivatie vormen voor brancheorganisaties om dit op te pakken.

6.3 Lock-in en padafhankelijkheid

Bij deze imperfectie in het innovatiesysteem speelt het legacyprobleem en onzekerheid over de vraag wat de beste aanpak is – ook of juist gericht op het voorkomen van toekomstige lock-in dan wel padafhankelijkheden.

Om deze imperfectie tegen te gaan kan gedacht worden aan een proces van standaardisering van privacydiensten die ook op langere termijn zekerheid bieden dat de juiste weg ingeslagen is. Dit kan leiden tot processen van certificering die de standaarden een grotere robuustheid meegeven. Dit geldt bijvoorbeeld voor de toe te passen Privacy Impact Assessments. Standaardisering en eventuele certificering

draagt bij aan professionalisering van de aanpak van privacy in de bedrijfsvoering. Dit pakt het legacyprobleem evenwel niet aan. Daarvoor is meer kennis nodig over de te leveren technische en organisatorische inspanningen om tot een betere waarborging van de privacy te komen.

6.4 Institutionele belemmeringen

Hier speelt enerzijds het probleem van wettelijke uitwerkingen die in verschillende landen verschillend zijn, en in Nederland het probleem dat de toezichthouder te weinig instrumenten heeft om effectief te opereren.

Het eerste probleem kan weggenomen worden door harmonisatie van internationale wetgeving. Binnen Europa worden hiertoe stappen gezet door het voorstel voor een verordening voor dataprotectie. Deze verordening moet op termijn de huidige richtlijn vervangen. Waar een richtlijn minimumeisen formuleert (en dus in bepaalde landen tot strengere eisen kan leiden dan in andere) moet een verordening rechtstreeks in nationale wetgeving geïmplementeerd worden. Dit is een stap in de goede richting. In de verordening zijn ook de mogelijk uit te delen boetes aanzienlijk verhoogd. De vraag of er ook mogelijkheden tot uitbreiding van de rol van de toezichthouder zijn, het pakket aan gehanteerde instrumenten door de toezichthouder en daarmee de effectiviteit van het optreden van de toezichthouder te vergroten, is een politieke.

6.5 Falende interacties

Bij deze imperfectie speelt het gebrek aan voldoende gedeelde kennis die voor alle partijen in de keten begrijpelijk en hanteerbaar is. Dit geldt bijvoorbeeld voor de vertaling van juridische kennis naar praktisch toepasbare technische kennis en andersom. Invoering van *Privacy by Design* vraagt om een multidisciplinaire kennisbenadering en dat is een verre van eenvoudige zaak.

De aanpak zou kunnen bestaan uit het articuleren van *best practices* die vanuit de verschillende perspectieven inzichtelijk maken hoe juridische kennis, organisatorische en technologische kennis op elkaar in kunnen werken en welke keuzes daarin gemaakt kunnen worden. Een platform waar deze kennisdeling georganiseerd en toegankelijk gemaakt kan worden is een manier om dit probleem aan te pakken. Een programma dat zich richt op de bestudering van *best practices* en *lessons learned* is een andere manier.

6.6 Onvoldoende vaardigheden en kennis

De complexiteit van de introductie van *Privacy by Design* vraagt om een voldoende toegeruste organisatie om deze introductie goed te managen. Kennis en vaardigheden over hoe dit te doen zijn onvoldoende aanwezig. De *Privacy Officer* die sommige organisaties hebben ingesteld, speelt hier een belangrijke rol. Maar niet alle organisaties kunnen zich dat veroorloven, terwijl ze wel met vergelijkbare vragen te maken krijgen.

Het ondersteunen van deze organisaties door middel van voorlichtingscampagnes, en cursussen/onderwijsmateriaal voor gerichte training van mensen binnen de

organisatie zijn twee manieren om deze kloof in kennis te overbruggen. Ook hier kunnen brancheorganisaties een rol spelen.

6.7 Ter afsluiting

De meeste instrumenten die in het voorgaande zijn genoemd, hebben betrekken op het initiëren van samenwerkingsverbanden, een platform dat zorgdraagt voor expertisebundeling, spreiding van kennis en gerichte benadering van vragen, training, informatie en voorlichtingscampagnes en op de rol van de overheid als *launching customer*. Instrumenten van financiële aard (subsidies, onderzoeksprogramma's) lijken minder van belang om de gesignaleerde imperfecties aan te pakken.

7 Literatuurlijst

Acquisti, A., Friedman, A., Telang, R. (2006) Is There a Cost to Privacy Breaches? An Event Study," Proceedings of the International Conference of Information Systems (ICIS), 2006. Available at http://www.heinz.cmu.edu/~acquisti/research.htm

Acquisti, A., John, L., en Loewenstein, G. (2010) *What is privacy worth?* Leading paper, 2010 Future of Privacy Forum's Best "Privacy Papers for Policy Makers"

Buttarelli, G. (2010), The Surveillance Policy in Europe, today and tomorrow, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-01-22_Namur_surveillance_EN.pdf (geraadpleegd 14 maart 2012)

Booz en Company (2008) *Digital Confidence: Sleutel tot de digitale groei van morgen*. Liberty Global Policy Series (in het Nederlands vertaald).

Borking J. (2010). *Privacyrecht is code – over het gebruik van Privacy Enhancing Technologies*. Kluwer, Deventer.

Burgoon, J., Parrott, R., LePoire, B., Kelley, D., Walther, J., Perry, D. (1989) Maintaining and restoring privacy through communication in different types of relationship. *Journal of Social and Personal Relationships* 6, pp. 131–158

Cavoukian, A. (2009), *Privacy by design – take the challenge*. Ontario: Privacy Commissioner.

Chuttur M.Y. (2009). *"Overview of the Technology Acceptance Model: Origins, Developments and Future Directions* ," Indiana University, USA . Sprouts: Working Papers on Information Systems, 9(37).

Davis, F (1993). User-acceptance of computer-technology: system characteristics, user perceptions. Int. J*. Man-Machine Studies* 38 (3), pp. 475-83.

Davis, F. & Venkatesh V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments*. Int J. Human Studies* 45(1), 19-45

Europese Commissie (1995) *Richtlijn van het Europees Parlement en de Europese Raad. 'Over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens'* (95/46/EC) Brussel, 24 oktober 1995.

Europese Commissie (2010) *A comprehensive approach on personal data protection in the European Union* COM(2010) 609 final, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (accessed 4 March 2011).

Europese Commissie (2012) *Voorstel voor een Verordening van het Europees Parlement en de Europese Raad. 'Over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens'* COM(2012)11 final. 25 januari 2012.

Europese Gemeenschap (2000) *Handvest van de Grondrechten van de Europese Unie,* (2000/C 364/01) www.europarl.europa.eu/charter/pdf/text_nl.pdf (geraadpleegd 14 maart 2012)

Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Yves Poullet et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. Forthcoming.

