

# Privacyrechtelijke aspecten van RFID

# Privacyrechtelijke aspecten van RFID

Een productie van:



In samenwerking met:



In opdracht van:



Ministerie van Economische Zaken

# Colofon

Dit is een uitgave van ECP.NL, Platform voor eNederland in opdracht van het Ministerie van Economische Zaken en in samenwerking met RFID Platform Nederland en GSI Nederland.

## **Teksten**

mr. Bart W. Schermer

mr. Marjolijn Durinck

## **Ontwerp omslag en binnenwerk:**

ECP.NL / Efficiënta Offsetdrukkerij BV

## **Druk**

Efficiënta Offsetdrukkerij BV

## **ISBN**

90-76957-14-2

© ECP.NL, mei 2005

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorgaande schriftelijke toestemming van de maker.

Alhoewel de auteurs en uitgever uiterste zorgvuldigheid betracht hebben bij het samenstellen van deze uitgave aanvaarden zij geen aansprakelijkheid voor schade van welke aard ook, die het directe of indirecte gevolg is van handelingen en/of beslissingen die (mede) gebaseerd zijn op de in deze uitgave vervatte informatie.

De wet- en regelgeving is een dynamisch terrein zodat de regels en richtlijnen die in deze uitgave worden genoemd inmiddels kunnen zijn veranderd.

## Voorwoord

De ontwikkeling van Radio Frequency Identification technologie (RFID) bevindt zich momenteel in een stroomversnelling. De verwachting is dat RFID binnen enkele jaren grootschalig zal worden toegepast in sectoren als de detailhandel, logistiek, transport, openbaar vervoer, onderwijs en gezondheidszorg. Als zodanig gaat RFID in de komende jaren een substantiële bijdrage leveren aan de Nederlandse economie, de kwaliteit van leven binnen onze samenleving en de veiligheid van de maatschappij. Maar wanneer deze veelbelovende technologie op een onverantwoorde of oneigenlijke manier wordt ingezet, kunnen mogelijk risico's ontstaan voor de privacy van de burger.

ECP.NL, platform voor eNederland, is van mening dat het van groot belang is dat de brede introductie van RFID in Nederland op een gecoördineerde en maatschappelijk verantwoorde manier plaatsvindt. Alleen op deze manier kan Nederland maximaal profiteren van de voordelen van RFID, zonder dat dit ten koste gaat van de privacy en individuele vrijheid van de burger.

Een eerste stap op weg naar een goede introductie van RFID is het in kaart brengen van de privacy-rechtelijke aspecten van RFID. ECP.NL heeft daarom onderzoek gedaan naar de mogelijke risico's die RFID kan hebben voor de privacy. Hierbij is ook gekeken in hoeverre ons huidig wet- en regelgevend kader voor de bescherming van de privacy op deze nieuwe technologie berekend is. De resultaten van dit onderzoek vindt u in dit rapport. Op basis van het onderzoek en de daaraan verbonden conclusies worden aanbevelingen gedaan richting overheid en bedrijfsleven.

Bij het onderzoek is ECP.NL ondersteund door een omvangrijke werkgroep samengesteld uit marktpartijen (aanbieders, gebruikers, consumenten), beleidsmakers, wetenschappers en belangenbehartigers.

Dit rapport is gericht aan beleidsmakers vanuit de overheid en beslissers binnen het bedrijfsleven die betrokken zijn bij de introductie van RFID in Nederland. Daarnaast is het rapport interessant voor een ieder die geïnteresseerd is in de introductie van RFID in Nederland.

ECP.NL blijft zich in de komende jaren inspannen voor een gecoördineerde en maatschappelijk verantwoorde invoering van RFID in Nederland.



Dhr. mr. A.J.M. van Bellen  
Directeur ECP.NL, platform voor eNederland

# Inhoudsopgave

<b>1</b>	<b>INLEIDING</b>	<b>7</b>
1.1	ACHTERGROND	7
1.2	PROBLEEMSTELLING	7
1.3	VRAAGSTELLING	7
1.4	DOELSTELLING EN AANPAK	7
1.5	SCOPE	8
1.6	DE WERKGROEP PRIVACY & RFID	8
<b>2</b>	<b>WAT IS RFID?</b>	<b>9</b>
2.1	TECHNOLOGIE	9
2.1.1	<i>Radiogolven</i>	9
2.1.2	<i>Tags</i>	9
2.1.3	<i>Readers</i>	10
2.1.4	<i>RFID middleware-oplossingen</i>	11
2.2	RFID-SYSTEMEN EN TOEPASSINGEN	11
2.2.1	<i>Smart labels</i>	11
2.2.2	<i>Tokens &amp; smart cards</i>	11
2.2.3	<i>Implantaten</i>	12
2.2.4	<i>Overige systemen</i>	12
2.3	HET EPCGLOBAL NETWORK	12
2.3.1	<i>Electronic Product Code (EPC)</i>	12
2.3.2	<i>Middleware</i>	13
2.3.3	<i>Physical Markup Language (PML)</i>	13
2.3.4	<i>Object Name Service (ONS)</i>	13
2.3.5	<i>EPC-Information Service (EPC-IS)</i>	13
2.3.6	<i>EPC Discovery Services (EPC-DS)</i>	14
2.4	TIJDSPAD RFID	14
2.5	TOEKOMSTVISIE RFID	14
<b>3</b>	<b>PRIVACY</b>	<b>16</b>
3.1	WAT IS PRIVACY?	16
3.2	HET RECHT OP PRIVACY	16
3.3	PERSOONSgegevens EN INFORMATIONELE PRIVACY	17
3.4	BEGINSELEN VAN BEHOORLIJK GEGEVENSBEHEER	17
3.5	ONDERSCHIED TUSSEN PUBLIEKE EN PRIVATE ORGANISATIES	18
<b>4</b>	<b>MOGELIJKE RISICO'S</b>	<b>19</b>
4.1	HET OP AFSTAND HEIMELIJK UITLEZEN VAN TAGS DOOR READERS	19
4.2	TRACEABILITY DOOR UNIEKE IDENTIFICATIE	19
4.3	DATA AGGREGATIE EN PROFILING	20
4.4	TAGGEN VAN MENSEN	20
4.5	ILLEGAAL GEBRUIK	20
4.6	SYSTEEMINTEGRATIE	21
<b>5</b>	<b>HUIDIG JURIDISCH KADER</b>	<b>22</b>
5.1	WET BESCHERMING PERSOONSgegevens	22
5.1.1	<i>Achtergrond</i>	22
5.1.2	<i>Wat is een persoonsgegeven?</i>	22
5.1.3	<i>Wanneer is er bij RFID sprake van een persoonsgegeven?</i>	24
5.1.4	<i>Inhoud Wet bescherming persoonsgegevens</i>	26
5.2	RICHTLIJN 2002/58/EG	28

<b>6</b>	<b>ANALYSE RISICO'S RFID</b>	30
6.1	SCENARIO'S	30
6.1.1	<i>RFID smart labels</i>	30
6.1.2	<i>RFID Tokens &amp; smart cards</i>	32
6.1.3	<i>RFID-implantaten</i>	33
6.1.4	<i>Overige Systemen</i>	34
6.2	VERONDERSTELDE RISICO'S GEANALYSEERD	34
6.2.1	<i>Het op afstand heimelijk uitlezen van tags door readers</i>	34
6.2.2	<i>Traceability door unieke identificatie</i>	35
6.2.3	<i>Data aggregatie en profiling</i>	36
6.2.4	<i>Taggen van mensen</i>	36
6.2.5	<i>Illegaal gebruik</i>	37
6.2.6	<i>Systeemintegratie</i>	37
6.3	TOEREIKENDHEID BESTAANDE WET- EN REGELGEVING	38
<b>7</b>	<b>TECHNISCHE VOORZIENINGEN</b>	39
7.1.1	<i>RFID-detectie</i>	39
7.1.2	<i>Kooi van Faraday</i>	39
7.1.3	<i>Verwijderen antenne</i>	39
7.1.4	<i>Encryptie</i>	39
7.1.5	<i>KILL Commando</i>	39
7.1.6	<i>RFID Deep Sleep mode</i>	40
7.1.7	<i>RFID Blocker tags</i>	40
7.1.8	<i>Informatiefiltering</i>	40
<b>8</b>	<b>CONCLUSIES</b>	41
<b>9</b>	<b>AANBEVELINGEN</b>	44
<b>10</b>	<b>LITERATUURLIJST</b>	46
<b>11</b>	<b>BIJLAGEN</b>	49
11.1	BIJLAGE I: INTERNATIONALE WETGEVING (ALGEMEEN)	49
11.1.1	<i>Universele Verklaring van de Rechten van de Mens</i>	49
11.1.2	<i>Het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR)</i>	49
11.1.3	<i>EVRM</i>	50
11.2	BIJLAGE II: REGELGEVING INFORMATIONELE PRIVACY	50
11.2.1	<i>Fair Information Practice Principles</i>	50
11.2.2	<i>OECD Privacy Guidelines</i>	50
11.3	BIJLAGE III: RFID SPECIFIEKE (ZELF)REGULERING	51
11.3.1	<i>EPC guidelines</i>	51
11.3.2	<i>RFID Bill of Rights</i>	52
11.3.3	<i>ICDPPC Resolution on Radio-Frequency Identification</i>	52
11.3.4	<i>ICC Principles on EPC deployment and operation</i>	52
11.4	BIJLAGE IV: VOORGESTELDE RFID SPECIFIEKE WETGEVING	53
11.4.1	<i>CASPIAN RFID Right to Know Act</i>	53
11.4.2	<i>RFID Right to Know Act 2004 (California)</i>	53
11.4.3	<i>RFID Right to Know Act 2004 (Utah)</i>	54
11.4.4	<i>RFID Right to Know Act 2004 (Missouri)</i>	54
11.5	BIJLAGE V: WERKGROEP PRIVACY & RFID ECP.NL	55



# 1 Inleiding

## 1.1 Achtergrond

RFID (Radio Frequency Identification) is een technologie die door middel van radiosignalen de unieke identificatie van producten, dieren en personen op afstand mogelijk maakt. Hoewel de technologie reeds in de jaren dertig van de vorige eeuw is ontwikkeld en in de Tweede Wereldoorlog is toegepast om vliegtuigen te identificeren, hebben technische en economische barrières tot op heden een brede maatschappelijke uitrol in de weg gestaan. Door de voortschrijdende stand van de technologie (lagere kosten, miniaturisatie) worden deze barrières echter in rap tempo geslecht en staan we aan de vooravond van de doorbraak van RFID in onze maatschappij.

Door de eenvoudige en unieke identificatie van producten, dieren en mensen kunnen tal van processen efficiënter en intelligenter worden gemaakt. De verwachting is dan ook dat RFID in de komende jaren in tal van sectoren zoals logistiek, transport, retail, zorg, defensie en onderwijs toegepast gaat worden en daarmee van grote waarde wordt voor economie en maatschappij. RFID zal in de toekomst een van de sleuteltechnologieën vormen voor het 'internet of things', een nieuw ICT-paradigma waarbij de focus zal verschuiven van de personal computer naar allerlei 'slimme' objecten (ambient intelligence) die met elkaar kunnen communiceren (Meloan 2003).

Zowel economisch als maatschappelijk biedt RFID dus vele mogelijkheden. Wanneer in de toekomst grootschalige toepassing op productniveau plaatsvindt kunnen echter ook onder bepaalde omstandigheden persoonsgegevens van de burger/consument verkregen worden. Hoewel dit op zichzelf niet noodzakelijkerwijs een probleem is, kan bij onverantwoord gebruik of misbruik van RFID-toepassingen de privacy van de burger in het geding komen. Inmiddels is er wereldwijd aandacht voor de privacyrechtelijke aspecten van RFID en wordt door marktpartijen en overheden gekeken naar mogelijke oplossingen.

## 1.2 Probleemstelling

RFID is een belangrijke ontwikkeling voor de Nederlandse maatschappij en economie. Er

bestaat echter ook onzekerheid over de invloed die RFID kan hebben op de privacy. Met name in de Verenigde Staten maken burgerrechtenorganisaties en belangengroeperingen voor consumenten zich zorgen over het gebruik van RFID. Dit protest spitst zich voornamelijk toe op het gebruik van RFID op consumentenproducten. Een belangrijke reden voor het felle protest in de Verenigde Staten is het ontbreken van degelijke wetgeving die ook van toepassing kan worden verklaard op RFID.

Om tot een maatschappelijk verantwoorde implementatie van RFID in Nederland te komen, is het van groot belang de burger de grootst mogelijke zekerheid te bieden met betrekking tot de bescherming van diens persoonlijke levenssfeer en individuele vrijheden. De vraag is of en hoe dit mogelijk is binnen het huidige juridische kader voor de bescherming van de persoonlijke levenssfeer, meer specifiek de bescherming van persoonsgegevens. Met andere woorden:

*Biedt de huidige Nederlandse wet- en regelgeving op het gebied van privacy afdoende waarborgen voor de bescherming van de persoonlijke levenssfeer en individuele vrijheid van de burger in het kader van de toepassing van RFID-systemen?*

## 1.3 Vraagstelling

Op basis van de in de probleemstelling geschetste problematiek kunnen wij voor dit rapport de volgende onderzoeksvragen stellen:

- (1) In hoeverre is de huidige wet- en regelgeving op het gebied van de bescherming van de privacy van toepassing op RFID-systemen?
- (2) Is de huidige wet- en regelgeving toereikend voor de bescherming van privacy en vrijheid van de burger in het kader van RFID?

## 1.4 Doelstelling en aanpak

Doelstelling van dit rapport is het analyseren van de privacyrisico's die RFID met zich mee zou kunnen brengen, het inventariseren in hoeverre het huidige wet- en regelgevend kader voor de bescherming van de privacy deze risico's kan uitsluiten of beperken, en het doen van aanbevelingen waarmee moge-

lijke dreigingen het best ondervangen kunnen worden.

