Samenvatting

> The White Rabbit put on his spectacles. `Where shall I begin, please your Majesty?' he asked. 'Begin at the beginning,' the King said gravely, `and go on till you come to the end: then stop.'
> Lewis Carroll, Alice in Wonderland, Chapter XII Alice Evidence, London, 1995, p.182.

Privacyrecht is code
Over het gebruik van Privacy Enhancing Technologies

Dit boek verkent twee zaken. Aan de ene kant onderzoekt het of privacybeschermende informatiesystemen preventief kunnen worden ingezet om onze persoonsgegevens en onze persoonlijke ruimte effectief te kunnen beschermen. Aan de andere kant onderzoekt het of 'privacy enhancing technologies' (PET) kunnen worden toegepast in informatiesystemen om onze privacy adequaat te beschermen. In acht hoofdstukken heb ik geprobeerd de volgende probleemstelling te beantwoorden:

Hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker, beide in de zin van de Europese Richtlijn 95/46/EG.

In de context van de probleemstelling worden in dit boek zes onderzoeksvragen behandeld, die in hoofdstuk 1 zijn opgesomd. De resultaten hiervan leiden tot het antwoord op de probleemdefinitie.

De onderzoeksvragen zijn:

OV 1: Welke juridische specificaties kunnen voor informatiesystemen uit de algemene beginselen betreffende persoonlijke informatie en de privacy wet- en regelgeving worden afgeleid?

OV 2: *Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger preventief in de gaten houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding?*

OV 3: Met welke privacybedreigingen en -risico's moeten de burger en de ontwerper van systemen rekening houden?

OV 4: Wat houdt het concept Privacy Enhancing Technologies (PET) in?

OV 5: Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen?

OV 6: Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?

Hoofdstuk 1

De omgevingsanalyse in hoofdstuk 1 vormt de aanleiding voor OV 1. Daaruit blijkt dat in postindustriële landen, zoals de Verenigde Staten, Canada, Australië, Japan en de landen van de Europese Unie, informatie- en communicatiesystemen worden gebruikt, die op een steeds verfijndere manier gegevens over personen verzamelen, opslaan, uitwisselen, (her)gebruiken, identificeren, analyseren en monitoren. Uit de omgevingsanalyse blijkt ook dat burgers (als inwoners, patiënten, hotelgasten, passagiers, studenten, kopers op internet, etc.) bang zijn dat de overheid, het bedrijfsleven en andere organisaties hun persoonlijke informatie misbruiken. Deze bezorgdheid wordt gevoed doordat er steeds meer informatiesystemen zijn, die via internet of andere netwerken verbonden kunnen worden met databanken en automatisch en onbelemmerd (persoons)gegevens kunnen uitwisselen. Hoe meer persoonlijke informatie beschikbaar is, des te groter wordt het risico van identiteitsdiefstal door kwaadwillige personen die persoonsgegevens van burgers zonder hun toestemming zich toe-eigenen en misbruiken. Burgers en consumenten zijn niet in staat na te gaan wat er met hun persoonsgegevens gebeurt en aan wie die worden verstrekt. Het ligt voor de hand dat zij controle willen hebben en houden over het gebruik van hun persoonsgegevens. In de praktijk blijkt het echter voor burgers en consumenten zeer moeilijk hun rechten op het gebied van de bescherming van persoonsgegevens te handhaven. Indringende technologieën zetten de persoonlijke ruimte (een onzichtbaar veld dat ieder mens omringt en voelbaar wordt als andere mensen te dichtbij komen) en de informationele privacy steeds meer onder druk. Zonder technische hulpmiddelen zal deze situatie in de toekomstige 'ambient intelligence omgeving' (AMI) sterk verergeren. AMI's zijn elektronische omgevingen die gevoelig en ontvankelijk zijn voor de aanwezigheid van mensen.