Gürses S., Troncoso C, and Diaz C (2011). *'Engineering Privacy by Design'*, paper University of Leuven.

Gustafsson, R. and E. Autio (2006): *Grounding for Innovation Policy: The Market, System and Social Cognitive Failure Rationales*. Paper presented at Innovation Pressure – Rethinking Competitiveness, Policy and the Society in a Globalised Economy – International ProACT conference, Tampere, Finland, March 15-17, 2006

Gutwirth, S., Gellert, R., Bellanova, R., Friedewald, M., Schütz, P., Wright, D., Mordini, E., Venier, S. (2011) *Legal, social, economic and ethical conceptualizations of privacy and data protection*, deliverable D1, Prescient – Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment.

IDC (2011) *Extracting Value from chaos*, http://www.emc.com/digital_universe.

ITRE (2011) *Does it help or hinder? Internet innovation and the citizens' right to privacy*. IP/A/ITRE/ST/2011-10

Koorn R, Gils H van, Hart J ter, Overbeek P, Tellegen R (2004). *Privacy Enhancing Technologies - Witboek voor beslissers*. Den Haag: Ministerie van Binnenlandse Zaken.

Lieshout M van, Kool L, Schoonhoven B van, Jonge M de (2011).'Privacy by design: an alternative to existing practices in safeguarding privacy'. *INFO - The Journal of policy, regulation and strategy for telecommunciations, information and media*, vol. 13, no. 6, pp. 55-68.

London Economics (2010) *Study on the economic benefits of Privacy Enhancing Technologies (PETs).* Report for the European Commission DG Justice, Freedom and Security

Maillart, T. and D. Sornette (2010) "Heavy-tailed distribution of cyber-risks", *Eur. Phys. J. B* 75, 357-364.

McKinsey (2011) *Big data: The next frontier for innovation, competition, and productivity.* McKinsey Global Institute, http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation

OECD (1980) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

OECD (2009) Online identity theft. OECD, Paris.

Pariser, E. (2011) *The Filter bubble: what the internet is hiding from you.* New York: The Penguin Press, 2011.

Poel en Kool (2009) "Innovation in information society policy: rationale, policy mix and impact in The Netherlands", *Info*, Vol. 11 Iss: 6, pp.51 - 68

Poel, M., Kool, L., en Giessen, A. van der (2009) *Afwegingskader voor ICT-beleid: Rationale, coördinatie en samenwerking.* TNO rapport

Regan, P (1995) *Legislating Privacy: Technology, social values and public policy*. University of North Carolina Press, Chapel Hill.

Schurink, W., *Elektronisch berichtenverkeer met de overheid: last of lust?, Onderzoek naar relevante factoren voor de adoptie van elektronisch berichtenverkeer, Open Universiteit, 3 juli 2006.*

Roosendaal, A (2010), *Facebook Tracks and Traces Everyone: Like This!* Tilburg Law School Research Paper No. 03/2011. Available at SSRN: http://ssrn.com/abstract=1717563 or http://dx.doi.org/10.2139/ssrn.1717563

Solove D (2008). *Understanding privacy*. Harvard UP, Cambridge

Spiekermann S. and Cranor L. (2009). 'Engineering privacy', IEEE Transactions on Software Engineering, vol. 35, no. 1, 67-82.

Spiekermann, S., J. Grossklags, and B. Berendt, 2001. "E-privacy In 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior.*" Proceedings of the ACM Conference on Electronic Commerce*, pp. 38–47.

Steen. M (2011). *Upon opening the black bo of participatory design and finding it filled with ethics.* Presentation Nordes 2011 Conference.

TNO (2009). *Perceptieonderzoek Veilig Internet: Onderzoek naar de ruimte tussen wat (on)veilig is en wat als zodanig gepercipieerd wordt.* Huveneers, S. en Geers, M. TNO-rapport, nr. 34982. Opdrachtgever Digivaardig & Digibewust (ECP-EPN.nl).

TNS-NIPO (2011) *Attitudes on Data Protection and Electronic Identity in the European Union*. Special Eurobarometer 359.

Tsai, J. Y. , S. Egelman, L. Cranor, A. Acquisti. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, 2010; 22 (2): 254 DOI: 10.1287/isre.1090.0260

U.S. Federal Trade Commission. *Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers*. Technical report, December 2010.

Verenigde Naties (1948) Universele Verklaring van de Rechten van de Mens, 1948. http://www.ohchr.org/en/udhr/pages/Language.aspx?LangID=dut (geraadpleegd 14 maart 2012).

Venkatesh, V., Morris, M., Davis, G., Davis, F. (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly,* (27)3, pp. 425-478.

Westin, A. (1967) *The right to privacy*, New York: Atheneum.

World Economic Forum (2010) *Personal data: the emergence of a new asset class*. Januari 2010.

Wikibon (2012) *Big Data market size and vendor revenues,* 7 Maart 2012, http://wikibon.org/wiki/v/Big_Data_Market_Size_and_Vendor_Revenues

Wright D. and De Hert P. (eds.)(2012) *Privacy Impact Assessment*. Springer, Dordrecht

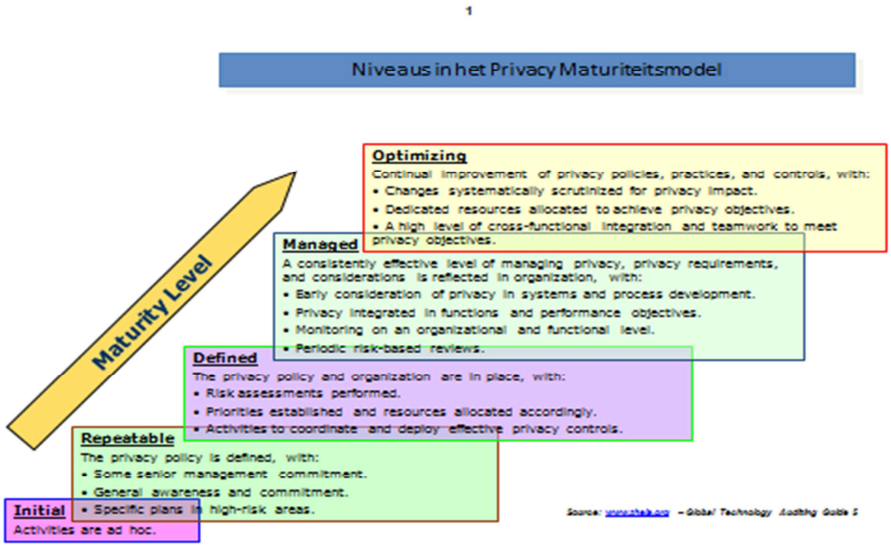
Appendix 1 Het Privacy Maturiteitsmodel

De geschetste indicatoren over de houding en perceptie tegenover invoering van PbD in de organisatie zeggen nog steeds weinig over *hoe* dit dan gebeurt. Een aanzet om dit systematisch in kaart te brengen vinden we in het *Privacy Maturity Model (PMM)*, ontwikkeld door de American Institute of Certified Public Accountants (AICPA) en de Canadian Institute of Chartered Accountants (CICA). AICPA heeft bijna 370.000 leden in 128 landen, en de CICA representeert 78.000 accountants uit Canada. Daarmee heeft het PMM een brede basis. Bij dit model moeten we ons er rekenschap van geven dat het belang van dit model voor organisaties er vooral in gelegen is dat het ze een systematische en gestructureerde methode biedt waarmee risico's rond het omgaan met persoonsgegevens in kaart worden gebracht en een organisatie op basis van de inschatting van de risico's en het gewenste niveau van beveiliging tegen deze risico's stappen kan zetten om de risico's te ondervangen.