Om deze doelstelling te bereiken wordt de volgende aanpak gevolgd:

Allereerst wordt in hoofdstuk 2 een overzicht gegeven van de technologie achter RFID. Dit technologisch overzicht is noodzakelijk omdat slechts met een goed begrip van de achterliggende technologieën een inventarisatie kan worden gemaakt van de privacy-rechtelijke aspecten van RFID.

In hoofdstuk 3 wordt getracht meer inzicht te verschaffen in het ambigue begrip privacy. Door een toelichting te geven op de ontwikkeling en interpretatie van het begrip privacy, kan de relatie tussen het recht op privacy en de mogelijke risico's beter in perspectief worden geplaatst.

In hoofdstuk 4 passeren de mogelijke risico's van RFID met betrekking tot privacy de revue.

In hoofdstuk 5 wordt het huidige juridische kader voor de verwerking van persoonsgegevens besproken.

In hoofdstuk 6 richten we ons op het beantwoorden van de onderzoeksvragen. Aan de hand van een aantal scenario's wordt in hoofdstuk 6 gekeken in hoeverre het huidige wet- en regelgevend kader van *toepassing* is op RFID en in hoeverre het *toereikend* is.

In hoofdstuk 7 komen technische voorzieningen aan de orde die bij kunnen dragen aan het verminderen van de privacyrisico's bij het gebruik van RFID.

Tot slot worden in hoofdstuk 8 een aantal conclusies getrokken en in hoofdstuk 9 een aantal aanbevelingen worden gedaan.

## **1.5 Scope**

In dit rapport wordt de nadruk gelegd op de toepassing van RFID in de private sector, met andere woorden: de toepassing van RFID door bedrijven en de mogelijke privacyrisico's die dit gebruik met zich mee kan brengen. Voorts wordt gekeken naar de toepassing van RFID in sectoren welke deels een publiek karakter hebben zoals de zorg, het openbaar vervoer, onderwijs, en de bibliotheekwereld. Privacy en individuele vrijheid

kunnen ook door handelingen van de overheid in het kader van de uitoefening van een publieke taak (opsporing van strafbare feiten, handhaving van wetgeving, nationale veiligheid) in het gedrang komen, maar het gaat de scope van dit rapport te buiten daar al te diep op in te gaan.

## **1.6 De Werkgroep Privacy & RFID**

Dit rapport is tot stand gekomen met de hulp en expertise van vele marktpartijen (aanbieders, gebruikers en consumenten), overheidspartijen en wetenschappers die samenkomen in de werkgroep Privacy & RFID van ECP.NL. ECP.NL dankt deze partijen voor hun ondersteuning, expertise en constructieve bijdragen. Een volledige lijst van leden van de werkgroep kunt u vinden in de bijlage bij dit rapport.

## 2 Wat is RFID?

Algemeen gesteld is Radio Frequency Identification (RFID) een methode om met behulp van radiosignalen objecten te identificeren. Op objecten bevestigde passieve of semi-passieve radio-etiketten (tags of transponders genaamd) identificeren zichzelf door het afgeven van een radiosignaal wanneer zij een signaal opvangen van een lezer (reader of interrogator genaamd) (IBM 2003, p. 7).

RFID is een overkoepelende term voor allerlei typen radio-identificatie welke voor verschillende doeleinden aangewend kunnen worden. Het is van belang een goed onderscheid te maken tussen verschillende toepassingen van RFID-technologie wanneer we kijken naar de privacyrechtelijke aspecten van RFID.

### 2.1 Technologie

Een RFID-systeem werkt met behulp van radiogolven en bestaat verder in het algemeen uit drie onderdelen:

- de RFID-tag;
- de RFID-reader; en
- een middleware oplossing (een systeem om RFID-data te verwerken).

#### 2.1.1 Radiogolven

Tags communiceren met readers door middel van radiogolven. Deze radiogolven (energie in de vorm van elektromagnetische trillingen) hebben een bepaalde frequentie. Het elektromagnetisch spectrum kent verschillende frequenties van laag tot extreem hoog. Omdat grote delen van dit spectrum al worden gebruikt voor andere toepassingen zoals bijvoorbeeld AM/FM radio, is niet elke frequentie vrij beschikbaar voor RFID. De voor RFID gangbare frequenties zijn 125KHz, 13.56MHz, 860 tot 950 MHz, en 2.45GHz<sup>1</sup>. Het gebruik van deze frequenties is echter deels nog niet wereldwijd geharmoniseerd. Het standaardisatiewerk inzake RFID richt zich er onder meer op om tot wereldwijde overeenstemming inzake frequenties te komen. Dit is met name van belang voor het gebruik van RFID op objecten die wereldwijd gedistribueerd worden, zoals consumentenartikelen.

Omdat radiogolven over het algemeen moeite hebben om door metalen objecten of vloeistoffen heen te dringen, zijn metalen objec-

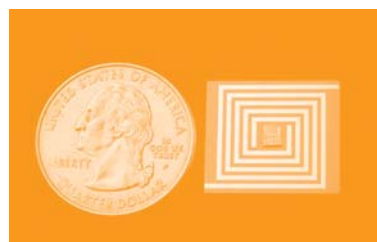
ten en objecten met een hoog vloeistofgehalte (bijvoorbeeld fruit en dranken) moeilijker te identificeren met behulp van RFID. Lage frequenties zijn het beste geschikt om door vloeistof en metaal heen te dringen. Hier staat tegenover dat de maximale leesafstand niet erg groot is en de snelheid waarmee data overgedragen kan worden laag is. Ultra High Frequency (UHF) heeft een grotere maximale leesafstand en hogere datatransmissie snelheid, maar is duurder, consumeert meer stroom en heeft meer moeite om door vloeistoffen en metalen te dringen. De keuze voor de technische inrichting van een RFID-systeem is dus in belangrijke mate afhankelijk van de gekozen toepassing en de bijbehorende kosten.

#### 2.1.2 Tags

Een RFID-radio-etiket (tag of transponder) is het onderdeel van een RFID-systeem dat wordt bevestigd op een object. Een tag bestaat uit een aantal onderdelen te weten: een chip, een antenne en een omhulsel.



Figuur 1. Een RFID-tag. De stip linksboven is de chip, de koperen banen vormen de antenne.



Figuur 2. De grootte van een RFID-tag. Op deze afbeelding is de grootte van de RFID-tag te zien tegenover een quarter dollar. Bron: Auburn University's website, Auburn University, AL 36849



Figuur 3. Een RFID-implantaat. De RFID-tag en antenne welke met glas zijn omhuld kunnen ingebracht worden in het menselijk lichaam. Bron: Verichip/AP

<sup>1</sup> Bron: Philips

- *Chip*

De chip is een halfgeleider die informatie over, of een verwijzing naar, het object waar het aan gehecht is in zich draagt. De hoeveelheid en het type informatie dat vastgelegd kan worden in de chip is afhankelijk van het gekozen dataformaat en de beschikbare geheugencapaciteit. De chip kan read only zijn, wat betekent dat data op de chip enkel is uit te lezen en niet is aan te passen, write once waarbij de chip maar één keer beschreven kan worden of read-write, wat betekent dat de chip uitgelezen kan worden maar dat ook informatie toegevoegd of verwijderd kan worden.

- *Antenne*

De antenne die aan de chip vastzit zendt, afhankelijk van het type tag, zelf radiogolven uit of gebruikt de energie van de ontvangen radiogolven om een signaal terug te zenden.

- *Omhulsel*

Om de chip en de antenne te beschermen en bevestiging op en in objecten mogelijk te maken, worden tag en antenne door een omhulsel omgeven.

10 Chip, antenne en omhulsel vormen samen de RFID-tag. Er zijn verschillende typen tags:

- *Actieve tag*

Een actieve tag bevat naast een chip en antenne ook een eigen krachtbron in de vorm van een batterij. Door de eigen krachtbron is de tag in staat om een zwakker radiosignaal te ontvangen en het antwoord uit te zenden over een grotere afstand. Hier staat tegenover dat de levensduur door de batterij beperkt is en de tag over het algemeen groter en tevens duurder is.

- *Passieve tag*

Een passieve tag heeft geen eigen batterij hetgeen betekent dat de tag energie moet ontvangen van het radiosignaal van de reader. De tag verkeert dus in een 'slaaptoestand' totdat deze een radiosignaal van een reader opvangt. Voordeel van passieve tags is dat ze relatief goedkoop zijn en door het ontbreken van een eigen batterij klein gehouden kunnen worden. Passieve tags zijn daarom bij uitstek geschikt om individuele producten van RFID te voorzien (item level tagging). Doordat de tag geen eigen krachtbron heeft is de maximale leesafstand van de tag beperkt tot ongeveer vijf meter.

- *Semi-passieve tag*

Een semi-passieve tag heeft een eigen batterij welke niet wordt gebruikt om de leesafstand te vergroten, maar om de intelligentie en de geheugenopslagcapaciteit van de chip te verbeteren.

### 2.1.3 Readers

Een reader (lezer of interrogator) is het apparaat dat tags kan uitlezen. Een reader bestaat uit een antenne en een controle eenheid. De controle eenheid codeert, decodeert, controleert en bewaart RFID-data en zorgt voor de communicatie met de tags en eventueel een achterliggend databasesysteem (IBM 2003, p. 11). De readers kunnen zowel vast (bijvoorbeeld boven een deur of in een schap) als mobiel zijn (handhelds, PDA's et cetera).

Zoals reeds eerder vermeld, wordt de maximale leesafstand van een reader en de bijbehorende tags bepaald door de gebruikte frequentie van het radiosignaal. Zo kan een UHF-reader de bijbehorende UHF-tags van grotere afstand lezen dan een laagbandige reader dat kan bij RFID-tags die gebruik maken van lage frequenties. Een andere factor die de leesafstand beïnvloedt is het vermogen van de reader. Een hoger vermogen betekent een grotere leesafstand.

Het is mogelijk dat een overlappend radiosignaal van verschillende readers onderlinge storing veroorzaakt (reader collision). Dit kan voorkomen worden door een systeem te ontwerpen waarbinnen de readers op verschillende intervals lezen (time division multiple access, or TDMA). Omdat het dan mogelijk is dat één tag twee of meer keer wordt gescand, moet aan dit systeem een functionaliteit worden toegevoegd die dubbel gescande codes wist.

Ook tegelijkertijd gescande tags kunnen voor problemen zorgen. Wanneer meerdere tags tegelijkertijd een signaal terugsturen naar de reader, dan kan deze verward raken (tag collision). De reader ondervangt dit door naar unieke nummers te vragen. Een reader vraagt bijvoorbeeld eerst alle tags te reageren wiens nummer met 0 begint. Reageert één tag, dan wordt deze gescand, reageren meerdere tags dan breidt de reader de vraag uit en met de vraag wiens nummer met 00 begint. De reader blijft dit doen totdat slechts één tag reageert.

#### 2.1.4 RFID middleware-oplossingen

Middleware-oplossingen zorgen voor de koppeling van RFID-data met de achterliggende ICT-infrastructuur van de gebruiker. RFID-readers die tags lezen genereren al snel een enorme hoeveelheid data en hoewel de eerste filtering en verwerking reeds in de reader plaatsvindt, is een verdere bewerkingslag vaak noodzakelijk. De data uit de reader wordt daartoe door een middleware-oplossing verwerkt en doorgestuurd om vervolgens gebruikt te kunnen worden in andere ICT-infrastructuren van de organisatie zoals bijvoorbeeld ERP- of CRM-systemen.

## 2.2 RFID-systemen en toepassingen

Omdat RFID een verzamelnaam is voor allerlei toepassingen van radio-identificatietechnologie worden verschillende soorten RFID-systemen veelal op één hoop gegooid. Met het oog op het bespreken van de privacy-rechtelijke aspecten van RFID is het echter van belang onderscheid te maken tussen verschillende toepassingen, omdat de concrete toepassing (en de daarbij behorende technische inrichting) bepaalt welke gevolgen voor de privacy er al dan niet zijn.

Gezien het feit dat het nagenoeg onmogelijk is om alle verschillende toepassingen van RFID-technologie die momenteel worden gebruikt, of in de nabije toekomst zullen worden gebruikt, afzonderlijk te bespreken is gekozen voor een andere aanpak: het beoordelen van de privacyrechtelijke aspecten van RFID op basis van de toegepaste RFID-technologie, aan de hand van een aantal toepassingsscenario's (zie hoofdstuk 6).

De systemen die worden gebruikt voor radio-identificatie kunnen grofweg worden verdeeld in vier categorieën: *smart labels*, *tokens & smart cards*, *implantaten* en *overige systemen*. Al naar gelang de concrete toepassing zal een van deze vier systemen worden gebruikt.

#### 2.2.1 Smart labels

Smart labels zijn passieve tags die door hun geringe prijs en afmeting op allerlei producten kunnen worden bevestigd. Omdat smart labels zo goedkoop mogelijk gehouden moeten worden om het rendabel te houden producten van RFID te voorzien, zal de op een smart label vastgelegde informatie nagenoeg altijd beperkt zijn tot een uniek nummer. Dit

nummer kan aan een achterliggende database met additionele informatie over het product worden gekoppeld. In feite is de veelgebruikte term smart label dus enigszins misleidend, omdat de smart label op zichzelf niet bijzonder intelligent is of veel data kan bevatten. In feite is een smart label een 'object tag', een RFID-tag die bedoeld is voor het registreren van objectgegevens en niet voor toepassingen op persoonsniveau.

Het gebruik van smart labels wordt voornamelijk binnen de logistiek en detailhandel (op de zogenaamde *fast moving consumer goods*) overwogen. Grote partijen als Wal\*Mart en Tesco stimuleren actief het gebruik van RFID smart labels in de detailhandel.