Hoofdstuk 2

Onze persoonlijke levenssfeer en onze persoonlijke informatie worden wettelijk beschermd. De begrippen 'privacy', 'persoonlijke ruimte' 'identiteit' en 'persoonsgegevens' zijn in dit hoofdstuk verkend. Vervolgens worden de algemene grondslagen over persoonlijke informatie die ten grondslag liggen aan de privacybescherming in kaart gebracht. Deze algemene grondslagen zijn uitgewerkt in de privacy realisatiebeginselen, die in de Convention 108 van de Raad van Europa, de OECD-richtlijnen en in de EU-Richtlijnen 95/46/EG en 2002/58/EG zijn vastgelegd en worden hier toegelicht. Hierbij komen ook de opvattingen van de Article 29 Working Party en een aantal relevante uitspraken van het Europese Hof voor de Rechten van de Mens en het Europese hof van Justitie aan

de orde. De privacy realisatiebeginselen (dat zijn de uitgangspunten om privacybescherming te effectueren) hebben directe gevolgen voor de ontwikkeling en de technische specificaties van informatiesystemen. Het gaat hierbij bijvoorbeeld om de beginselen van gegevensminimalisering, doelbinding en transparantie, (informatieverschaffing en toegangrechten) en informatiebeveiliging. Het antwoord op de eerste onderzoeksvraag leidt tot de opsomming van zeven noodzakelijke juridische specificaties voor het ontwerpen van privacyveilige informatiesystemen. In hoofdstuk 2 is aangegeven dat de data retentie Richtlijn 2006/24/EG gevolgen heeft voor de privacy bescherming. Er zijn een aantal kritische kanttekeningen bij de EU-privacyrichtlijnen geplaatst.

Hoofdstuk 3
Alvorens in te gaan op de privacybedreigingen vanuit de omgeving van het informatiesysteem komt de risicotoezichtsamenleving aan de orde die ertoe leidt dat privacyinbreuken toenemen. In dit hoofdstuk zijn enkele maatschappelijke ontwikkelingen toegelicht, die de erosie van privacy lijken te bevorderen. Met name is ingegaan op een aantal surveillance (recherche) technologieën, zoals data warehousing, data mining, videocamera's, biometrie en localisering (bijvoorbeeld via mobiele telefoons). De overheid en het bedrijfsleven zetten deze technologieën in om diensten aan te bieden, maar evenzeer om terrorisme, misdaad en fraude te bestrijden. Zijn '9/11' en de Richtlijn 2006/24/EG of de daarvan afgeleide wetgeving verantwoordelijk voor de afbrokkeling van onze privacy? Het antwoord op die 'schuldvraag' is ontkennend. In dit hoofdstuk wordt gesteld dat de diepere oorzaak voor de antiterrorismewetgeving niet direct ligt in de aanslagen die wereldwijd de afgelopen zes jaar hebben plaatsgevonden, maar in de geleidelijke ontwikkeling van onze netwerksamenleving. In die samenleving is de nadruk steeds meer op risicoanalyse komen te liggen. Om de collectieve veiligheid in de samenleving zo goed mogelijk te garanderen is een vorm van surveillance opgekomen die door de ict wordt ondersteund. Panoptische technologie zal steeds vaker worden ingezet om mensen heimelijk in de gaten te houden. Omdat de sensoren (RFIDs) die ons omringen steeds kleiner worden, zal surveillance door overheid en bedrijfsleven voor het individu steeds onzichtbaarder (vooral in een AMI-omgeving) worden. Het is de vraag in hoeverre individuen en groepen in zo'n surveillancemaatschappij zelf nog kunnen bepalen hoeveel ze blootgesteld willen worden aan toezicht en hoezeer zij de persoonlijke informatie kunnen beperken die over hen verzameld en gebruikt wordt. Toezichtsystemen zijn voor een leek vaak te technisch om te begrijpen. Zij zijn steeds meer onzichtbaar en gaan daardoor ongemerkt op in de alledaagse structuren en systemen van de maatschappij: op het werk, thuis, op school, op reis en bij het gebruik van telecommunicatie. De risicotoezichtmaatschappij zorgt voor sociale uitsluiting en informatieapartheid. Aanbiedingen met kortingen worden bijvoorbeeld niet aangeboden aan mensen uit achterstandswijken omdat daar geen koopkracht is of dubieuze debiteuren wonen. Het antwoord op de tweede onderzoeksvraag bevestigt dat onze privacy op het spel staat wanneer er geen privacyveilige informatiesystemen voor de surveillance worden ingezet.