Een maturiteitsmodel is een hulpmiddel waarmee bedrijven en organisaties hun voortgang ("volwassenheid") op een specifiek gebied kunnen toetsen aan veelal erkende standaarden (zie ook Borking 2009). Niet elke organisatie hoeft aan alle criteria in een maturiteitsmodel te voldoen; meestal wordt een afweging gemaakt tussen de (gepercipieerde) inschatting van de risico's en de kosten om een bepaald niveau te bereiken. De meeste gangbare maturiteitsmodellen zijn gebaseerd op het Capability Maturity Model. Dit model onderscheidt vijf niveaus van "volwassenheid" van softwareontwikkelingsprocessen. Het AICPA/CICA Privacy Maturity Model gebruikt ook deze vijf niveaus (zie Figuur 8):

1. *Ad-hoc*: er is geen sprake van een procesmatige aanpak van privacy maar slechts van een informele en inconsistente aanpak.
2. *Repeatable*: sommige processen zijn deels gedocumenteerd en herhaalbaar.
3. *Defined*: processen zijn volledig gedocumenteerd en geïmplementeerd.
4. *Managed*: het management heeft inzicht in en effectieve controle over processen.
5. *Optimizing*: de effectiviteit van processen wordt voortdurend verbeterd door regelmatige controles en organisatorische en technologische verbeteringen.

Figuur 8 De verschillende niveaus in het Privacy Maturity Model van AICPA en CICA (www.theia.org – Global technology Auditing Guide 5)



Los van de vraag of een bedrijf or organisatie op alle vlakken het hoogste niveau van maturiteit heeft bereikt, heeft het hanteren van een maturiteitsmodel ook waarde in het versterken en verbeteren van de organisatie en bedrijfsvoering op weg naar een hoger niveau van maturiteit (AICPA/CICA, 2011). Een dergelijk maturiteitsmodel kan naast het vaststellen van de huidige mate van privacybescherming binnen de organisatie ook gebruikt worden om vervolgstappen vast te stellen.

Het AICPA/CICA Privacy Maturiteitsmodel gaat uit van de zogenoemde *Generally Accepted Privacy Principles* (GAPP). De GAPP bestaat uit tien principes (zie Tabel 11).

Tabel 11: Generally Accepted Privacy Principles (GAPP)

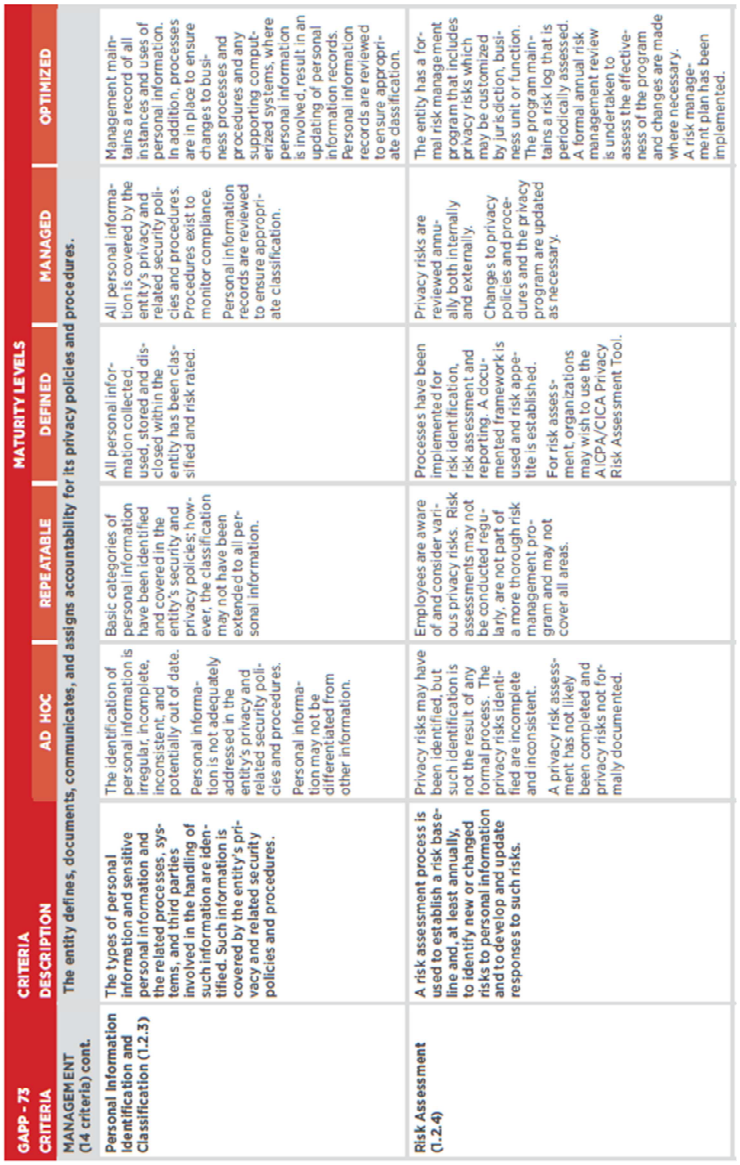
Principe	Omschrijving
Management	De organisatie definieert, documenteert, communiceert haar privacybeleid en procedures, en wijst verantwoordelijken aan.
Informeren	De organisatie informeert individuen over haar privacybeleid en procedures en geeft aan voor welke doeleinden persoonsgegevens worden verzameld, gebruikt, opgeslagen en gedeeld.
Keuze en toestemming	De organisatie beschrijft de keuzes die een individu heeft, en verkrijgt impliciet of expliciet toestemming van het individu voor het verzamelen, gebruiken en delen van persoonsgegevens.
Verzamelen	De organisatie verzameld enkel persoonsgegevens die nodig zijn voor de aangegeven doeleinden.
Gebruiken, bewaren en vernietigen	De organisatie gebruikt persoonsgegevens enkel voor de aangegeven doeleinden waarvoor toestemming is verkregen. De organisatie bewaart gegevens niet langer dan nodig voor

	de aangegeven doeleinden nodig is, of voor zover de wet dit eist, en vernietigt de informatie daarna.
Toegang	De organisatie geeft individuen toegang tot hun persoonsgegevens voor inzage en correctie.
Delen met derden	De organisatie deelt persoonsgegevens alleen met derden voor zover dit nodig is voor het bereiken van de aangegeven doeleinden, en met toestemming van het individu.
Veiligheid voor privacy	De organisatie beschermt persoonsgegevens tegen ongeautoriseerde toegang (zowel fysiek als digitaal).
Kwaliteit	De organisatie draagt zorg dat accurate, complete en relevante persoonsgegevens worden gebruikt voor de aangegeven doeleinden.
Monitoren en handhaven	De organisatie monitort de handhaving van haar privacybeleid en heeft procedures om privacy-gerelateerde klachten af te handelen.