#### 2.2.2 Tokens & smart cards

RFID kan ook gebruikt worden om bestaande identificatie-, authenticatie- en autorisatiemethoden te vergemakkelijken en beter te beveiligen. Er is een aantal methoden op basis waarvan de identiteit van een persoon kan worden vastgesteld (identificatie), kan worden bekeken in hoeverre deze persoon ook is wie hij zegt dat hij is (authenticatie), en kan worden bepaald wat deze persoon mag doen binnen een bepaalde context (autorisatie). Deze methoden maken veelal gebruik van de gerelateerde concepten *wie je bent*, *wat je weet* en *wat je hebt*. Met behulp van biometrische kenmerken (wie je bent) kan je bijvoorbeeld redelijk onomstotelijk worden geïdentificeerd. Maar identificatie en authenticatie kan ook tot stand komen doordat jij als enige iets weet (bijvoorbeeld een wachtwoord). Tot slot kan het zijn door iets dat je hebt, zoals bijvoorbeeld een bepaalde cryptografische sleutel of een token.

Het gebruik van tokens die helpen bij de identificatie, authenticatie en autorisatie van personen is wijdverbreid in onze maatschappij, denk bijvoorbeeld maar aan het gebruik van bankpassen en toegangskaarten. De gebruikte tokens worden steeds geavanceerder en intelligenter. De opkomst van zogenaamde 'smart cards' is hier het beste voorbeeld van. Smart cards zijn pasjes die een chip bevatten waarop (persoons)gegevens kunnen worden opgeslagen.

Vooralsnog dient in de meeste gevallen de smart card uitgelezen te worden met behulp van een smart card reader. Er bestaan echter ook contactloze smart cards die van een

afstand uitgelezen kunnen worden. Het gaat hierbij niet om afstanden van meters, maar eerder van centimeters. Deze smart cards maken gebruik van RFID-technologie.

Naast contactloze smart cards bestaan er ook andere draagbare RFID-tokens, een voorbeeld hiervan is de RFID-armband die in Legoland wordt gebruikt om zoekgeraakte kinderen te localiseren.<sup>2</sup>

### 2.2.3 Implantaten

Het is ook mogelijk om RFID-tags in het menselijk lichaam te plaatsen. In de meeste gevallen zullen deze subdermale implantaten dezelfde functie vervullen als de hierboven genoemde tokens: zij vereenvoudigen het proces van identificatie, authenticatie en autorisatie. Uiteraard is een bijkomend voordeel dat de token niet verloren of gestolen kan worden, waardoor er een hoger beveiligingsniveau gerealiseerd wordt. Het gebruik van implantaten wordt wereldwijd voor diverse toepassingen overwogen, met name in de zorg.

De eerste implantaten zijn in Nederland reeds ingebracht. De VIP-gasten van de Baja Beach Club in Rotterdam krijgen met een RFID-tag in hun arm automatisch gratis toegang tot de club, het VIP-deck en kunnen met behulp van hun tag ook de drank afrekenen.<sup>3</sup>

### 2.2.4 Overige systemen

Naast deze drie redelijk uniforme systemen bestaat er nog een restcategorie waarin alle systemen vallen die niet onder de drie bovenstaande categorieën geschaard kunnen worden. Het gaat dan om zogenaamde maatwerksystemen waarbij de concreet toegepaste RFID-technologie afhankelijk is van de toepassing.

## 2.3 Het EPCglobal Network

Het EPCglobal Network is een door GS1 en het Uniform Code Council (UCC)<sup>4</sup> binnen het Auto-ID lab ontwikkelde set van standaarden voor het onder meer het vastleggen van unieke nummers in RFID-tags binnen de logistieke keten. Deze nummers kunnen gekoppeld worden aan databases waarin eveneens gestandaardiseerde informatie is vastgelegd over het product. Hiermee wordt het moge-

lijk om individuele producten te identificeren en bijbehorende informatie over deze producten op te zoeken. Gezien het belang van het EPCglobal Network en het feit dat de discussie rondom RFID en privacy zich momenteel grotendeels toespitst op het gebruik van RFID in consumentengoederen, zal nadere aandacht worden besteed aan dit initiatief. De standaardisatie werkzaamheden rondom het EPCglobal Network dienen echter in breder verband te worden gezien. Zo zullen de EPCglobal standaarden bijvoorbeeld in ISO en CEN normen geïncorporeerd worden. Daarnaast zijn er nog tal van gebieden waar RFID gebruikt wordt maar waarop het EPCglobal Network niet ziet (bijvoorbeeld de identificatie van personen). Ook op deze gebieden wordt gewerkt aan internationale standaarden.

Voordat we overgaan tot de bespreking van het EPCglobal Network dient de kanttekening te worden gemaakt dat de technische en organisatorische werking van het EPCglobal Network nog niet volledig uitgekristalliseerd is. Bepaalde technische voorzieningen zijn nog niet volledig uitgewerkt waardoor een verkenning van het systeem (ook in juridische zin) tot op zekere hoogte tentatief blijft.

### 2.3.1 Electronic Product Code (EPC)

Aan de basis van het EPCglobal Network ligt de Electronic Product Code. Electronic Product Code, afgekort EPC, is de nummerstandaard die voor de identificatie van objecten wordt gebruikt. De huidige EAN.UCC nummerstandaard wordt gebruikt in het EPCglobal Network. De EPC is een (vooralsnog 96 bits) code die de fabrikant, de productcategorie en het itemnummer van een artikel aangeeft. Het Auto ID Center heeft een 64 bits versie en een 96 bits versie van de code voorgesteld. Versies met meer bits, worden voorlopig niet toegepast omdat het extra geheugen de chip (en daarmee de tag) duurder maken.

<sup>2</sup> <<http://www.rfidjournal.com/article/articleview/921/1/1/>>

<sup>3</sup> <<http://www.baja.nl>>

<sup>4</sup> De beide organisaties gaan sinds februari 2005 verder onder de naam GS1 (zie: <<http://www.gs1.org>>)

01.2651977.171978.421534308		
Code	Naam	Betekenis
01	Header	versienummer EPC
2651977	EPC Manager	28 bits identificatiecode fabrikant (> 268 miljoen unieke fabrikanten)
171978	Object Manager	24 bits identificatiecode producten (> 16 miljoen producten per fabricant)
421534308	Serial Number	36 bits identificatiecode individuele artikelen (> 68 miljard individuele artikelen per product)

Op de chip zelf wordt enkel de EPC vastgelegd, geen additionele informatie. Omdat binnen het EPCglobal Network de EPC te koppelen is aan informatie in een achterliggende database (zie verderop in dit hoofdstuk), is het niet noodzakelijk om alle informatie op te slaan op de chip zelf, hetgeen kostenbesparend werkt.

### 2.3.2 Middleware

De koppeling tussen readers en achterliggende applicaties (zoals voorraadbeheer) geschiedt via middleware-oplossingen. In de oorspronkelijke opzet van het systeem werd dit deel van het EPCglobal Network de 'Savant' genoemd. De middleware-oplossing wordt gevormd door gedistribueerde, hiërarchisch georganiseerde netwerkcomponenten welke de informatiestromen die worden gegenereerd door diverse readers aggregeren, organiseren en coördineren. Met behulp van middleware kan een lokaal netwerk van readers worden gecreëerd. De middleware-oplossing kan de (georganiseerde) informatie van diverse readers doorsturen naar een hiërarchisch hoger middleware-component van de middleware-oplossing. Op deze manier kan een robuust, decentraal georganiseerd netwerk worden gemaakt dat goed schaalbaar is en bestaande of publieke bedrijfsnetwerken niet overbelast met EPC-data.

### 2.3.3 Physical Markup Language (PML)

De Physical Markup Language (PML) is een op XML-gebaseerde vocabulaire om informatie over producten uitgerust met EPC-tags weer

te geven en te distribueren. Het doel van de PML is om de informatieuitwisseling tussen het EPCglobal Network (bijvoorbeeld de readers) en bestaande ERP- en SCM-systemen te standaardiseren, waardoor communicatie tussen deze verschillende systemen mogelijk wordt.<sup>6</sup>

### 2.3.4 Object Name Service (ONS)

Omdat op de tags binnen het EPCglobal Network alleen de EPC wordt opgeslagen en geen verdere informatie, is een systeem noodzakelijk dat de EPC koppelt aan informatie over het product. De Object Name Service (ONS) vervult deze taak. Het ONS is een volledig geautomatiseerde adresseringsdienst welke qua werking te vergelijken is met het Domain Name System (DNS). De Object Name Service koppelt een EPC aan het IP-adres van een EPC-IS waarin meer informatie is te vinden over het product (Saram 2002). Het beheer en de operatie van het ONS is door EPCglobal uitbesteed aan Verisign.

### 2.3.5 EPC-Information Service (EPC-IS)

De EPC-Information Services zijn de daadwerkelijke opslagplaatsen waar informatie over met een EPC geëtiketteerd object vastgelegd is. Een informatievragende partij kan middels de EPC-IS informatie krijgen over een met een EPC geëtiketteerd product. Een EPC-IS bevat de voor het EPC-netwerk relevante gegevens van het object. Dit betreft een subset van de informatie die in een bedrijfsinterne applicatie is geregistreerd welke buiten de 'firewall' van het bedrijf aan het netwerk beschikbaar

<sup>5</sup> Bewerkt van <<http://www.rfidwizards.com>>

<sup>6</sup> <<http://www2.inf.ethz.ch/~floerkem/>>

wordt gesteld. Zo'n EPC-IS kan bij het bedrijf zelf zijn opgesteld, maar ook bij een dienstverlener, die dan een EPC-Information Service aanbiedt.

### *2.3.6 EPC Discovery Services (EPC-DS)*

De EPC Discovery Services maken het (in samenhang met de Object Name Service) mogelijk voor de betrokken partijen om binnen de logistieke keten meerdere gedistribueerde EPC Information Services aan te spreken. Dit betekent dat Bedrijf A informatie over een product kan opvragen welke ligt opgeslagen in de EPC-IS van bijvoorbeeld Bedrijf B en Bedrijf C. Een EPC-DS verschaft een verwijzingsmechanisme dat gebruikers in staat stelt om snel te achterhalen in welke EPC-IS'en informatie over de EPC te vinden valt. Een EPC-DS is dus als het ware een zoekmachine op het EPCglobal netwerk. Dit soort software gaat een belangrijke rol spelen in de strijd tegen namaak en bij recall acties.

## **2.4 Tijdspad RFID**

In tegenstelling tot wat velen denken is RFID geen nieuwe technologie en wordt het reeds op grote schaal voor verschillende toepassingen gebruikt. Zo wordt RFID wereldwijd onder andere gebruikt voor toegangscontrole bij gebouwen, het identificeren van vee, anti-diefstalsystemen en het automatisch afrekenen van tol bij tolwegen.

De privacy gerelateerde vragen bij het gebruik van RFID hebben voornamelijk betrekking op het gebruik van RFID in de detailhandel waar wordt gestreefd naar 'item level tagging'. Dit houdt in dat ieder consumentengoed voorzien zal worden van een uniek nummer dat met behulp van een RFID-signaal eenvoudig is uit te lezen. Dit unieke nummer kan vervolgens automatisch gekoppeld worden aan achterliggende informatie die is opgeslagen in de databases van de diverse partners in de logistieke keten. Dit systeem wordt het EPCglobal Network genoemd. Dankzij het EPCglobal Network wordt het in de nabije toekomst mogelijk om specifieke informatie over individuele producten op te vragen zoals productiedatum, houdbaarheidsdatum en kleur, maar bijvoorbeeld ook zaken als de route die het product in de logistieke keten heeft afgelegd.

De redenen waarom RFID niet al eerder op grote schaal is toegepast in de logistiek en de detailhandel zijn hoofdzakelijk van tech-

nische en economische aard. Zo vormden de prijs, afmeting en gebrek aan standaardisatie van RFID-tags lange tijd een barrière voor een brede toepassing. Deze barrières worden echter in hoog tempo geslecht door de voortschrijdende stand van de technologie, miniaturisering, standaardisatie en massaproductie. De verwachting is dat binnen enkele jaren de prijs van RFID-tags dermate gedaald is, dat RFID-tags in of op elk product geplaatst kunnen worden. De schattingen wanneer item level tagging daadwerkelijk plaats gaat vinden lopen echter uiteen van 2007 tot 2015.

De toepassing van RFID op productniveau is hoofdzakelijk afhankelijk van de prijs van de individuele RFID-tag. Als het 'magische' prijskaartje voor een passieve RFID-tag wordt vijf dollarcent genoemd, pas bij deze prijs wordt item level tagging daadwerkelijk aantrekkelijk. Maar naast de prijs voor de RFID-tag zelf vormen ook de kosten voor de overige onderdelen van de EPCglobal Network-infrastructuur voornamelijk een barrière voor de uitgebreide toepassing van RFID. Tot die tijd zal RFID in de logistieke keten naar verwachting met name worden toegepast op returnable transport items (pallets, kratten, rolcontainers, trolleys) binnen een onderneming.

Wat betreft andere sectoren zoals transport en zorg dient per individuele toepassing een kosten-baten afweging gemaakt te worden.

## **2.5 Toekomstvisie RFID**

De verwachting is dat RFID-technologie in de komende jaren een enorme vlucht zal nemen. Volgens consultancyfirma Frost en Sullivan zal in 2010 de omzet in de markt voor RFID-technologie 11,7 miljard dollar bedragen (Frost & Sullivan 2004). Hierbij zal de ontwikkeling van RFID in de komende jaren waarschijnlijk het hierboven beschreven groeipad volgen. In de toekomst zal RFID echter een nog prominentere rol in onze leefwereld gaan spelen.

De algemene verwachting is dat RFID een van de sleuteltechnologieën gaat worden voor de ontwikkeling van 'Ambient Intelligence'. Ambient Intelligence (Aml) is een visie op de toekomst van de informatiesamenleving, waarbij gebruikersvriendelijkheid, efficiëntie en het ondersteunen van gebruikers en communicatie tussen gebruikers centraal staan. In deze visie worden mensen in de toekomst

omgeven door objecten (van sleutels tot ondergoed) die intelligentie bevatten en via intelligente interfaces kunnen reageren en anticiperen op menselijke behoeften.<sup>7</sup>

Hierbij moet gedacht worden aan intelligente koelkasten die zelf de boodschappen doen, wasmachines die was op kleur en textielsoort kunnen sorteren, auto's die zichzelf besturen en persoonlijke elektronische assistenten die onze afspraken plannen.