Hoofdstuk 4
In dit hoofdstuk wordt betoogd dat, om persoonsgegevens te mogen verwerken en privacybescherming in informatiesystemen te kunnen inbouwen het noodzakelijk is vooraf een privacyrisico- en bedreigingsanalyse uit te voeren. Daarbij moet niet alleen een beveiligingstechnische maar ook een juridische afweging worden gemaakt. Uit artikel 17 van Richtlijn 95/46/EG kan niet anders worden geconcludeerd dan dat een privacyrisico of bedreigingsanalyse *ex ante* een *sine qua non* is. Organisaties negeren echter deze wettelijke eis massaal alsof deze verplichting niet zou bestaan. Uit een onderzoek van KPMG uit 2004 blijkt dat 95 procent van alle Nederlandse organisaties bij de verwerking van persoonsgegevens in strijd met de Wet bescherming persoonsgegevens handelt en dat privacyinbreuken op grote schaal plaatsvinden.

De privacyrisico- en bedreigingsanalyses brengen de gevaren bij de verzameling, verwerking, uitwisseling, en verspreiding van persoonsgegevens voor het individu en de gegevensverwerkende organisaties aan het licht. De Europese privacyrichtlijnen en de daarop geënte nationale wetgevingen van de EU-lidstaten schrijven voor dat de beveiliging van persoonsgegevens zodanig moet zijn dat die risico's worden afgedekt.

Er zijn zeven risicoanalyse- en risicomanagementmethoden behandeld, zoals onder meer de methode van de Registratiekamer (nu CBP) om de risicoklasse voor een specifieke verwerking van persoonsgegevens te bepalen. Daarnaast zijn aan bod gekomen de privacy impactanalyse (PIAs), die door de Treasury Board van de Canadese overheid is ontwikkeld, de privacy bedreigingsanalyse met de pentagonale aanpak die in het Europese PISA-project is ontwikkeld en de privacybedreigingsontologie, die voor het eerst in 2007 in het Noorse PETWEB-project is toegepast. Het is belangrijk om een privacyrisico- of bedreigingsanalyse uit te voeren die met zo veel mogelijk omstandigheden rekening houdt. Vaak geven beveiligingsdeskundigen vanuit de praktijk een opsomming van potentiële privacyinbreuken en daarmee verbonden bedreigingen en risico's. Dit verdient niet de voorkeur. Een ontologische beschrijving van bedreigingen is geschikter.

Uit de onderzochte privacyrisico- en bedreigingsanalyses is duidelijk geworden dat persoonsgegevens het best beschermd kunnen worden als ze geanonimiseerd of gescheiden worden van andere gegevens. Dat laatste betekent dat de persoonsgegevens wel worden verwerkt, maar dat de identificerende persoonsgegevens direct worden losgekoppeld van de overige persoonsgegevens. De derde onderzoeksvraag levert een lijst van privacybedreigingen op.

Hoofdstuk 5
Dit hoofdstuk behandelt de vierde onderzoeksvraag door de inhoud en reikwijdte van het concept 'privacy enhancing technologies' (PET) te verkennen en gaat na hoe PET kunnen bijdragen aan de bescherming van persoonsgegevens in informatiesystemen. Daarnaast wordt onderzocht welke rol is weggelegd voor de 'Identity Protector' (IDP) en hoe de privacy realisatiebeginselen in programmacode kunnen worden omgezet. In dit hoofdstuk is een aantal belangrijke ontwerpelementen in