Bron: GAPP genoemd in (AICPA/CICA, 2009)

Deze principes zijn gebaseerd op een studie naar verschillende nationale en internationale privacy wetten, richtlijnen en *best practices*. Bedrijven en organisaties die de GAPP omzetten in acties zijn daarmee dus ook goed op weg om te voldoen aan deze wetten en richtlijnen, zoals de richtlijn 95/46/EC van de Europese Unie, de set privacyrichtlijnen van de OECD en de Safe Harbour principes (AICPA, 2005). De tien privacybeginselen van de GAPP zijn uitgewerkt in 73 criteria. Voor ieder van de criteria is een uitwerking naar de verschillende niveaus van maturiteit gegeven. Een voorbeeld van de uitwerking van twee van deze criteria is weergegeven in Figuur 9.

Figuur 9 Voorbeeld van koppeling tussen GAPP-beginselen en de maturiteitsniveaus uit het AICPA/CICA Privacy Maturity Model



GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Personal Information Identification and Classification (1.2.3)	The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.	The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the entity's privacy and related security policies and procedures. Personal information may not be differentiated from other information.	Basic categories of personal information have been identified and covered in the entity's security and privacy policies; however, the classification may not have been extended to all personal information.	All personal information collected, used, stored and disclosed within the entity has been classified and risk rated.	All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance. Personal information records are reviewed to ensure appropriate classification.	Management maintains a record of all instances and uses of personal information. In addition, processes are in place to ensure changes to business processes and procedures and any supporting computerized systems, where personal information is involved, result in an updating of personal information records. Personal information records are reviewed to ensure appropriate classification.
Risk Assessment (1.2.4)	A risk assessment process is used to establish a risk baseline and, at least annually, to identify new or changed risks to personal information and to develop and update responses to such risks.	Privacy risks may have been identified, but such identification is not the result of any formal process. The privacy risks identified are incomplete and inconsistent. A privacy risk assessment has not likely been completed and privacy risks not formally documented.	Employees are aware of and consider various privacy risks. Risk assessments may not be conducted regularly, are not part of a more thorough risk management program and may not cover all areas.	Processes have been implemented for risk identification, risk assessment and reporting. A documented framework is used and risk appetite is established. For risk assessment, organizations may wish to use the AICPA/CICA Privacy Risk Assessment Tool.	Privacy risks are reviewed annually both internally and externally. Changes to privacy policies and procedures and the privacy program are updated as necessary.	The entity has a formal risk management program that includes privacy risks which may be customized by jurisdiction, business unit or function. The program maintains a risk log that is periodically assessed. A formal annual risk management review is undertaken to assess the effectiveness of the program and changes are made where necessary. A risk management plan has been implemented.

Het Privacy Maturiteitsmodel is ook voorzien van enkele korte begeleidende teksten die aangeven hoe het model gebruikt kan worden. Het AICPA/CICA positioneert het PMM dan ook niet als een theoretische beschouwing maar vooral als een praktisch hulpmiddel voor bedrijven en organisaties. De aanwijzingen hebben vooral betrekking op de procesaansturing en sporen met de privacybeginselen: het identificeren van een persoon uit het management die een project voor het toepassen van het PMM kan sponsoren, het samenstellen van een projectleiding met afdoende kennis van privacy en een afdoende mandaat, inventariseren of privacy-expertise van buiten nodig is en het vaststellen van een gewenst maturiteitsniveau voor de gehele organisatie (AICPA/CICA, 2011).

Appendix 2 Overzicht adoptiefactoren

Tabel 12 Overzicht kenmerken van innovatieprocessen, de bij deze kenmerken behorende constructen en de indicatoren per construct

Categorie	Construct	Indicator	Omschrijving
Innovatie-kenmerken	Performance expectancy	Relatief voordeel / Unique Selling Point	De mate waarin PbD een relatief (concurrentie) voordeel biedt en PbD wordt beschouwd als een Unique Selling Point
		Herkenbaarheid	De mate waarin PbD-maatregelen zichtbaar zijn voor consumenten en als zodanig herkend kunnen worden
		Toename verkoop	De mate waarin PbD-maatregelen leiden tot extra verkoop van producten van de organisatie bij consumenten
		Efficiëntie in dataverwerking	De mate waarin PbD-maatregelen efficiëntie van dataverwerking vergroten (of verkleinen)
		Effectiviteit / impact	De mate waarin PbD wordt beschouwd (gepercipieerd) als effectieve manier om (privacy)risico's voortkomend uit dataverwerking te verminderen
		Toename vertrouwen klanten	De mate waarin PbD-maatregelen leiden tot meer vertrouwen van klanten in de organisatie en haar diensten.
		Verantwoordelijkheid en aansprakelijkheid	De mate waarin PbD wordt beschouwd als een manier om de kans op aansprakelijkheidsprocedures te verkleinen
		Financiële impact	De kosten die gemoeid zijn met implementatie van PbD, betreft zowel de (eenmalige) investeringskosten als lange termijn onderhoudskosten
	Effort expectancy	Compabiliteit	De mate waarin implementatie PbD 'past' bij bestaande systemen, processen e.d.
		Complexiteit	De mate van complexiteit die de invoering van PbD-maatregelen voor de organisatie betekent
		Gepercipieerde uitvoerbaarheid	De mate waarin PbD makkelijk te gebruiken is (te implementeren is)