Samen met technologieën als bijvoorbeeld IPv6, Near Field Communication (NFC), wireless, breedband, mobiele telefonie, GPS, Bluetooth, agenttechnologie, swarm intelligentie, embedded systems en grid computing, zal RFID deze toekomstvisie realiseerbaar maken.

## 3 Privacy

In met name de Verenigde Staten is fel protest ontstaan tegen het gebruik van RFID-technologie.<sup>8</sup> Daar is momenteel ongeveer een kwart tot een derde van de burgers bekend met RFID, en ongeveer drie kwart hiervan maakt zich zorgen om hun privacy als het om RFID gaat (Big Research 2004). De sterke anti-RFID lobby in de Verenigde Staten valt met name te verklaren vanuit het feit dat in de Verenigde Staten minder sterke wetgeving geldt voor de bescherming van persoonsgegevens dan die in Europa. Toch beperkt het protest tegen RFID zich niet tot de Verenigde Staten, ook in Duitsland en het Verenigd Koninkrijk is protest op gang gekomen.<sup>9</sup>

In Nederland is momenteel zo'n twaalf procent van de bevolking bekend met de term RFID (Capgemini 2005a). De Nederlandse consument staat in zijn algemeenheid positiever tegenover RFID dan de Amerikaanse consument: ongeveer de helft van de Nederlandse consumenten die bekend zijn met RFID ziet voornamelijk voordelen, slechts zeven procent ziet voornamelijk nadelen, de resterende consumenten staan neutraal tegenover RFID of hebben geen mening. Toch maakt men zich in Nederland ook zorgen over RFID. Hierbij worden als belangrijkste issues genoemd: het gebruik van (persoons)gegevens door derden, het kunnen volgen van consumenten via hun aankopen, het lezen van tags over langere afstand, en de toename van direct marketing. Al deze zorgen zijn gerelateerd aan privacy; de consument maakt zich minder zorgen over gezondheidskwesties (straling) en milieuproblemen (Capgemini 2005a).

### 3.1 Wat is privacy?

Om tot een zorgvuldige analyse te komen van de mogelijk privacyrisico's van RFID is het zaak het begrip privacy nader te belichten en het in de context van RFID-toepassingen verder te onderzoeken. Een eenduidige definitie van het begrip privacy is namelijk moeilijk tot niet te geven. Dit komt hoofdzakelijk door het feit dat het begrip privacy slechts vorm krijgt door verwijzing naar een complex geheel van sociale, culturele, politieke, juridische en filosofische factoren

waarvan het afhankelijk is (Gutwirth 1998, p. 40). Het geven van een definitie is daarom vaak verwarrender dan het niet geven van een definitie omdat iedereen verschillende voorstellingen heeft bij het begrip privacy en verschillende waardes hecht aan de diverse onderdelen die het begrip privacy invulling geven.

Privacy is een noodzakelijke voorwaarde voor de ontwikkeling en de autonomie van het individu. In dit kader vervult privacy verschillende functies. Zo maakt privacy het onder andere mogelijk om ons tijdelijk te onttrekken aan sociale omgang en oordeelsvorming, beschermt het ons tegen ongewenste inmenging in ons persoonlijke leven en verschaft het de tijd en ruimte om onze gedachten te vormen, ordenen en formuleren.

De hiervoor genoemde functies van privacy behoren tot het klassieke denken over privacy en vormen als zodanig de kern van de functies die privacy vervult. Een modernere functie van privacy die steeds verder toeneemt in belang is die van het limiteren van macht over onze persoon. Deze functie heeft zijn oorsprong in het moderne wetenschappelijke wereldbeeld waar kennis gelijk wordt gesteld aan macht. Hoe meer informatie over een object bekend is, hoe beter iemand in staat is om dit object te gebruiken, controleren of manipuleren. Dit geldt voor objecten in de natuur, maar ook voor personen. Door onze persoonlijke informatie af te schermen van de buitenwereld zijn we minder beïnvloedbaar door deze buitenwereld. Privacy wordt in deze zin dus gebruikt om informatie over onszelf af te schermen waardoor deze informatie niet door derden gebruikt kan worden om invloed over ons te krijgen.

### 3.2 Het recht op privacy

Omdat het recht op privacy van dusdanig groot belang is voor de mens, is het een van de grondrechten waarop een ieder zich kan beroepen. Het recht op privacy is echter niet absoluut en dient te worden afgewogen tegen de gerechtvaardigde belangen van de maatschappij of delen daarvan, bijvoorbeeld andere individuen (Etzioni 1999).

<sup>8</sup> Zie onder andere: <<http://www.nocards.org>> ; <<http://www.boycottgilllette.com>> en <<http://www.boycottbenetton.org/>>  
<sup>9</sup> <<http://www.spychips.com/metro/>> en Alok Jha 2003

In het recht duidt het begrip privacy op een levenssfeer die eigen is aan de persoon. Het recht op privacy is het recht op ontoegankelijkheid van de persoonlijke levenssfeer (Blok 2002, p. 278). Uit welke elementen deze persoonlijke levenssfeer precies bestaat vormt evenals de definitie van privacy een niet aflatende bron van discussie.

De woning, het intieme leven, de vertrouwelijke communicatie en de lichamelijke integriteit vormen sinds de conceptie van het privacybegrip de kern van de persoonlijke levenssfeer. Sinds de komst van het computertijdperk begin jaren zestig worden ook persoonsgegevens tot de persoonlijke levenssfeer gerekend. Dit betekende een aanzienlijke uitbreiding van de persoonlijke levenssfeer, welke de helderheid van het privacybegrip volgens sommigen geen goed heeft gedaan (Blok 2002).

### **3.3 Persoonsgegevens en informationele privacy**

Het begrip privacy is in de laatste decennia aan een sterke verandering onderhevig. Toenemende digitalisering en informatisering maken de huidige samenleving in steeds hogere mate transparant (Franken 2000). Informatie die betrekking heeft op personen is in toenemende mate vast te leggen en te koppelen aan andere informatie. Op deze manier wordt het steeds beter mogelijk om aan de hand van informatie over een persoon een accuraat profiel van deze persoon samen te stellen. Dit kan allerlei voor het individu onwenselijke gevolgen hebben, zeker als dit profiel niet helemaal volledig is of subjectief wordt geïnterpreteerd. Zo kan bijvoorbeeld op basis van het profiel worden beoordeeld of iemand wel in aanmerking komt voor een bepaalde dienst, of kunnen bepaalde aspecten van iemands persoonlijkheid publiekelijk worden gemaakt. Om deze redenen is het denken over privacy in het kader van persoonsgegevens uitgegroeid tot een recht op *informationele privacy*, oftewel het recht op ontoegankelijkheid van persoonlijke informatie. Alan Westin heeft in zijn grondleggende werk *Privacy and Freedom* het begrip informationele privacy als volgt gedefinieerd:

*'The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated.'* (Westin 1967)

In feite betreft het hier een recht op *informationele zelfbeschikking*, hetgeen wil zeggen dat een ieder het recht heeft zelf te bepalen welke informatie over hem- of haarzelf openbaar wordt gemaakt. Nu is het voor de werking van onze moderne maatschappij en economie van groot belang dat (persoons)gegevens onder bepaalde omstandigheden wél verwerkt kunnen worden, immers zonder het verwerken van persoonsgegevens zouden vele processen en transacties in onze maatschappij een stuk moeilijker, minder efficiënt of simpelweg onmogelijk zijn. Daarom is er in Nederland geen absoluut recht op informationele zelfbeschikking. De verwerking van persoonsgegevens dient uiteraard wel zorgvuldig plaats te vinden.

Voorts zijn er gevallen denkbaar dat het algemeen belang of dat van een derde zwaarder weegt dan het recht op informationele privacy. Om deze reden, dient bij de verwerking van persoonsgegevens te worden gekeken welk belang zwaarder weegt: dat van de degene wiens gegevens worden verwerkt, of dat van de verwerker.<sup>10</sup> Bij deze afweging dient wel het bijzondere karakter van het grondrecht in ogenschouw te worden genomen.

De idee van informationele privacy komt tot uitdrukking in de wet- en regelgeving op het gebied van privacy. Om zaken als het profileren van individuen en willekeurige openbaarmaking te beperken is in Nederland de Wet bescherming persoonsgegevens (WBP) van kracht (zie hoofdstuk 5).

### **3.4 Beginselen van behoorlijk gegevensbeheer**

In 1973 publiceerde de US Department of Health, Education and Welfare een rapport naar aanleiding van de toenemende geautomatiseerde verwerking van gegevens (US Dept. Health 1973). Dit grondleggende rapport bevatte een aantal 'Fair Information Practice Principles' (beginselen van behoorlijk gegevensbeheer) welke de basis vormden voor veel internationale wet- en regelgeving. Zo staan de Fair Information Practice

Principles aan de basis van de gezaghebbende OECD Privacy Guidelines welke op hun beurt weer ten grondslag hebben gelegen aan Richtlijn 95/46/EG en de WBP. Een uitgebreidere bespreking van de beginselen en hun oorsprong kunt u vinden in bijlage II van dit rapport.

### ***3.5 Onderscheid tussen publieke en private organisaties***

Er bestaat een verschil in de manier waarop het recht op privacy wordt geïnterpreteerd voor publieke organisaties en voor private organisaties. De algemene stelregel die voor zowel overheden als bedrijven geldt is dat niet meer informatie mag worden verzameld over natuurlijke personen dan strikt noodzakelijk.

Binnen de overheid kan een onderscheid worden gemaakt tussen zaken als: administratieve taken (bijvoorbeeld de sociale zekerheid en de belastingheffing), taken die horen bij het handhaven van de openbare orde en veiligheid en tot slot de opsporingstaken van het Openbaar Ministerie. Voor al deze taken geldt dat een eventuele inbreuk op het recht op privacy bij de wet voorzien moet zijn, een gerechtvaardigd doel moet dienen en noodzakelijk moet zijn in een democratische samenleving.

De meeste bedrijven zien de zorgvuldige verwerking van persoonsgegevens niet alleen als wettelijke plicht maar ook als een onderdeel van verantwoord ondernemen. Een belangrijke reden hiervoor is dat bedrijven naast de eisen uit wet- en regelgeving ook rekening dienen te houden met het sentiment in de markt. Wanneer een bedrijf niet zorgvuldig omgaat met gegevens, of de persoonlijke levenssfeer van de consument schendt, dan kan dit een negatieve weerslag hebben op de reputatie van het bedrijf. Een verantwoord privacybeleid is dus in het voordeel van zowel bedrijf als consument.

## 4 Mogelijke risico's

De unieke eigenschappen van RFID kunnen bij onzorgvuldig of onrechtmatig gebruik van RFID een inbreuk op de privacy en individuele vrijheid van de burger veroorzaken. Het bezwaar van tegenstanders van RFID is dan ook dat het gebruik van RFID-systemen afbreuk doet aan het recht op privacy, meer in het bijzonder het recht op informatiele zelfbeschikking. De reden hiervoor is dat de hoeveelheid persoonsgegevens die in potentie heimelijk (dus zonder wetenschap van de betrokkene) zou kunnen worden verzameld enorm is. Deze informatie zou kunnen worden aangewend om burgers of consumenten te beïnvloeden of te controleren. In dit hoofdstuk worden enkele veel gehoorde bezwaren tegen RFID op een rij gezet. In hoofdstuk 6 worden de risico's die in dit hoofdstuk worden genoemd nader geanalyseerd en in perspectief geplaatst.

Een kanttekening die gemaakt dient te worden voordat we de privacyrisico's van RFID verkennen, is dat niet gezegd is dat bij het gebruik van RFID-systemen per definitie een risico voor de privacy ontstaat. RFID kent vele toepassingsvormen die geen enkel risico voor de privacy vormen. Voor de toepassingen die dit mogelijk wel vormen zijn allerlei maatregelen denkbaar die risico's helpen verkleinen of uitsluiten. Uiteindelijk zullen de concrete toepassing en de daarbinnen genomen maatregelen ter bescherming van de privacy bepalen wanneer er wel of niet een risico ontstaat.

Een tweede kanttekening betreft het feit dat een aantal risico's die soms expliciet aan RFID toegewezen worden, in feite ook al bestaat bij het gebruik van huidige identificatietechnieken zoals de barcode. Zo is de koppeling van gegevens binnen een database geen nieuw privacyrisico dat is ontstaan door de opkomst van RFID, maar een risico dat al veel langer bestaat omdat het samenhangt met het gebruik van databases. Dit risico wordt ondervangen doordat er wet- en regelgeving bestaat die het gebruik van persoonsgegevens in databases reguleert (zie hoofdstuk 5).

### **4.1 Het op afstand heimelijk uitlezen van tags door readers**

De onzichtbaarheid van RFID-tags wordt als een van de belangrijkste privacyrisico's van RFID gezien. Met name passieve RFID-tags kunnen dermate klein worden gemaakt, dat deze voor het blote oog niet of nauwelijks zichtbaar zijn.<sup>11</sup> Op deze manier is het dus voor een individu moeilijk tot onmogelijk vast te stellen of een product een RFID-tag bevat. De mogelijkheid bestaat dus dat er informatie via de RFID-tag wordt verzameld over een product – en als gevolg daarvan ook over de persoon aan wie het product toebehoort (wat hij op dat moment draagt, in zijn tas heeft, gaat eten) - zonder dat deze persoon daarvan op de hoogte is. Een aspect dat daarbij mede van belang is, is de maximale leesafstand tussen reader en tag.

Naast RFID-tags kunnen ook readers verborgen worden. Hoewel de readers qua afmetingen een stuk groter zijn dan RFID-tags bestaan er tal van mogelijkheden om de aanwezigheid van readers te verhullen. Dit brengt het gevaar met zich mee dat individuen niet weten waar en wanneer ze gescand worden op de aanwezigheid van RFID-tags in producten, kleding et cetera die zij bij zich dragen. Wat daarbij eveneens meespeelt is de maximale leesafstand van de reader, met andere woorden: welke reikwijdte heeft het radiosignaal en van welke afstand is het dus mogelijk producten uit te lezen. Het mogelijk duidelijk zijn dat het risico voor de privacy groter is naarmate de leesafstand van de reader tot de tag toeneemt.