samenhang met PET besproken, die kunnen worden ingezet bij de het ontwerp en de bouw van privacyveilige systemen. Het concept PET kan theoretisch gezien worden als een belangrijke aanvulling op het bestaande juridische kader en de technologische uitwerking daarvan. PET kunnen ervoor zorgen dat organisaties persoonsgegevens niet of aanmerkelijk minder gebruiken of volgens de wettelijke voorwaarden verwerken. De privacybescherming door de verantwoordelijken wordt hierdoor in de praktijk geen lege huls. Bovendien stellen PET de burger en consument in staat de verwerking van hun persoonsgegevens te controleren zodat hun vertrouwen in de rechtmatige verwerking ervan toeneemt. De in dit hoofdstuk besproken research toont aan dat de privacy van burgers en consumenten steeds effectiever kan worden beschermd. De noodzaak om adequate technologische middelen te ontwikkelen om de persoonlijke levenssfeer te beschermen wordt steeds groter. Steeds meer transacties zullen in de nabije toekomst niet alleen meer direct tussen mensen plaatsvinden, maar in toenemende mate rechtstreeks tussen informatiesystemen, software agents, intelligente sensoren en robots. In dit hoofdstuk zijn tevens de gereedschappen om persoonsgegevens te beschermen behandeld, zoals encryptie, 'rule-based' privacy managementsystemen en privacy ontologieën.

Hoofdstuk 6

Dit hoofdstuk behandelt de vijfde onderzoeksvraag aan de hand van vier privacyveilige informatiesystemen die met succes gerealiseerd zijn in verschillende sectoren van de samenleving. In de vier voorbeelden zijn de ontwerpbeginselen en technieken uit hoofdstuk 5 toegepast. Deze vier voorbeelden tonen aan dat persoonsgegevens van individuen technisch goed zijn te beschermen zonder dat de functionaliteit van informatiesystemen in gevaar komt. Het concept PET speelt als onderdeel van de informatiearchitectuur een belangrijke rol bij de bescherming van persoonsgegevens. Om persoonsgegevens van het individu adequaat te beschermen, moeten PET een onderdeel van de informatiearchitectuur zijn. Dit betekent doorgaans dat de architectuur fundamenteel moet worden herzien, vooral met betrekking tot de onderlinge relaties van de onderdelen en de relaties met de omgeving van het systeem. Integratie van PET in nieuw te ontwikkelen systemen is een reële optie. PET zijn het meest effectief in het proces van het verzamelen van persoonsgegevens, omdat de privacy dan bij de bron wordt beschermd. De besproken metazoekmachine Ixquick in dit hoofdstuk geeft daar blijk van. Zoals uit het voorbeeld van het ziekenhuis Veldwijk-Meerkanten blijkt, kunnen met PET de persoonsgegevens tijdens verwerking en opslag uitstekend beschermd worden. Complexere systemen als NTIS en ViTTS zouden zonder PET niet kunnen bestaan. Ook zijn PET goed inzetbaar bij de verspreiding van gegevens, omdat PETs voorkomen dat gegevens ongeoorloofd aan elkaar gekoppeld worden. Het PISA-project toont aan, dat PETs persoonsgegevens afdoende binnen netwerkomgevingen kunnen beschermen ondanks de complexiteit om privacyrecht in systemen in te bouwen en te handhaven. Organisaties maken nog weinig gebruik van privacymanagementsystemen die verwerking conform de privacyregels afdwingen. Het PISA-project is een

geavanceerde toepassing daarvan en levert kennis op die gebruikt kan worden in een 'ambient intelligence'-omgeving.