Organisatie-kenmerken	Faciliterende condities	Bewustzijn en perceptie privacyregulering	De mate waarin (het topmanagement) van de organisatie zich bewust is van PbD-maatregelen en mogelijkheden
		Risico van privacy-schendingen	De mate waarin (het topmanagement van de) organisatie mogelijke privacyschendingen (frequentie, kans, impact) als risico beschouwd
		Attitude topmanagement PbD (leiderschap)	De houding van het topmanagement in de organisatie ten opzichte van de verandering die de implementatie van PbD-maatregelen met zich meebrengt
		Omvang en structuur (organisatie, cultuur, innovativiteit)	Voor kleine organisaties kan het lastiger zijn om [ingewikkelde, kostbare] PbD-maatregelen te implementeren. Aan de andere kant kunnen kleine, innovatieve organisaties hier ook voorop lopen
		Data-intensiteit	De mate waarin (gevoelige) persoonsgegevens door de organisatie worden verwerkt
		Diversiteit van gebruikte IT-systemen	De mate waarin PbD-maatregelen in verschillende IT-systemen moeten worden geïntegreerd
	Sociale beïnvloeding	Banden met toezichthouders en adviesinstituten	De mate waarin organisaties banden hebben met toezichthouders draagt positief bij aan de adoptie van PbD-maatregelen
Externe omgeving	Faciliterende condities	Rol toezichthouders	De mate waarin organisaties banden hebben met toezichthouders draagt positief bij aan de adoptie van PbD-maatregelen
		Verkrijgbaarheid van PbD oplossingen	De mate waarin (technische?) PbD-oplossingen verkrijgbaar zijn/worden geleverd door softwareleverancier. Zijn er standaardpakketten beschikbaar?
		Wettelijk kader: externe druk door (strengere) wetgeving (druk om te voldoen aan wetgeving) en complexiteit	De mate waarin privacywetgeving druk legt op de organisatie om te voldoen aan de wetgeving (effectiviteit sancties, mate waarin wet wordt gehandhaafd door toezichthouders)
		Gebrek aan vraag van consumenten	De mate waarin consumenten vragen ('vereisen') dat organisatie PbD-maatregelen toepassen
	Sociale beïnvloeding	Concurrentie / samenwerking	De mate waarin directe concurrenten en partners van de organisatie PbD-maatregelen toepassen

Appendix 3 Dataverwerkend Nederland

Het speelveld van dataverwerkend Nederland bestaat uit een grote diversiteit aan bedrijven en organisaties, die acteren in verschillende sectoren en industrieën. In dit onderzoek wordt het speelveld omschreven vanuit een maatschappelijke indeling naar het gebruik van persoonsgegevens, aangevuld met een vraag- en aanbodindeling naar *Privacy by Design*. Als vertrekpunt om het speelveld van dataverwerkend Nederland in kaart te brengen, volgen we de indeling in maatschappelijke sectoren die het College bescherming persoonsgegevens (CBP) hanteert[26]: Bedrijfsleven, Overheid, Politie en Justitie, Werk en Sociale zekerheid en Zorg en Welzijn.

Het bedrijfsleven maakt in toenemende mate gebruik van persoonsgegevens voor gepersonaliseerde dienstverlening.. De mate waarin dit gebeurt hangt af van een aantal factoren. In een recente studie van London Economics is met een survey onder bedrijven het gebruik van persoonlijke data in kaart gebracht[27] [28]. Hieruit blijkt dat meer dan 80% van de bedrijven persoonlijke data gebruikt voor commerciële doeleinden zoals *direct marketing* activiteiten. Deze 'verhandelbare' data bestaat voornamelijk uit contactdetailinformatie.We kunnen ervan uitgaan dat dit soort data vooral wordt verzameld om te worden verhandeld aan derde partijen. Het LE-onderzoek veronderstelt dat een kwart van de bedrijven ook gedetailleerde persoonlijke data commercieel aanbiedt. Het grootste deel van de persoonlijke data bestaat uit gegevens over consumenten en consumentengedrag.

De grootte van de organisatie speelt, aldus het LE-onderzoek, een rol bij het verwerken van persoonlijke data. Kleinere bedrijven slaan zowel minder data als minder gedetailleerde data op, dan grotere bedrijven. Van de MKB bedrijven heeft iets minder dan 4% meer dan 10.000 persoonlijke data records in de database. Bij de grotere bedrijven heeft 29% dezelfde hoeveelheid opgeslagen. De omvang van een bedrijf heeft ook invloed op de risicoperceptie omtrent het gebruik van persoonlijke data, waarbij grotere bedrijven de privacyrisico's hoger inschatten dan kleine bedrijven. Dergelijke privacyrisico's vormen voor deze grote bedrijven tevens barrières om nieuwe business te starten.

Het gebruik van persoonlijke data wordt ook beïnvloed door de sector waarin een bedrijf zich bevindt. Een aantal sectoren is zeer data-intensief en zal meer (gedetailleerde) persoonlijke informatie verwerken. Voorbeelden van deze sectoren zijn: financiële dienstverlening, sociale dienstverlening, zorgdienstverlening, ICT-dienstverlening.

Om een beeld te schetsen van het speelveld van dataverwerkend Nederland kijken we naar de belangrijkste data-intensieve sectoren in het bedrijfsleven. De London Economics studie en de 'Bedrijfsleven' indeling volgens het CPB vormen de basis hiervoor.

---

[26] http://www.cbpweb.nl/Pages/ind_bedrijfsleven.aspx

[27] Study on the economic benefits of privacy□enhancing technologies (PETs), London Economics, 2010

[28] De studie is uitgevoerd in een Europese context, met participatie van 293 Nederlandse bedrijven verdeeld over verschillende sectoren.

Direct Marketing

Het gebruik van persoonlijke data voor commerciële doeleinden is sterk gerelateerd aan het domein van *Direct Marketing*. Op verschillende manieren worden gegevens verzameld van consumenten, welke worden opgeslagen in commerciële databases en worden gebruikt voor commerciële doeleinden. De *direct marketing* sector in Nederland laat zich kenmerken door opdrachtgevers en aanbieders van *Direct Marketing*.

Opdrachtgevers zijn partijen die baat hebben bij informatie over consumenten. De belangrijkste bedrijfstakken op het gebied van *Direct Marketing* zijn:

- Automotive
- Charitatieve instellingen
- Energieaanbieders
- FMCG / Retail: hieronder vallen de grote fabrikanten van FMCG (Procter & Gamble, Unilever, Coca Cola) , Retail (Albert Heijn, Schuitema), Telecom (KPN).
- Financiële dienstverleners (marketing / sales afdeling) waaronder banken en verzekeraars

De aanbieders vallen uiteen in mediabureaus, reclamebureaus en grafische en audiovisuele ontwerpbureaus. Communicatiebureaus verrichten diensten op het gebied van mediaplanning, communicatie en reclame. Mediabureaus adviseren adverteerders in hun mediamix en inkoop van advertentieruimte; ontwerp- en reclamebureaus creëren de campagnes. Er zijn bureaus die een breed scala aan diensten aanbieden. Er zijn ook gespecialiseerde bureaus die zich concentreren op een bepaald segment van de markt (bijvoorbeeld online marketing, cross media). In het segment mediabureaus is een twintigtal middelgrote en kleine bedrijven dat de markt in handen heeft. De vier grootste bureaus genereren ongeveer de helft van de omzet van de branche: Mindshare, Kobalt, MediaEdge, OMD. Enkele kengetallen:

- Totaal aantal bedrijven in marketing/communicatie branche: 21.225
- Aantal reclamebureau's: 16.340
- Aantal communicatiebureau's: 795
- MKB-aandeel: >99%

Financiële dienstverlening

In de financiële sector worden veel en vaak gevoelige persoonsgegevens verzameld en gebruikt. In de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen zijn duidelijke regels vastgelegd voor het verzamelen en gebruiken van persoonsgegevens binnen deze sector [29]. De Gedragscode is van toepassing op Financiële instellingen die (i) lid zijn van de NVB; (ii) aangesloten zijn bij Rabobank Nederland; of (iii) lid zijn van het Verbond. Banken en verzekeraars spelen in het maatschappelijk verkeer een belangrijke sleutelrol die in het teken staat van 'vertrouwen'. Het waarborgen van vertrouwen is niet alleen voor een individuele organisatie van belang maar voor de gehele sector financiële dienstverlening. Uit een eerder onderzoek komt naar voren dan 93% van de burgers het zeer belangrijk vind dat financiële instellingen zorgvuldig met persoonsgegevens omgaan[30].

[29] http://www.cbpweb.nl/downloads_gedragscodes/gedr_financiele_instellingen.pdf
[30] Burgers en Privacy, TNS NIPO, 2005

Telecom en Internet
De beschikbare informatie in telecommunicatiesystemen wordt steeds meer gebruikt voor het leveren van allerlei diensten, als gevolg van toenemende samenwerkingen tussen verschillende partijen in de waardeketen. Daarnaast leidt het openbare en grensoverschrijdende karakter van het medium internet ertoe dat online persoonsgegevens toegankelijk zijn voor iedereen en overal ter wereld. Dit confronteert gebruikers met vragen over hun privacy, de veiligheid van hun persoonsgegevens en het mogelijke misbruik daarvan.

Aandachtsgebieden voor telecombedrijven zijn:
- E-commerce (Redcoon, Coolblue, Wehkamp)
- Online marketing: Online behavioural marketing en zoekmachines (Marketing/communicatie bureaus's gespecialiseerd in online (zoek) marketing.
- Online sociale netwerken en virtuele communities (Relatieplanet, Playstation Network, Hyves, Facebook)
- Internetbedrijven (Google)

Zorgdienstverlening
Het zorgstelsel wordt in hoog tempo veranderd. De informatisering gaat gestaag door en vraagt aandacht voor de bescherming van het medisch beroepsgeheim. De belangrijkste ontwikkeling is de introductie van de nieuwe Zorgverzekeringswet op 1 januari 2006. Door de nieuwe taken krijgen de verzekeraars – veelal onderdeel van grote financiële concerns – veel (medische) persoonsgegevens. De ziektekostenverzekeraars zullen in hun organisatie en systemen zogenaamde "Chinese muren" moeten bouwen. Zo kan voorkomen worden dat persoonsgegevens, afkomstig van hulpverleners, en andere medische gegevens kunnen worden uitgewisseld tussen de basisverzekering, aanvullende verzekeringen en eventueel nog andere producten of diensten binnen of buiten een concern.

Een belangrijke en recente ontwikkelingen in de zorg is de invoering van het gebruik van het Burgerservicenummer. Zorginstellingen en zorgverzekeraars zullen verplicht zijn met dit persoonsnummer te werken. Het gebruik van een uniek identificerend persoonsnummer in de zorg brengt risico's met zich mee. In Nederland is discussie gaande over de beste manier om de informatie-architectuur in te richten zodat medische gegevens toegankelijk zijn maar ook een adequaat niveau van bescherming en beveiliging van medische gegevens geboden kan worden.

Particuliere recherche
De particuliere recherche is een sterk groeiende sector waarin vergaande methoden van particulier onderzoek worden toegepast. Particuliere onderzoeksbureaus verrichten vanuit een eigen commercieel belang recherchewerkzaamheden voor verschillende soorten opdrachtgevers. Daarbij valt te denken aan verzekeraars, privaatrechtelijke en publiekrechtelijke rechtspersonen (al dan niet in de hoedanigheid van werkgever) en aan particulieren. Deze sector omvat circa 1665 bedrijven.[31]

[31] http://www.cbs.nl/nl-NL/menu/themas/veiligheid-recht/cijfers/default.htm

Het CBP heeft de Privacygedragscode[32] voor de particuliere onderzoeksbureaus op 21 oktober 2009 goedgekeurd. De gedragscode is opgesteld door de Vereniging van Particuliere Beveiligingsbureaus (VPB). De gedragscode is algemeen verbindend verklaard voor alle particuliere onderzoeksbureaus die een vergunning behoeven. De gedragscode geeft daarbij normen voor deze praktijk van onder andere heimelijke observatie, verborgen camera's, het afluisteren van telefoongesprekken en het onderscheppen van e-mail. Bedrijven – de grote opdrachtgevers voor de particuliere recherche – en ook particulieren kunnen zich nu beter informeren over de mogelijkheden die zij hebben voor de bestrijding van onregelmatigheden.

Incasso en Handelsinformatie

Incassobedrijven werken nauw samen met (handels)informatiebureaus. Deze partijen zijn gespecialiseerd in het achterhalen van (voornamelijk) financiële gegevens over debiteuren. De meest voorkomende opdrachten zijn het achterhalen van de inkomenspositie van de debiteur en het achterhalen van het bank- of girorekeningnummer van de betrokkene en diens werkgever of uitkeringsinstelling. Gerechtsdeurwaarders zijn vaak ook incassobureau. Voor de bescherming van persoonsgegevens is het belangrijk dat deze twee rollen goed gescheiden worden. De Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBvG) heeft daarom een gedragscode opgesteld. In totaal zijn er 660 deurwaarders- en incassobedrijven, waarvan circa 40% deurwaarderskantoren.

[32] http://www.cbpweb.nl/downloads_gedragscodes/gedr_vpb.pdf

Appendix 4 Voorstel voor Europese verordening voor dataprotectie

In het voorstel voor een nieuwe Europese verordening voor ‘de bescherming van natuurlijke personen in verband met de verwerking en het vrije verkeer van persoonsgegevens’ is nadrukkelijk gekozen voor het perspectief van gegevensbescherming. In eerdere documenten ter voorbereiding van de verordening was nog sprake van *Privacy by Design* en *Privacy Impact Assessments*. In het voorstel dat januari 2012 publiek is gemaakt, is dit systematisch gewijzigd in *Data Protection by Design* en *Data Protection Impact Assessment*. Dat is een consequente doorvoering van de insteek van de verordening die handelt over *data protection* en niet over privacy. Privacy komt op verschillende plaatsen in de verordening terug, bijvoorbeeld bij de behandeling van datalekken (artikel 32, lid 1). Dan wordt het begrip gebruikt in de betekenis van de Europese verdragen waarin privacy expliciet wordt benoemd, zoals in de Handvest van de Grondrechten van de Europese Unie (artikel 7) (EG 2000). In deze Charter verwijst privacy naar het recht op en het respecteren van privé- en gezinsleven, huis en communicatie-uitingen.