### **4.2 Traceability door unieke identificatie**

RFID-systemen maken het in theorie mogelijk om mensen te volgen aan de hand van de RFID-tags die zij op of bij zich dragen. Dit probleem wordt relevanter op het moment dat verschillende RFID-systemen geïntegreerd worden tot een groter surveillance-systeem.

Volledigheidshalve moet worden vermeld dat er ook barcodesystemen beschikbaar zijn waarmee unieke identificatie van afzonderlijke objecten mogelijk is. Deze worden op consumentenartikelen nauwelijks toegepast, maar wel op verzendeenheden. Het kunnen

<sup>11</sup> Zo wordt bijvoorbeeld al gewerkt aan 'smart dust', RFID-tags van slechts enkele millimeters groot.

volgen van afzonderlijke objecten, door gebruik van zulke unieke codes, zowel in barcode als in chipformaat, levert goede mogelijkheden voor het onverhoopt moeten terughalen van artikelen ("recall", bijvoorbeeld bij een productiefout), en ook bij het vaststellen van de echtheid van het object, in de strijd tegen namaak ("counterfeiting"). De identificatie mogelijkheden zijn dus niet uniek voor RFID, maar wel eenvoudiger.

Het kunnen volgen van een individueel product vormt een risico voor de privacy op het moment dat het product te koppelen is aan een persoon. In geval van een barcode kan ook een koppeling met een persoon plaatsvinden, maar bij de meeste barcodes zal dit slechts een 'algemeen' nummer zijn. Men weet, bijvoorbeeld bij het afrekenen aan de kassa, op dat moment alleen dat een bepaald persoon een sprookjesboek heeft gekocht. Mocht op een andere plaats, verderop in de winkelstraat, de barcode opnieuw gescand worden -hetgeen zeer onwaarschijnlijk is omdat dit een actieve handeling vereist- ziet men alleen dat het een sprookjesboek betreft. Omdat er duizenden sprookjesboeken worden verkocht kan het spoor van het boek echter niet meer worden achterhaald (uit welke winkel het komt, hoe oud het is) en is koppeling met de natuurlijke persoon die het heeft gekocht niet mogelijk.

Wanneer dit sprookjesboek echter onderdeel uitmaakt van een uitgebreid RFID-systeem zoals het EPCglobal Network, dan is dit specifieke boek en (indien koppeling plaatsvond) de persoon die het gekocht heeft te volgen alsmede alle producten die hij of zij bij zich draagt (traceability). Daarbij komt nog dat het scannen van een barcode stukken lastiger zonder medeweten van de bezitter van het product is uit te voeren, dan het lezen van RFID-tags.

De mogelijkheid dat derden (andere bedrijven, maar ook particulieren) tags kunnen scannen is ook een bezwaar dat tegenstanders tegen bepaalde toepassingen van RFID hebben. Omdat het scannen van een tag (in het geval van het EPCglobal Network) enkel een EPC zal opleveren, is er pas sprake van relevante informatie op het moment dat een koppeling kan worden gemaakt met het EPCglobal Network waarbinnen de koppeling tussen EPC en achterliggende informatie gemaakt kan worden. Nu zullen particulieren deze toegang niet hebben, maar bedrijven

die deel uitmaken van het EPCglobal Network vaak wel. Er dient bij deze constatering wel rekening te worden gehouden met het feit dat indien het unieke nummer langdurige tijd gerelateerd kan worden aan een individu deze informatie mogelijkerwijs voor bepaalde partijen toch relevant wordt.

### **4.3 Data aggregatie en profiling**

De hoeveelheid informatie die in potentie door middel van een RFID-systeem verzameld kan worden is groot. Persoonlijke informatie verkregen door middel van een RFID-systeem kan gebruikt worden om een redelijk accuraat profiel van een individu samen te stellen. Deze informatie kan aangewend worden om een beter inzicht te krijgen in het gedrag van individuele personen waardoor er in het uiterste geval een verschuiving in de 'machtsbalans' tussen consument en aanbieder ontstaat. Een eerlijke overeenkomst kan onder druk komen te staan als de aanbieder over een uitgebreide kennis van de behoeften, gewoonten en interesses van een specifieke consument beschikt, terwijl deze niet weet dat de aanbieder deze kennis heeft (Artz 1999, p. 7).

### **4.4 Taggen van mensen**

Naast producten kunnen ook mensen worden uitgerust met een RFID-tag. De RFID-tag kan worden aangebracht op een drager die een persoon bij zich draagt (bijvoorbeeld een kaart, sleutel of halsketting), of daadwerkelijk direct (onderhuids) op de persoon. Het taggen van mensen opent een groot spectrum aan controlemogelijkheden dat wellicht misbruikt kan worden. Zo kunnen mensen gevolgd worden, kan hen de toegang tot bepaalde locaties, goederen of diensten worden ontzegd en kan informatie ontleend aan de RFID-tag voor andere doeleinden worden aangewend.

### **4.5 Illegaal gebruik**

Een ander bezwaar betreft de mogelijkheden die RFID kan bieden voor illegaal gebruik. Consumenten maken zich zorgen dat andere burgers met draagbare RFID-readers in hun boodschappentas, kleding of huis kunnen kijken. Consumenten voelen met name angst voor gerichte berovingen op basis van de informatie verkregen uit de RFID-tags.

## **4.6 *Systeemintegratie***

Een bedreiging die zich niet beperkt tot RFID maar zich uitstrekt tot alle systemen waarmee toezicht of controle kan worden uitgeoefend is systeemintegratie. Het koppelen van verschillende systemen zoals databases, camera's en RFID-systemen zorgt ervoor dat deze systemen tezamen veel effectiever worden. Met andere woorden, het geheel is meer dan de som der delen. Hoewel systeemintegratie vanuit het oogpunt van effectiviteit, efficiency en gemak toe te juichen valt, dient rekening te worden gehouden met de privacy en individuele vrijheid van de burger.

## 5 Huidig juridisch kader

Zo'n zeventig procent van de consumenten geeft aan dat zij eerder RFID-getagde producten zouden kopen als er wettelijke privacy-bescherming zou zijn voor RFID (Capgemini 2005a).<sup>12</sup> Zowel vanuit het oogpunt van consumentenbescherming, als vanuit het oogpunt van een versnelde en gecoördineerde invoering van RFID is het dus raadzaam de wettelijke bescherming van privacy in deze rapportage te verkennen.<sup>13</sup>

Er bestaat in Nederland, in tegenstelling tot wat velen denken, geen 'Wet op de Privacy'. Naast het recht op bescherming van de persoonlijke levenssfeer, vastgelegd in artikel 10 Grondwet, is het recht op privacy en de regels omtrent de omgang met persoonsgegevens gecodificeerd in een aantal wetten. Wij zullen ons in dit rapport beperken tot de bespreking van de Wet bescherming persoonsgegevens (WBP) en Richtlijn 2002/58/EG (geïmplementeerd in de Telecommunicatiewet) omdat deze wetten met het oog op de bescherming van de privacy in het kader van RFID het meest relevant zijn.

22

### 5.1 Wet bescherming persoonsgegevens

De informationele privacy, een facet van het recht op privacy wat in het kader van RFID het meest relevant is, wordt in Nederland hoofdzakelijk via de WBP beschermd. De WBP geeft nadere invulling aan het grondrecht op bescherming van de persoonlijke levenssfeer (artikel 10 Grondwet) en vloeit voort uit een aantal internationale beginselen voor de behoorlijke verwerking van persoonlijke gegevens. Voor een uitgebreid overzicht van de achtergrond bij de WBP verwijzen wij u naar de bijlagen van dit rapport. De WBP, welke gezien de techniekonafhankelijke structuur, van toepassing kan worden geacht op de verwerking van persoonsgegevens met behulp van een RFID-systeem, vormt het uitgangspunt voor onze bespreking van de privacyrechtelijke aspecten van RFID.

#### 5.1.1 Achtergrond

De toenemende ontwikkelingen en mogelijkheden van informatie- en communicatietechnologie deden het belang van een effectieve bescherming van persoonsgegevens binnen de Europese Unie steeds evidenter worden. In 1981 werd hiertoe het 'Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens' in Straatsburg opgesteld.<sup>14</sup> De Raad van Europa voorzag dat de verwerking en de uitwisseling van persoonsgegevens aanzienlijk werd vergemakkelijkt en dat tussen ondernemingen in verschillende Lidstaten steeds meer gegevens zouden worden uitgewisseld.

De beginselen die aan het Verdrag ten grondslag lagen vormden ook de basis voor het huidige juridisch kader dat hoofdzakelijk voortvloeit uit Richtlijn 95/46/EG (Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens). Deze richtlijn moest er toe leiden dat het niveau van de bescherming van de rechten en vrijheden van personen -met name het recht op bescherming van de persoonlijke levenssfeer- in alle Lidstaten gelijkwaardig zou zijn en vrij verkeer van persoonlijke data gereguleerd en vereenvoudigd werd. Inmiddels is Richtlijn 95/46/EG door alle Lidstaten geïmplementeerd. In Nederland heeft dit geleid tot de invoering van de WBP (als vervanging voor de Wet persoonsregistraties).

#### 5.1.2 Wat is een persoonsgegeven?

De WBP is van toepassing op verwerkingen van persoonsgegevens. Een persoonsgegeven is iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene).<sup>15</sup> Als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.<sup>16</sup> We kunnen meerdere categorieën persoonsgegevens onderscheiden:

12 Deze constatering geeft aan dat burgers veelal niet op de hoogte zijn van hun rechten en plichten uit onder andere de WBP.

13 Zie hiervoor ook de bijlagen bij dit rapport.

14 Raad van Europa, European Treaty Series Nr. 108. ondertekend op 28 januari, 1981

15 Artikel 1 WBP

16 Tweede Kamer, vergaderjaar 1997-1998, 25892, nr. 3 (MvT).

- *Gegevens die naar hun aard feitelijke informatie over een persoon geven.*  
Sommige gegevens verschaffen duidelijk feitelijke informatie over een persoon. De meest sprekende voorbeelden zijn iemands naam, geboortedatum of geslacht. Ook gegevens die een waardering over een natuurlijke persoon geven, bevatten informatie over die persoon (Sauerwein 2002, p. 12).
- *Gegevens die naar hun aard geen feitelijke informatie over een persoon geven.*  
Sommige gegevens hebben naar hun aard geen betrekking op een persoon. Desondanks kunnen deze gegevens persoonsgegevens zijn, indien de betrokkene identificeerbaar is. Gegevens die onder omstandigheden toch persoonsgegevens kunnen zijn, zijn bijvoorbeeld gegevens over ondernemingen en organisaties of informatie over voorwerpen. Met name deze laatste categorie is natuurlijk interessant in het kader van RFID.
  - *Gegevens over ondernemingen of organisaties.*  
Omdat het bij gegevens over ondernemingen of organisaties over het algemeen geen informatie aangaande natuurlijke persoon betreft, zijn deze gegevens geen persoonsgegevens. Echter gegevens die op natuurlijke personen betrekking hebben (bijvoorbeeld contactpersonen) zijn wel persoonsgegevens. Ook kunnen onder bepaalde omstandigheden gegevens over ondernemingen toch als persoonsgegevens worden aangemerkt, bijvoorbeeld in het geval van een eenmanszaak.
  - *Gegevens over voorwerpen of objecten.*  
Ook gegevens over voorwerpen of objecten die naar hun aard geen betrekking hebben op een persoon, kunnen toch onder omstandigheden als persoonsgegevens worden aangemerkt. Of een gegeven over een voorwerp of een object een persoonsgegeven is, hangt af van de context waarin het gegeven wordt verwerkt. Het gaat om de vraag of het gegeven mede bepalend is voor de wijze waarop iemand in het maatschappelijk verkeer wordt beoordeeld of behandeld (Sauerwein 2002, p. 13). Een specifieke

voorkeur voor bepaalde boeken of films kan, wanneer deze informatie gemakkelijk te koppelen is aan een persoon, bepalend zijn voor de manier waarop iemand in het maatschappelijk verkeer wordt beoordeeld of behandeld.

- *Bijzondere gegevens*  
Bijzondere gegevens, ook wel gevoelige gegevens genoemd, zijn gegevens betreffende een natuurlijke persoon welke iets zeggen over diens godsdienst, ras, politieke gezindheid, gezondheid, seksuele leven of gegevens omtrent het lidmaatschap van een vakvereniging.<sup>17</sup> Denk aan de medicijnen of andere producten die iemand koopt en die een indicatie van de gezondheid geven, seksuele hulpmiddelen die worden aangeschaft, het soort boeken dat iemand bestelt et cetera.

#### *Identificatie*

Om van een persoonsgegeven te kunnen spreken moet de persoon op wie het gegeven betrekking heeft identificeerbaar zijn. Een persoon is identificeerbaar indien de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning, is vast te stellen aan de hand van de gegevens die over deze persoon beschikbaar zijn. Er moet dus een direct of indirect verband zijn tussen de persoon en het gegeven.

Een direct verband (*direct identificerende gegevens*) wordt aangenomen indien de gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is. Direct identificerende gegevens zijn gegevens als naam, adres, geboortedatum, die in combinatie met elkaar dermate uniek en dus kenmerkend zijn voor een bepaalde persoon dat deze in brede kring met zekerheid of met een grote mate van waarschijnlijkheid, kan worden geïdentificeerd. Dergelijke gegevens worden in het maatschappelijk verkeer ook gebruikt om personen van elkaar te onderscheiden.<sup>18</sup>

Er is sprake van een indirect verband (*indirect identificerende gegevens*) indien de gegevens niet direct tot identificatie van een bepaald persoon leiden maar via nadere stappen de gegevens in verband kunnen worden gebracht met een bepaalde persoon. Deze gegevens kunnen zijn ontdaan van de naam,

<sup>17</sup> Art. 16 WBP

<sup>18</sup> Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3, p. 48

maar onder omstandigheden door combinatie met andere gegevens, of spontane herkenning weer worden teruggebracht op een bepaalde persoon (Sauerwein 2002, p. 13).