Hoofdstuk 7
Hier is de zesde onderzoeksvraag beantwoord, waarom privacyveilige architecturen nauwelijks worden geïmplementeerd en PET nauwelijks worden toegepast. De organisatorische en economische belemmeringen bij de adoptie van PET worden geanalyseerd, onder meer aan de hand van casestudies. Het blijkt dat organisaties door een groot aantal factoren beïnvloed worden bij hun beslissing om wel of niet PET toe te passen. Wanneer de positieve adoptiefactoren worden benut, zouden organisaties PET sneller op grote schaal in hun informatiesystemen kunnen toepassen. Het gaat hierbij vooral om organisaties die een grote informatie-intensiteit kennen, vanuit hun organisatiestrategie een grote behoefte hebben persoonsgegevens te beschermen en financieel en operationeel daartoe in staat zijn. Om PET toe te passen moet de organisatie een bepaalde maturiteit hebben. Het hoofdstuk gaat hierop in. Of PET binnen een organisatie kunnen worden toegepast hangt af van de maturiteit die de organisatie heeft op het gebied van Identity & Access Management (IAM) en privacybescherming. Het verloop van deze processen en het beslissingsmoment om PET toe te passen wordt in drie gerelateerde S-curven uitgedrukt. Beproefde businessmodellen om in PET te investeren bestaan niet. Om te investeren in PET, is een positieve businesscase vereist die de financiële haalbaarheid van de PET investering aantoont. Daarom wordt in dit hoofdstuk een aantal methoden besproken om de rentabiliteit van investeringen te berekenen waaronder de 'Return On Investment'-methode met een specifieke investeringsformule voor PET (ROI-PI) en de 'Net Present Value'-formule. Empirische gegevens over privacyincidenten zijn in de Europese Unie niet beschikbaar, waardoor de consequenties van dergelijke incidenten niet accuraat kunnen worden ingeschat en de rendementsberekeningen onnauwkeurig zijn. Een verplichte bekendmaking en registratie van verlies of diefstal van persoonlijke informatie, zoals voorzien in het wijzigingsvoorstel van de Richtlijn 2002/58/EG, zullen ervoor zorgen dat dergelijke gegevens op termijn wel beschikbaar komen.

Hoofdstuk 8
Dit hoofdstuk heeft de onderzoeksvragen uit hoofdstuk 1 weer opgepakt, de probleemstelling beantwoord en komt met tien aanbevelingen die zijn gebaseerd op de positieve adoptiefactoren voor PET uit hoofdstuk 7. Naast voorlichting is de rol van de privacytoezichthouder (Data Protection Authorities (DPAs)) van cruciaal belang voor de implementatie van PET in informatiesystemen. De DPAs, zoals het CBP in Nederland, zouden zich niet ex post (klachtenbehandeling en controles achteraf), maar vooral ex ante (preventief adviserend) moeten opstellen. Zij zouden hun technologische experts als PET consulenten moeten inzetten. Die kunnen aan de hand van de privacyrisico-, privacybedreigings- of privacyimpactanalyses (PIAs) vaststellen of de in te voeren informatiesystemen voldoen aan de privacywetgeving en kunnen zo nodig adviseren PET toe te

passen. De expertise over PET-toepassingen is echter schaars. Het zou daarom wenselijk zijn een PET Expertisecentrum in het leven te roepen. Om PET succesvol in nieuwe informatiesystemen te implementeren beveel ik een specifiek PET-stappenplan aan. Het hoofdstuk sluit af met voorstellen voor een aantal aanpassingen van de Richtlijn 95/46/EG die noodzakelijk zijn om persoonsgegevens beter te beschermen. Privacyveilige systemen zorgen voor het noodzakelijke vertrouwen van de burger en consument dat hun persoonsgegevens worden verwerkt overeenkomstig hun privacyvoorkeuren en de wet- en regelgeving. Met ingebouwde PET-maatregelen in informatiesystemen zullen zij zichzelf ook in de komende AMI-wereld effectiever tegen privacyinbreuken kunnen beschermen.

Uit de de research is op te maken dat wij privacyveilige systemen kunnen bouwen (het *hoe* in de probleemstelling), maar dat deze ook voorzien dienen te zijn van een certificaat met de verklaring, dat het systeem privacyveilige verwerking van persoonsgegevens waarborgt. Voor algemeen maatschappelijk *vertrouwen* is het nodig dat privacyveilige systemen grootschalig worden ingezet. Nochtans als er geen politieke wil is om de privacy adequaat te beschermen en men gaat onverkort door met het gebruik van privacy onveilige informatiesystemen in onze risicotoezichtsamenleving dan dreigt er ernstig gevaar voor onze privacy.