Hoewel het voorstel nog niet de kracht van een wet heeft, werpt het wel zijn schaduw vooruit in de vereisten die in de toekomst mogelijk gesteld gaan worden aan de bescherming van persoonsgegevens. We geven daarom een aantal in het oog liggende verschilpunten van dit ingediende voorstel met zijn voorganger, de richtlijn (95/46/EU):

- Ten eerste betreft het een verordening, en geen richtlijn. Een verordening is bindend waar een richtlijn een minimale basis geeft die door afzonderlijke lidstaten in nationale wetgeving aangescherpt kan worden. Dat wil zeggen dat de verordening, mocht deze overgenomen worden door het Europese parlement en de Raad van Europa, letterlijk wordt neergelegd in nationale wetgeving. Dit beoogt de harmonisering van de wetgeving tussen de 27 lidstaten.
- Ten tweede wordt *data protection by design* expliciet genoemd in de verordening. In artikel 23 wordt aangegeven dat de verantwoordelijke voor de gegevensbewerking vooraf en tijdens de verwerking de geëigende technische en organisatorische maatregelen treft. Ook wordt het begrip *data protection by default* ingevoerd waarmee wordt aangegeven dat de te treffen maatregelen bij het eerste ontwerp van een nieuw systeem als *default* moeten worden meegenomen.
- Ten derde voegt de verordening nieuwe elementen toe aan de rechten van het individu, zoals het recht om vergeten te worden (artikel 17), het recht om persoonsgegevens van de ene provider naar de andere mee te nemen (dataportabiliteit, artikel 19), en het recht op verzet tegen beslissingen die tot stand komen door automatische verwerking van gegevens (profilering; artikel 20).
- Ten vierde voegt de verordening nieuwe plichten toe aan de plichten van de verantwoordelijke en de bewerker, zoals de plicht om een *data protection impact assessment* uit te voeren in bepaalde gevallen (zoals wanneer sprake is van een systematische en uitvoerige verwerking van persoonsgegevens, van verwerking van gevoelige gegevens en van verwerking van gegevens afkomstig

van monitoring van openbare plaatsen; artikel 33), de plicht om een datalek binnen 24 uur na constatering van het lek te melden aan de toezichthouder en aan de individuen die getroffen worden waarbij ook aangegeven wordt wat individuen kunnen doen om hun risico's te beperken (artikel 32) en het aanstellen van een *Privacy Officer* indien het bedrijf op reguliere en systematische wijze persoonsgegevens verzameld en bewerkt dan wel persoonsgegevens bewerkt en meer dan 250 werknemers in dienst heeft. Bij overheidsorganisaties dient altijd een *privacy officer* aangesteld te zijn.

Het niet nakomen van alle verplichtingen kan de verantwoordelijke op een boete komen te staan die, afhankelijk van de nalatigheid, op kan lopen tot 1 miljoen Euro dan wel tot 2% van de totale jaarlijkse omzet indien het een bedrijf betreft. De verordening bevat uitzonderingsbepalingen die kleine ondernemingen (minder dan 250 werknemers) op belangrijke punten vrijwaren van de genoemde verplichtingen en die overheidsorganisaties de mogelijkheid bieden in het belang van de staatsveiligheid en de maatschappelijke orde uitzonderingen te creëren.

Appendix 5 Overzicht geïnterviewde organisaties

Nationaal

	Organisatie	Sector	Type
1	Nederlandse Spoorwegen	Transport	Verantwoordelijke
2	GGZ Meerkanten	Zorg	Verantwoordelijke
3	Genkey	Technologie	Aanbod
4	Lilly	Farmacie	Verantwoordelijke
5	KLM	Transport	Verantwoordelijke
6	Logica	ICT dienstverlening	Aanbod
7	Carinova	Zorg	Verantwoordelijke
8	DUO	Onderwijs	Verantwoordelijke
9	Acxiom	Marketing	Verantwoordelijke
10	Cap Gemini	ICT dienstverlening	Aanbod
11	T-Systems	Telecom en ICT	Aanbod
12	HP	ICT dienstverlening	Aanbod
13	Sensor Universe	Technologie	Aanbod
14	Qiy	Privacy & Identity	Aanbod
15	Ois	Informatiebeveiliging	Aanbod
16	ING	Financiële dienstverlening	Verantwoordelijke
17	PWC advisory	Zakelijke dienstverlening	Aanbod
18	Stichting Surf	Onderwijs	Aanbod
19	Sogeti	ICT dienstverlening	Aanbod

Internationaal

	Naam	Organisatie	Land
1	Ira Rubenstein	Research Fellow, Adjunct Professor of Law, New York University School of Law	VS
2	Marilyn Prosch	Associate Professor, Arizona State University	VS
3	Colin O'Malley	Chief Strategy Officer, Evidon	VS
4	Michelle Chibba	Director of Policy, Office of the Information and Privacy Commissioner of Ontario	Canada
5	Fred Carter	Senior Policy and Technology Advisor, Office of the Information and Privacy Commissioner of Ontario	Canada
6	Marit Hansen	Vice President of the Independent Centre for Privacy Protection Schleswig-Holstein (en verantwoordelijk voor European Privacy Seal)	Duitsland
7	Mathias Reinis	Concept Factory	Duitsland
8	Sarah Spiekermann	Institute for Management Information Systems, Vienna University of Economics and Business (WU Vienna)	Oostenrijk
9	Mikko Niva	Global Privacy Counsel, Nokia	Finland
10	Riikka Turunen	Head of Consumer Privacy, Nokia	Finland

Appendix 6 Interviewprotocol

Protocol voor verantwoordelijke

1 – Context

1. Kunt u vertellen wat de kernactiviteit is van uw organisatie en in welke branche of sector uw organisatie actief is?

2. Hoeveel werknemers heeft uw organisaties ongeveer?

3. Wat is uw functie binnen de organisatie?

4. Wat voor type persoonsgegevens verwerkt uw organisatie?

2 – Privacy by Design

5. Bent u bekend met de term Privacy by Design? Wat verstaat u er onder?

Toelichting Privacy by Design.
Er bestaan verschillende definities en invullingen van Privacy by Design. Privacy by Design heeft als doel privacyschendingen zoveel mogelijk te vermijden door privacybescherming vooraf en tijdens de gehele levenscyclus van een informatiesysteem systematisch 'in te bakken' in het informatiesysteem en de organisatie. Het gaat bij Privacy by Design niet alleen om technische maatregelen maar ook om organisatorische maatregelen en de rol van eindgebruikers (consumenten).