Daarnaast zijn er gegevens die dermate uniek zijn dat zij ook identificerend zijn. Zo is een sofi-nummer een persoonsgegeven omdat het uniek gekoppeld is aan een natuurlijke persoon en deze persoon daarmee identificeerbaar is. Aan het sofi-nummer gekoppelde informatie is hiermee potentieel ook een persoonsgegeven, omdat het door middel van het sofi-nummer terug te voeren valt op een natuurlijke persoon. Andere voorbeelden zijn biometrische kenmerken zoals het gezicht, de stem of een vingerafdruk.<sup>19</sup>

Een belangrijk aspect bij identificatie zijn de mogelijkheden van de verantwoordelijke voor de gegevensverwerking om een persoon te identificeren. Er dient gekeken te worden naar de middelen die een verantwoordelijke kan of zal inzetten om een persoon te identificeren. Hierbij moet in concrete gevallen rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.<sup>20</sup>

### *5.1.3 Wanneer is er bij RFID sprake van een persoonsgegeven?*

De WBP is van toepassing op het moment dat persoonsgegevens van een betrokkene door een verantwoordelijke gedeeltelijk of geheel geautomatiseerd worden verwerkt. Er bestaan echter een aantal uitzonderingen op deze hoofdregel. In welke gevallen de WBP wel en niet van toepassing is wordt uiteengezet in artikel 2 van de WBP. Dit betekent dat het antwoord op de vraag of er sprake is van geautomatiseerde verwerking van persoonsgegevens in het kader van RFID van geval tot geval beoordeeld zal moeten worden. Hierbij hangt veel af van de technische inrichting van een RFID-systeem.

Zoals in de vorige paragraaf reeds is aangegeven blijkt uit de WBP dat onder een persoonsgegeven wordt verstaan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

De informatie die wordt verkregen uit een RFID-tag kan dus een persoonsgegeven zijn indien de informatie terug te voeren valt op een geïdentificeerde of identificeerbare per-

soon. Een dergelijke situatie kan op de volgende manieren ontstaan:

#### *Opslag van persoonsgegevens in de RFID-tag*

De eerste mogelijkheid waarbij er vrijwel direct sprake is van de verwerking van persoonsgegevens als een RFID-tag wordt uitgelezen, is indien persoonsgegevens opgeslagen liggen in de RFID-tag zelf. Afhankelijk van de gekozen toepassing (zoals beveiliging of zorg) kan het nuttig of noodzakelijk zijn persoonsgegevens (NAW gegevens, biometrische kenmerken et cetera) op te slaan in een RFID-tag om daarmee het proces van identificatie, authenticatie, en autorisatie te vergemakkelijken. De opslag van persoonsgegevens op een RFID-tag gebeurt met name op smartcards, andersoortige tokens en implantaten.

#### *Koppeling van persoonsgegevens aan informatie uit de RFID-tag*

De meeste smart labels en tags van maatwerksystemen zullen enkel een unieke code bevatten. Zo wordt in het EPCglobal Network (de dominerende standaard op dit gebied) enkel een unieke code opgeslagen. De unieke code die op een smart label wordt opgeslagen kan met behulp van de reader en achterliggende middleware gekoppeld worden aan additionele productinformatie die ligt opgeslagen in een database. Op dit moment is er nog geen sprake van een persoonsgegeven, immers de informatie is nog niet terug te voeren op een natuurlijke persoon.

De koppeling komt pas tot stand op het moment dat de unieke productcode in de tag gekoppeld wordt aan een natuurlijke persoon bijvoorbeeld via een (pin)betaling, factuur, of loyaltycard systeem. In geval van een betaling in een supermarkt zou er dus sprake zijn van het verwerken van persoonsgegevens indien de supermarkt de gegevens omtrent de afgerekende producten koppelt aan de persoon die ze gekocht heeft, bijvoorbeeld door middel van een klantenkaart, betaling met creditcard, maar bijvoorbeeld ook door het koppelen van camerabeelden van de consument aan informatie uit RFID-tags.

Dit betekent echter ook dat in het geval van het lezen van tags zonder dat er koppeling met een natuurlijke persoon plaatsvindt, geen sprake is van het verwerken van per-

19 Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3, p. 48

20 Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3, p. 49

soonsgegevens. Bij het uitlezen van tags in de kleding van een persoon die in een winkel loopt, zonder dat deze gegevens gekoppeld worden aan de persoon die ze draagt, is de WBP veelal niet van toepassing. Het is echter voor de privacy en de privacybeleving van de burger ook van belang rekening te houden met privacyvraagstukken die niet direct zijn terug te voeren op de verwerking van persoonsgegevens. Om deze reden bestaat momenteel internationaal nog enige discussie over de vraag of het enkel dragen van een RFID-tag op het lichaam (in bijvoorbeeld kleding of een boodschappentas) of het bezit ervan voldoende voorwaarde is om van een persoonsgegeven te spreken.

#### *De RFID-tag als persoonsgegeven?*

Een laatste zienswijze is om alle informatie uit een RFID-tag per definitie als een persoonsgegeven te beschouwen, hetgeen dus betekent dat wanneer een reader een RFID-tag uitleest die in het bezit is van een persoon, er reeds sprake is van de verwerking van persoonsgegevens. De Franse toezichthouder op de bescherming van persoonsgegevens, de CNIL, is deze mening voorsnog toegedaan.<sup>21</sup> Zij heeft op basis van de verwachting dat de hoeveelheid RFID-tags op objecten waarmee een persoon zich omringt enorm groot gaat worden (en individuele profiling daarmee een dusdanig groot risico gaat vormen) besloten RFID-tags op zichzelf al te zien als een persoonsgegeven. De Nederlandse organisatie voor digitale burgerrechten Bits of Freedom is dezelfde mening toegedaan.<sup>22</sup> Deze zienswijze heeft vanuit het oogpunt van consumentenbescherming als grootste voordeel dat de waarborgen uit de WBP in alle gevallen waar consumenten in aanraking komen met RFID van toepassing zijn.

Maar het voordeel dat de WBP in alle gevallen van toepassing is, is ook direct het grootste nadeel van deze interpretatie. Gezien de technische omstandigheid dat een RFID-tag (waaronder de EPC smart label) automatisch

communiceert met een reader op het moment dat deze binnen het stralingsveld daarvan komt, zou dit betekenen dat het enkele uitlezen van een RFID-tag, zelfs als dit alleen een nummer bevat, reeds een verwerking is in de zin van de WBP. Een dergelijke redenering gaat behoorlijk ver, omdat dit tot gevolg zou hebben dat nagenoeg iedere RFID-toepassing waarbij tags in aanraking komen met consumenten zou vallen onder het regime van de WBP. Dit zal in bepaalde gevallen voor gebruikers van RFID tot onwerkbaar situaties kunnen leiden. Immers, bedrijven zouden aan alle bepalingen van de WBP moeten voldoen, waaronder zaken zoals aanmelding van de verwerking bij het College bescherming persoonsgegevens, zelfs als zij niks met de informatie uit de uitgelezen tag kunnen of willen doen.<sup>23</sup> Het kunnen uitlezen van een nummer op een tag, betekent immers niet dat er ook sprake is van toegang tot de achterliggende database met productinformatie. Een reader in een electronicazaak kan misschien wel EPC-nummers uitlezen die uit een supermarkt afkomstig zijn, maar zal niet automatisch weten welke producten aan die nummers gekoppeld zijn, omdat deze geen toegang heeft tot de EPC-IS'en van de supermarkt.<sup>24</sup> Maar ook in gevallen waarin wél de productinformatie gelezen kan worden, betekent dit niet automatisch dat er ook daadwerkelijk wat mee wordt gedaan. Een reader kan enorme hoeveelheden data uitlezen, maar enkel die gegevens selecteren voor verdere verwerking die relevant zijn voor het doel van de RFID-toepassing.

Het in dit stadium van toepassing verklaren van de WBP op alle smart label toepassingen van RFID lijkt onnodig en onverstandig. Het risico bestaat dat door een dergelijk uitgebreid toepassingsbereik handhavingsproblemen ontstaan waardoor de kracht van de WBP verwaterd.<sup>25</sup> De WBP heeft tot doel de privacy van de burger te beschermen, op het moment dat de WBP ook van toepassing is op gegevensverwerkingen die totaal geen rele-

---

21 <<http://www.cnil.fr/index.php?id=1514&print=1>>

22 <<http://www.bof.nl>>

23 Wat melden van RFID-verwerkingen aangaat: daarvoor kan, indien daar aanleiding toe is, wellicht een vrijstelling gecreëerd worden door het College bescherming persoonsgegevens.

24 Uiteraard hangt de validiteit van deze redenering wel grotendeels af van de uiteindelijke inrichting van de autorisatieprocedures en authenticatievoorzieningen van het EPCglobal Network.

25 Een beslissing dat RFID-tags per definitie persoonsgegevens zijn zal naar alle waarschijnlijkheid tot grote capaciteitsproblemen leiden bij het College Bescherming Persoonsgegevens. Overigens is het capaciteitsargument op zichzelf natuurlijk nooit een reden om wel of niet te concluderen dat iets een persoonsgegeven is. De criteria uit de WBP bepalen uiteindelijk wanneer er sprake is van een persoonsgegeven.

vantie hebben voor de privacy van de burger wordt afbreuk gedaan aan zowel de *raison d'être* als de handhaving van de WBP, hetgeen een negatieve uitwerking kan hebben op de kracht en de geloofwaardigheid ervan.

De Werkgroep Privacy & RFID is daarom van mening dat altijd aan de hand van de omstandigheden van het geval bekeken moet worden of er sprake is van het verwerken van persoonsgegevens bij RFID en daaraan gerelateerde privacyrisico's. Het uitgangspunt dat elke RFID-tag op zichzelf al een persoonsgegeven is, is niet noodzakelijk, zal uiteindelijk zelfs afbreuk kunnen doen aan de bescherming van de privacy en maakt veel toepassingen voor gebruikers van RFID praktisch onhaalbaar. De mening van de Werkgroep vormt ook het uitgangspunt van de Artikel 29 Werkgroep (Artikel 29 Werkgroep 2005, p. 8).<sup>26</sup>

De Werkgroep zal er dan ook vooralsnog vanuit gaan dat er sprake is van geautomatiseerde verwerking van persoonsgegevens in het geval van (1) persoonsgegevens opgeslagen op de RFID-tag en (2) in het geval van koppeling van een uniek nummer opgeslagen in een RFID-tag welke gekoppeld kan worden aan een natuurlijk persoon via (a) een achterliggende ICT-infrastructuur of (b) anderszins, bijvoorbeeld door (video)camera's. In deze gevallen is de WBP van toepassing. In gevallen waarbij geen koppeling met een natuurlijke persoon plaatsvindt, is de WBP niet van toepassing. Voorbeelden zijn niet tot een persoon herleidbare klantenkaarten en algemene profielschetsen van klanten. In deze gevallen gaat het vaak om algemene informatie die een bedrijf wil verkrijgen: is mijn winkel inderdaad in trek bij de doelgroep waarop ik me gericht heb, is mijn winkel handig ingericht of moeten klanten te veel zoeken et cetera.

In bepaalde gevallen zou een aantasting van de privacy plaats kunnen vinden welke buiten de traditionele kaders van de WBP valt (Artikel 29 Werkgroep 2005, p. 6). Een supermarkt kan bijvoorbeeld herbruikbare RFID-tokens (bijvoorbeeld voor winkelwagentjes) uitgeven aan klanten welke weliswaar anoniem zijn, maar door een unieke nummering toch gekoppeld kunnen worden aan een indi-

vidu. Een tweede voorbeeld is het koppelen van koopgedrag van consumenten aan een unieke RFID-tag welke de consument altijd bij zich draagt (bijvoorbeeld een horloge of jas). Een derde voorbeeld is het uitlezen van data uit RFID-tags welke de aard van het object prijsgeven (bijvoorbeeld bepaalde medicatie, of de maat van kleding). Volgens de Artikel 29 Werkgroep zal in deze gevallen de WBP ook van toepassing kunnen zijn. Dergelijke gevallen zullen altijd aan de omstandigheden van het geval beoordeeld moeten worden.

Bedrijven dienen altijd rekening te houden met de privacy en privacybeleving van de consument, ook indien hiertoe geen directe verplichting bestaat vanuit de WBP. Transparantie richting de consument, goede beveiliging van gegevens, goede autorisatie- en authenticatievoorzieningen (wie mag welke gegevens zien?) en de algemene eis van 'verantwoord ondernemerschap' zijn van blijvend belang. Aan deze uitgangspunten kan in dit stadium het beste door middel van (sectorspecifieke) zelfregulerende initiatieven nadere invulling worden gegeven. De bepalingen uit de WBP kunnen hier als leidraad dienen. Dergelijke zelfregulerende initiatieven dienen wel gepaard te gaan met effectieve handhavingssystemen, om een adequaat niveau van bescherming te bieden en het vertrouwen van de consument te stimuleren.

#### 5.1.4 Inhoud Wet bescherming persoonsgegevens

Zoals eerder aangegeven zijn de beginselen van behoorlijk gegevensbeheer een belangrijk uitgangspunt geweest bij het opstellen van Richtlijn 95/46/EG welke ten grondslag ligt aan de WBP. De beginselen van behoorlijke gegevensverwerking zijn in de WBP als volgt verwerkt:

- Gegevensverwerking dient in overeenstemming met de wet en behoorlijk en zorgvuldig te gebeuren (artikel 6 WBP).
- Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld (artikel 7 WBP).
- Er bestaat een rechtmatige grondslag voor het verzamelen van persoonsgegevens (art 8 WBP). Dit is het geval indien:

<sup>26</sup> De Artikel 29 Werkgroep is het gezaghebbende onafhankelijke adviesorgaan in Europa op het gebied van de bescherming van persoonsgegevens. De werkgroep dankt zijn naam aan het artikel in Richtlijn 95/46/EG waaronder zij is opgericht.