Organisaties kunnen op verschillende manieren PbD toepassen. Voorbeelden zijn: het standaard uitvoeren van een Privacy Impact Assessment bij het ontwerp van een nieuw product of dienst, het aanstellen van een Privacy Officer, het regelmatig trainen van personeel over de omgang met persoonsgegevens, gebruik maken van access management en access control (niet elke werknemer mag bij alle databestanden), het anonimiseren van persoonlijke gegevens, of afnemers van diensten informeren over het gebruik van persoonsgegevens, het jaarlijks monitoren van het privacybeleid van de organisatie, etc.

6. Wat verwacht u van Privacy by Design als het gaat om het voorkomen of verkleinen van de kans op privacyschendingen? M.a.w. in hoeverre acht u Privacy by Design 'in staat' om de kans op privacyschendingen te verkleinen?

7. Wat zou de toepassing van Privacy by Design voor uw organisatie betekenen? In termen van impact op:
   a. informatietechnologie
   b. bedrijfsprocessen
   c. bedrijfsstrategie
   d. afname van uw producten/diensten
   e. Business model en/of mogelijk concurrentievoordeel

8. Wat verwacht u van de financiële impact van de toepassing van (onderdelen van) PbD voor uw organisatie?

9. Wat is voor uw organisatie het belangrijkste voordeel en het belangrijkste nadeel van het toepassen van Privacy by Design?

10. Wat zijn voor uw organisatie de belangrijkste redenen om wel/niet in Privacy by Design te investeren?

3. Kernmerken van de organisatie

11. In hoeverre is uw organisatie in staat om zelf instrumenten te ontwikkelen voor PbD en in hoeverre zou uw organisatie hiervoor externe expertise inhuren (en waarvoor)? (technologie, procesverbeteringen, ...)

12. Hoe beoordeelt u de beschikbaarheid en het aanbod van toepassingen, diensten en consultancy op het gebied van Privacy by design? Is dit voldoende voor handen? Vindt u het aanbod transparant? Vindt u de kwaliteit van het aanbod voldoende?

13. Zijn er bepaalde eigenschappen van uw organisatie die het moeilijker of juist makkelijker maken om PbD toe passen in uw organisatie? Bijvoorbeeld ...
    a. de complexiteit van de ICT;
    b. het doel van de organisatie;
    c. de cultuur binnen de organisatie;
    d. de manier waarop binnen de organisatie gewerkt wordt;
    e. de omvang van de organisatie.

4. Externe omgeving

14. Welke factoren uit de externe omgeving beïnvloeden de toepassing van PbD binnen uw organisatie en waarom?
    a. Wetgeving
    b. Technologische ontwikkeling
    c. Houding/visie concurrenten
    d. Houding consumenten
    e. Rol toezichthouder
    f. Overig

Slotvraag

15. Hoe ziet u de toekomstige relatie tussen innovatie in het bedrijfsleven en de roep om meer privacybescherming in het algemeen en voor uw organisatie?

16. Tips richting bedrijven die niet voorlopen op het gebied van PbD

Protocol voor aanbieder

1 – Context

1. Kunt u vertellen wat de kernactiviteit is van uw organisatie en in welke branche of sector uw organisatie actief is?

2. Hoeveel werknemers heeft uw organisaties ongeveer?

3. Wat is uw functie binnen de organisatie?

2 – Privacy by Design

4. Bent u bekend met de term Privacy by Design? Wat verstaat u er onder?

Toelichting Privacy by Design.
Er bestaan verschillende definities en invullingen van Privacy by Design. Privacy by Design heeft als doel privacyschendingen zoveel mogelijk te vermijden door privacybescherming vooraf en tijdens de gehele levenscyclus van een informatiesysteem systematisch 'in te bakken' in het informatiesysteem en de organisatie. Het gaat bij Privacy by Design (PbD) niet alleen om technische maatregelen maar ook om organisatorische maatregelen en de rol van eindgebruikers (consumenten).

Organisaties kunnen op verschillende manieren PbD toepassen. Voorbeelden zijn: het standaard uitvoeren van een Privacy Impact Assessment bij het ontwerp van een nieuw product of dienst, het aanstellen van een Privacy Officer, het regelmatig trainen van personeel over de omgang met persoonsgegevens, gebruik maken van access management en access control (niet elke werknemer mag bij alle databestanden), het anonimiseren van persoonlijke gegevens, of afnemers van diensten informeren over het gebruik van persoonsgegevens, het jaarlijks monitoren van het privacybeleid van de organisatie, etc.

3 – Privacy by Design bij uw afnemers

5. Hoe verwacht u dat de toepassing van PbD bij uw afnemers zich zal ontwikkelen in de komende jaren?

6. Welke factoren uit de externe omgeving beïnvloeden de toepassing van PbD bij uw afnemers en waarom?
   g. Wetgeving
   h. Technologische ontwikkeling
   i. Houding/visie concurrenten
   j. Houding afnemers/klanten
   k. Rol toezichthouder
   l. Overig

7. Wat zijn de belangrijkste drivers en barriers voor uw afnemers (denk bijvoorbeeld aan complexiteit van systemen, omvang van de organisatie, organisatiecultuur,e.d.) om PbD toe te passen?

8. In hoeverre verwacht u dat het budget voor privacybeschermende maatregelen bij uw afnemers in de komende jaren zal toe- of afnemen?

4 – Privacy by Design binnen uw organisatie

9. Wat zou de toepassing van Privacy by Design door uw afnemers voor uw organisatie betekenen? In termen van impact op:
   a. informatietechnologie (kennis en ontwikkeling van Privacy Enhancing Technologies)
   b. bedrijfsprocessen
   c. bedrijfsstrategie
   d. afname producten/diensten (in hoeverre is er aandacht van afnemers voor PbD?)

e. business model en/of mogelijk concurrentievoordeel (waardecreatie door privacybeschermende technologie?)

10. Zal uw organisatie, en zo ja op welke wijze, een business model rondom Privacy by Design ontwikkelen? Hoe zou uw propositie er uit zien? Wat is er voor nodig om de propositie te ontwikkelen? Wat zijn de belangrijkste drivers en barriers om die waardepropositie te ontwikkelen?

Slotvraag

11. Hoe ziet u de toekomstige relatie tussen innovatie in het bedrijfsleven en de roep om meer privacybescherming in het algemeen en voor uw organisatie?

12. Extra vraag: welke tips heeft u voor organisaties die PbD willen toepassen / implementeren?

Appendix 7 Leden klankbordgroep

	Naam	Organisatie
1	Richard Blad	Ministerie van Economische Zaken, Landbouw en Innovatie
2	John Borking	Extern adviseur Privacy-by-Design bij CMS Derks Star Busmann, advocaten, notarissen en belastingadviseurs
3	Manon Langius	Ministerie van Veiligheid en Justitie
4	David de Nood	VNO-NCW/MKB Nederland
5	Bart Pegge	ICT Office
6	Jan de Zeeuw	Nederlands Genootschap van Functionarissen voor de Gegevensbescherming