- a. Er ondubbelzinnige toestemming van de betrokkene is.
  - b. Gegevensverwerking noodzakelijk is voor het uitvoeren van een overeenkomst waarbij de betrokkene partij is.
  - c. Gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen.
  - d. Gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene.
  - e. Gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan.
  - f. Gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of degene aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.
- Persoonsgegevens worden niet verdere verwerkt op een wijze die onverenigbaar is met doeleinden van verkrijging (artikel 9 WBP).
  - Persoonsgegevens mogen slechts worden verwerkt indien zij met het oog op het doel van de verwerking toereikend, ter zake dienend en niet bovenmatig zijn (artikel 11 WBP).
  - Persoonsgegevens dienen met het oog op het doel van de verwerking juist en nauwkeurig te zijn (artikel 11 WBP).
  - Persoonsgegevens dienen te worden beveiligd (artikelen 12, 13 en 14 WBP).
  - Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor werkingsdoeleinden (artikel 10 WBP).

Verwerking van *gevoelige* persoonsgegevens is in principe niet toegestaan. In de wet worden uitzonderingen op dat verbod genoemd (artikelen 17 t/m 23 WBP). Zo is het bijvoorbeeld voor ziekenhuizen en hulpverleners wel toegestaan gegevens omtrent de gezondheid van een patiënt te verwerken en voor kerkgenootschappen om gegevens over personen die tot dat genootschap behoren te verwerken. De uitzondering die voor wat betreft RFID van belang is, is de "uitdrukkelijke toestemming van de betrokkene". Om te beoordelen of daarvan sprake is zijn de volgende drie punten van belang (Artz 1999, p. 16):

1. De betrokkene moet in alle vrijheid zijn wil met betrekking tot de gegevensverwerking kunnen uiten en deze wil moet daadwerkelijk geuit zijn. De betrokkene mag derhalve niet onder druk van de omstandigheden of de relatie met de verantwoordelijke, overgaan tot het geven van toestemming.
2. De wilsuiting moet betrekking hebben op een bepaalde gegevensverwerking of op een beperkte categorie van gegevensverwerkingen. Een zeer brede en onbepaalde machtiging tot het verwerken van gegevens is niet voldoende.
3. De betrokkene moet over de noodzakelijke informatie beschikken om tot toestemmingsverlening te kunnen komen. De betrokkene dient daarom voldoende en begrijpelijk door de verantwoordelijke te worden geïnformeerd over de verschillende aspecten van de gegevensverwerking die voor hem van belang zijn. Deze informatieplicht impliceert niet dat de betrokkene geen enkele verantwoordelijkheid draagt. Deze heeft ook zelf een zekere onderzoeksplicht voor hij toestemming verleent.

Bij de verwerking van persoonsgegevens is verder nog het volgende van belang: de betrokkene moet op de hoogte zijn van de geplande gegevensverwerking (artikelen 33 en 34 WBP) en zijn rechten moeten worden gerespecteerd (artikelen 35 t/m 42 WBP).

Informatieverstrekking aan de betrokkene houdt in dat:

- Indien de persoonsgegevens worden verkregen bij de betrokkene, dan moet deze vóór het moment van verkrijgen van persoonsgegevens informatie krijgen over de identiteit van de partij die zijn gegevens verwerkt en de doeleinden van de verwerking. Bovendien dient nadere informatie te worden verstrekt indien dat gezien de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat er van wordt gemaakt nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen (artikel 33 WBP).
- Indien de persoonsgegevens op een andere manier worden verkregen dan bij de betrokkene dient de bovenstaande informatie aan hem te worden medegedeeld op het moment van vastlegging van de gegevens of, wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste ver-

strekking. In het geval dit onmogelijk blijkt of een onevenredige inspanning kost, geldt deze informatieplicht niet. Wel dient de verwerker van persoonsgegevens dan de herkomst van de gegevens vast te leggen (artikel 34 WBP).

De rechten van de betrokkene zijn de volgende:

- Het transparantiebeginsel: de betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of zijn persoonsgegevens worden verwerkt. De verantwoordelijke dient binnen vier weken schriftelijk te antwoorden. In dat antwoord dient een volledig overzicht te staan in begrijpelijke vorm, een omschrijving van het doel of doeleinden, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers en de beschikbare informatie over de herkomst van de gegevens (artikel 35 WBP). De verantwoordelijke kan hiervoor een bij algemene maatregel van bestuur vast te stellen vergoeding vragen (artikel 39 WBP).
- Mogelijkheid tot correctie: de betrokkene mag de verantwoordelijke verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of doeleinden onvolledig of niet ter zake dienend zijn of anderszins in strijd met een wettelijk voorschrift worden verwerkt. De verantwoordelijke bericht binnen vier weken na ontvangst van het verzoek schriftelijk of en in hoeverre hij aan dat verzoek voldoet. Weigering dient met redenen omkleed te zijn (artikel 36 WBP).
- Indien een gewichtig belang van de verzoeker dit eist, kunnen de antwoorden bedoeld in artikel 35 en 36 WBP ook mondeling worden gegeven. (artikel 37 WBP).
- Wanneer de verantwoordelijke naar aanleiding van het verzoek van artikel 36 persoonsgegevens verbetert, aanvult, verwijdert of afschermt is hij verplicht om derden die hij de gegevens heeft verstrekt daarover in kennis te stellen, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost (artikel 38 WBP).
- Recht van verzet: indien er sprake is van verwerking van persoonsgegevens op basis van artikel 8 e en f WBP, kan de betrokkene bij de verantwoordelijke te allen tijde verzet aantekenen in verband

met zijn bijzondere persoonlijke omstandigheden. De verantwoordelijke kan voor het in behandeling nemen van het verzet een kostenvergoeding vragen, die niet hoger is dan een bij algemene maatregel van bestuur vast te stellen bedrag (artikel 40 WBP).

- Indien de gegevens worden verwerkt in verband met de totstandbrenging of instandhouding van een directe relatie tussen de verantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële en charitatieve doelen, kan de betrokkene daarentegen te allen tijde *kosteloos* verzet aantekenen. De verantwoordelijke dient de verwerking dan ook terstond te beëindigen. Wanneer de verantwoordelijke van plan is de gegevens aan derden te verstrekken, moet hij passende maatregelen nemen om de betrokkenen bekend te maken met het recht van verzet (bijvoorbeeld dag-, nieuws- of huis-aan-huisbladen). Bovendien moet de betrokkene in rechtstreekse boodschappen die aan hem worden toegezonden telkens gewezen worden op het recht van verzet (artikel 41 WBP).
- Niemand kan worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen worden genomen op grond van een geautomatiseerde verwerking van persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid, tenzij:
  - het besluit wordt genomen in het kader van het sluiten of uitvoeren van een overeenkomst en aan het verzoek van de betrokkene is voldaan of passende maatregelen zijn genomen ter bescherming van zijn gerechtvaardigd belang; óf
  - het besluit zijn grondslag vindt in een wet waarin maatregelen zijn vastgelegd die strekken tot de bescherming van het gerechtvaardigde belang van de betrokkene (artikel 42 WBP).

## 5.2 Richtlijn 2002/58/EG

Om de privacy in de elektronische communicatiesector te beschermen is in 2002 door het Europees Parlement en de Raad Richtlijn 2002/58/EG aangenomen (richtlijn betreffende de privacy en elektronische communicatie). Deze richtlijn is in mei 2004 in de Telecommunicatiewet (TW) geïmplementeerd. Richtlijn 2002/58/EG is de opvolger

van Richtlijn 97/66/EG welke hetzelfde beoogde als de huidige richtlijn.

Een aantal auteurs is van mening dat Richtlijn 2002/58/EG zonder meer van toepassing is op RFID-systemen, met name wanneer er sprake is van ongevraagde elektronische communicatie van commerciële aard of de verwerking van verkeers- of locatiegegevens.<sup>27</sup> De vraag is echter of dit wel het geval is, omdat het regulatief kader voor elektronische communicatienetwerken en -diensten voornamelijk gebaseerd is op de verhoudingen zoals die gelden in de telecommunicatiesector (vast, mobiel en internet). In deze sector is er over het algemeen sprake van een telecommunicatieaanbieder die een openbare telecommunicatiedienst aanbiedt welke afgenomen wordt door een abonnee. Wanneer we kijken naar de inrichting van RFID-systemen en dan met name naar het EPCglobal Network, dan zien we dat deze verhoudingen anders liggen.

Er is bij RFID-systemen geen sprake van een aanbieder in de zin van de Telecommunicatiewet, omdat individuele bedrijven hun eigen RFID-systemen zullen gaan gebruiken. Verder is er bij het gebruik van RFID in zijn algemeenheid geen sprake van (eind)gebruikers, abonnees of consumenten in de zin van de Telecommunicatiewet: de consument die met RFID geconfronteerd wordt is over het algemeen 'lijdend voorwerp' en maakt niet actief gebruik van RFID. Dit betekent in het kader van RFID dat in de meeste gevallen de bepalingen uit de Telecommunicatiewet niet van toepassing zijn. Een ander belangrijk punt is dat de definities van verkeers- en locatiegegevens zoals deze in Richtlijn 2002/58/EG worden gehanteerd wezenlijk verschillen van de data die in een RFID-systeem worden opgeslagen. Het is dan ook onduidelijk hoe de bepalingen uit Richtlijn 2002/58/EG in het kader van RFID zouden moeten worden toegepast daar er geen sprake is van abonnees of gebruikers.

In bijzondere gevallen waarbij RFID wordt gebruikt in combinatie met elektronische communicatiediensten kan evenwel niet worden uitgesloten dat bepalingen van de richtlijn (onder andere over locatiegegevens niet zijnde verkeersgegevens, zie artikel 11.5a TW) van toepassing kunnen zijn. Hierbij moet gedacht worden aan mobiele telefoons welke

uitgerust zijn met een RFID-tag en waarbij deze RFID-tag gebruikt wordt om de geografische positie van de mobiele telefoon te bepalen, waardoor location based services kunnen worden aangeboden. Het is echter in dit stadium nog te vroeg om daar een definitieve uitspraak over te doen.

---

27 Zie bijvoorbeeld: Natsui 2004 en Ustaran 2004

## 6 Analyse risico's RFID

In dit hoofdstuk wordt op basis van de informatie en conclusies uit de voorgaande hoofdstukken bekeken of het huidige wetgevende kader toereikend is voor de regulering van RFID, of dat aanvullende (zelf)regulering noodzakelijk is. Bij de beoordeling van het juridisch kader wordt gebruik gemaakt van scenario's om de abstracte dreigingen en toepasselijke regels beter in perspectief te plaatsen. Het bespreken van deze scenario's gebeurt in algemene termen en beperkt zich tot de meest in het oogspringende aspecten van RFID.

### 6.1 Scenario's

De in hoofdstuk 4 gesignaleerde risico's voor de privacy dienen per RFID-toepassing en systeem bekeken te worden, daarom is door de Werkgroep een aantal scenario's opgesteld. Aan de hand van deze scenario's kan beter beoordeeld worden in hoeverre de veronderstelde dreigingen van RFID realistisch zijn. De scenario's zijn ingedeeld naar type RFID-systeem en bevatten naast een standaard scenario ook varianten die met het oog op de privacy mogelijk gevoeliger liggen.

#### 6.1.1 RFID smart labels

RFID smart labels vormen de meest in het oog springende toepassing van RFID. Het gebruik van smart labels in met name de retail sector (op de *fast moving consumer goods*) vormt momenteel de grootste driver voor RFID. Naar verwachting zullen binnen de retail smart labels allereerst op het niveau returnable transport items (kratten, trolleys, containers en fusten) worden toegepast. In een later stadium zullen mogelijk ook individuele producten worden uitgerust met RFID. Het is met name deze laatste toepassing waar consumenten- en burgerrechtenorganisaties angstig voor zijn.

#### Scenario:

Binnen een logistieke keten wordt gebruik gemaakt van smart labels en het EPCglobal Network om returnable transport items en individuele producten te volgen binnen de logistieke keten. Nadat de fabrikant de tag heeft bevestigd op de producten gaan de producten naar de diverse distributiecentra. Bij binnenkomst van de vrachtwagens worden de tags uit-

gelezen. Op deze manier kan gecontroleerd worden of alle producten daadwerkelijk aanwezig zijn. De producten worden opgenomen in de voorraad die periodiek gescand wordt. Bij vertrek uit het distributiecentrum worden de tags opnieuw gelezen alvorens zij de vrachtwagen in gaan. Vanuit de distributiecentra worden de producten per vrachtwagen naar de supermarkt gebracht. Ook hier worden de producten bij binnenkomst gescand. In de supermarkt worden de producten in 'smart shelves' geplaatst. Het koopgedrag van de consument wordt *niet* vastgelegd door de RFID informatie te koppelen aan de consument via bijvoorbeeld een loyaltycard.

*Variant I: de door het RFID-systeem verkregen informatie wordt gebruikt om de prestaties van werknemers te monitoren.*

*Variant II: het gedrag van de consument wordt vastgelegd door de RFID-informatie te koppelen aan een loyaltycard die direct identificerende gegevens bevat.*

*Variant III: De winkel volgt de tags die de klant bij zich draagt in de winkel om zo een beter inzicht te krijgen in het winkelgedrag van de klant.*

*Variant IV: Iemand scant de codes van dure producten en gebruikt deze informatie om slachtoffers uit te kiezen voor een overval.*

Bij de toepassing van smart labels op het niveau van returnable transport items voorziet de Werkgroep Privacy & RFID geen risico's voor de privacy omdat deze returnable transport items niet de schappen (en daarmee de consument) bereiken en er dus geen (persoons)gegevens van de consument worden verwerkt.

Bij tagging met EPC smart labels op productniveau kan er eerder een risico ontstaan voor de privacy van de consument omdat de consument in dit scenario wél in contact komt met de RFID-tags maar, omdat er geen koppeling tot stand komt tussen consument en de EPC smart labels in het product blijven de risico's beperkt tot de situaties beschreven onder variant II en III.

#### *Variant I:*

In deze variant kan er sprake zijn van een inbreuk op de privacy van een werknemer, maar hierbij moet worden opgemerkt dat een dergelijke inbreuk onder bepaalde omstandigheden gerechtvaardigd kan zijn. In feite zullen hier dezelfde waarborgen en beperkingen moeten gelden als in het geval van (heimelijk) cameratoezicht, het monitoren van e-mailverkeer en het controleren van surfgedrag. Deze eisen zijn grofweg:

- Er dient sprake te zijn van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
- Er dient sprake te zijn van een gerechtvaardigd belang van de werkgever.
- Controlemaatregelen dienen beperkt te zijn en er dienen geen onnodige gegevens te worden vastgelegd.
- Er dient sprake te zijn van transparantie richting de werknemers.
- Tenslotte geldt natuurlijk de algemene eis van goed werkgeverschap.

#### *Variant II:*

In dit scenario is er sprake van het verwerken van persoonsgegevens, de eisen van de WBP zijn dan ook van toepassing. Wanneer die correct worden nageleefd, zal het privacyrisico voor de consument tot een minimum beperkt blijven. Belangrijk is dat de consument keuzevrijheid heeft (wel of geen loyalty-card; wel of niet actief laten van de EPC smart labels), goed geïnformeerd wordt over doel en aard van de verwerking, en dat de verwerker van persoonsgegevens zich aan de overige eisen uit de WBP houdt (goede beveiliging, niet langer bewaren dan noodzakelijk et cetera). De consument zou in dit scenario ook de mogelijkheid geboden moeten worden de EPC smart labels met behulp van een 'KILL commando' uit te schakelen (zie hoofdstuk 7).

Met betrekking tot de keuzevrijheid van de consument is nog enige toelichting op zijn plaats. De consument zal zich bij het maken van de keuze voor uitschakeling of verwijdering laten leiden door de voor- en nadelen die dit met zich meebrengt. Indien de nadelen van het uitschakelen niet opwegen tegen de voordelen van het actief laten, dan zal de consument de tag niet uitschakelen of verwijderen. Met andere woorden: als de voordelen van het actief laten van EPC smart labels groter zijn dan de wens van de consument om zijn privacy te beschermen, dan zal hij de

smart labels niet snel deactiveren. Om de afweging tussen actief laten of uitschakelen volledig in vrijheid te kunnen maken dienen gebruikers van RFID de consument niet onredelijk te bezwaren. Zo is het bijvoorbeeld niet wenselijk dat consumenten veel moeite moeten doen om de RFID-tag uit te schakelen, dat commerciële garantiebepalingen afhankelijk zijn van het actief laten van de RFID-tag, of dat deactivering ontmoedigd wordt door prijsstelling. Als er onvoldoende rekening wordt gehouden met privacybelangen van de betrokkene en/of er geen sprake is van een vrijelijke toestemmingsverlening, dan kan daarmee de grondslag van het verwerken van persoonsgegevens wegvallen. Verwerkingen die binnen de WBP vallen maar zonder grondslag zijn, zijn onrechtmatig.

Tot slot verdient het nog nadruk te vermelden dat het hier geen nieuwe situatie betreft die door de toepassing van RFID mogelijk wordt. Het in kaart brengen van koopgedrag is ook mogelijk met behulp van barcode scanning.

#### *Variant III:*

Dit is een verwerking van gegevens die naar mening van de Werkgroep anoniem en niet herleidbaar tot een persoon zou moeten plaatsvinden. Een bedrijf moet zich goed bewust zijn van het doel van het verzamelen van dit soort gegevens. In de meeste gevallen zal het bedrijf dergelijke informatie willen verzamelen met het oog op de ideale inrichting van een winkel. Met andere woorden: om een goed beeld te krijgen welke producten het beste lopen, hoe de inrichting van schappen moet zijn en hoe paden het best kunnen worden uitgezet. Deze toepassing kan geanonimiseerd verlopen en een bedrijf maakt het zichzelf een stuk makkelijker door geen persoonsgegevens te verwerken. Wanneer er voor een bedrijf toch gegronde redenen zijn de RFID-tags te koppelen aan identificeerbare personen, hoort het zich uiteraard aan de eisen uit de WBP te houden.

#### *Variant IV:*

In dit geval is er mogelijk sprake van het verwerken van persoonsgegevens, maar de WBP-waarborgen zullen in dit scenario van beperkte waarde zijn voor de betrokkenen. Dit probleem is dan ook veeleer een probleem van openbare orde en veiligheid dan van privacy. Toch ziet de Werkgroep hier wel een zekere maatschappelijke verantwoordelijkheid voor het bedrijfsleven. In het geval

van een duur, diefstalgevoelig product zouden bedrijven kunnen besluiten de RFID-tags altijd te 'killen' als een klant de winkel verlaat, of besluiten een wat duurdere RFID-tag te gebruiken die encryptie bevat.

#### 6.1.2 RFID Tokens & smart cards

Het gebruik van RFID in tokens, met name in contactloze smartcards, is sterk in opkomst. Door de toenemende behoefte aan veiligheid en risico management is er steeds meer behoefte aan toegangscontrole. Contactloze smartcards vormen een veilige en gebruiksvriendelijke methode om dit te faciliteren.

##### **Scenario 1:**

In het openbaar vervoer van een grote stad wordt gebruik gemaakt van contactloze smartcards. Door de kaart tegen een reader te houden bij vertrek en aankomst kan eenvoudig worden afgerekend. De kaart heeft een maximale leesafstand van enkele centimeters. De kaart bevat geen direct identificerende gegevens, en kan bij speciale laadpunten anoniem worden opgeladen. De kaart is niet gekoppeld aan een achterliggende database waarmee de gegevens herleid kunnen worden tot een identificeerbare persoon.

*Variant I: De kaart bevat enkel een uniek aboneenummer dat is gekoppeld aan een achterliggende database waar evenwel de RFID-gegevens via bijvoorbeeld het aboneenummer herleid kunnen worden tot een identificeerbare persoon.*

*Variant II: De kaart bevat direct identificerende gegevens. Deze zijn door middel van encryptie beschermd.*

In het hoofdsценario ziet de Werkgroep geen risico's voor de privacy, daar de toepassing volledig geanonimiseerd is en de RFID-gegevens niet herleidbaar zijn tot een identificeerbare persoon.

##### *Variant I:*

Bij de eerste variant dient allereerst opgemerkt te worden dat dit niet een RFID-specifieke toepassing betreft, maar dat dezelfde mogelijkheden bestaan bij gebruik van magneetstrips of barcodes. In deze variant is er sprake van de verwerking van persoonsgegevens en dus dienen de bepalingen uit de WBP te worden nageleefd.

##### *Variant II:*

Hier is sprake van de verwerking van persoonsgegevens en moet dus voldaan worden aan de eisen uit de WBP. Omdat er sprake is van een kaart die beschermd is door middel van encryptie is het risico op misbruik door derden tot een minimum beperkt. De Werkgroep is overigens wel van mening dat de reiziger de mogelijkheid geboden moet worden een anonieme kaart tegen een vergelijkbaar tarief aan te schaffen.

##### **Scenario 2:**

Een onderwijsinstelling gaat RFID gebruiken om de dienstverlening aan de scholier te verbeteren. De RFID-toepassing maakt het mogelijk voor scholieren om boeken te lenen, eten en drinken af te rekenen en zich eenvoudig in te schrijven voor tentamens met één scholierenkaart.

*Variant I: De RFID-toepassing wordt ook gebruikt om scholieren te volgen, hiervoor wordt de contactloze smartcard aangepast of aangevuld met een additioneel token (bijvoorbeeld een armband) waarmee spijbelgedrag gecontroleerd kan worden.*

*Variant II: Een stichting stelt voor om deze informatie te gebruiken om het effect van voorlichting te maximaliseren waar het gaat om de eetgewoonten van de scholieren.*

In het hoofdsценario is sprake van het verwerken van persoonsgegevens, de WBP is dan ook van toepassing. Er is geen bezwaar zolang wordt voldaan aan de criteria uit de WBP, de toepassing afdoende is beveiligd en de scholieren, waar mogelijk, niet tot een persoon herleidbare alternatieven worden geboden.

##### *Variant I:*

In dit scenario dient er een aantoonbare noodzaak te zijn voor de verwerking van de persoonsgegevens, bijvoorbeeld om excessief spijbelgedrag of te laat komen te signaleren. Aangezien de keuzevrijheid beperkt is (de scholier wordt waarschijnlijk de facto gedwongen het systeem te gebruiken), dient er goed gekeken te worden naar de noodzaak van het systeem alsmede naar de beveiliging van de toepassing. De ouders dienen ook bij het besluitvormingsproces betrokken

te worden, zeker als de scholieren minderjarig zijn. Dat de betrokkenheid van ouders en scholieren wenselijk is blijkt uit het geslaagde protest van ouders en kinderen tegen een school in Californië die RFID-tags voor scholieren verplicht wilde stellen.<sup>28</sup>

*Variant II:*

Waar de Werkgroep variant I nog als proportioneel ziet, wordt het bij deze variant twijfelachtig. Het volgen van eetgedrag van een scholier is niet direct een taak en verantwoordelijkheid van een school. Uiteraard speelt hier ook de inspraak van de ouders een belangrijke rol.

### 6.1.3 RFID-implantaten

Alhoewel voor de identificatie van personen tokens gebruikt kunnen worden bestaat ook de mogelijkheid om RFID-tags te laten implanteren. Het implanteren van RFID-tags wordt reeds gedaan of overwogen in het uitgaansleven, de medische wereld en het gevangeniswezen.

**Scenario 1:**

In een populaire nachtclub kunnen gasten een RFID-chip laten implanteren. Het gaat om chips van elf millimeter die ingebracht worden in het vetweefsel onder de rechter triceps. Draggers van de chip hebben toegang tot extra privileges zoals gratis toegang tot de club en het VIP-deck, versnelde entree bij de deur en de mogelijkheid om drank af te rekenen. De maximale leesafstand bedraagt één meter en de informatie over de klant is opgeslagen in een achterliggende database.

*Variant I: de over de VIP-leden verzamelde informatie wordt ook gebruikt voor persoonsgerichte reclame.*

In het hoofdsenario is zeker sprake van de verwerking van persoonsgegevens, dus is de WBP van toepassing. Indien de klant echter ondubbelzinnige toestemming voor het implanteren van de chip heeft gegeven, bestaat er een grondslag voor de verwerking conform artikel 8 WBP en bestaat hiertegen dus niet noodzakelijkerwijs een bezwaar. Wel moet aandacht worden besteed aan in hoeverre het nog goed mogelijk is die toestem-

ming in te trekken (dient de chip dan operationeel verwijderd te worden?) en invulling valt te geven aan het recht van verzet.

*Variant I:*

Hierbij is weer van belang: heeft de klant hiervoor zijn ondubbelzinnige toestemming gegeven? Als dat het geval is, bestaat er geen bezwaar tegen deze toepassing.

**Scenario 2:**

In een ziekenhuis worden patiënten met een tag geïmplanteerd. Doel van de implantaten is ziekenhuispersoneel sneller toegang te verschaffen tot medische dossiers en patiënten beter en gemakkelijker te identificeren. De informatie over patiënten ligt niet opgeslagen op de tag zelf maar in een achterliggende database.

*Variant I: De gegevens van de patiënt liggen opgeslagen in de tag.*

*Variant II: Nederlanders kunnen zich vrijwillig uit laten rusten met een tag. Op deze tag staat hun sofi-nummer. Dit sofi-nummer kan gekoppeld worden aan een achterliggende database met medische gegevens en DNA. Zo kan bij een ongeluk snel informatie over de patiënt worden opgevraagd. Mensen die zich laten taggen krijgen een korting op hun ziekenfondspremie.*

De Werkgroep staat negatief tegenover alle toepassingen die in dit scenario zijn geschetst. Zij is van mening dat het effect van een armbandje of anderszins door de patiënt uitwendig te dragen chip niet dusdanig zal verschillen met het effect van een implantaat, dat het de aantasting van de lichamelijke integriteit rechtvaardigt. Uiteraard dient de uiteindelijke beslissing hierover (in samenspraak met de behandelend arts) bij de patiënt te liggen.

Uiteraard zal ook in het geval van een uitwendig gedragen tag sprake zijn van persoonsgegevens en zal de WBP moeten worden nageleefd. Met name de WBP-bepalingen omtrent bijzondere gegevens (waar medische gegevens onder vallen) zijn dan van belang.

28 <<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/02/16/financial/f075453S34.DTL>>

#### *Variant II:*

Voor wat betreft variant II wordt daar nog aan toegevoegd dat voor gebruik van het sofnummer een apart artikel in de WBP is opgenomen, artikel 24 WBP. Dit artikel bepaalt dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, slechts gebruikt mag worden ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. Dit betekent dat het sofnummer voor de toepassing die hier is geschetst niet mag worden gebruikt.

#### *6.1.4 Overige Systemen*

De restcategorie 'overige systemen' omvat al die RFID-systemen die niet onder een van de andere categorieën te scharen vallen. Het is lastig om aan deze categorie scenario's te koppelen omdat deze categorie zo groot en divers is. Er is daarom gekozen voor twee realistische scenario's die nu reeds worden toegepast c.q. in de planning liggen.

#### **Scenario 1:**

In een bibliotheek wordt een RFID-systeem gebruikt om boeken te taggen. De tag bevat enkel een uniek nummer dat verwijst naar een titel die opgenomen is in een aparte database. Het leengedrag kan op deze manier eenvoudig worden gekoppeld aan de bibliotheekgangers.

*Variant I: de tag bevat wél informatie over het boek welke met een reader kan worden uitgelezen.*

In dit scenario vindt verwerking van persoonsgegevens plaats, dus de WBP is van toepassing. Omdat informatie over het leesgedrag van bibliotheekgangers onder bepaalde omstandigheden de verwerking van bijzondere persoonsgegevens met zich mee kan brengen dient zorgvuldig omgesprongen te worden met deze informatie. Dit is echter niet een RFID gerelateerd onderwerp, maar heeft eerder betrekking op de algemene omgang met dergelijke informatie in de back-office (databases) van de bibliotheek.

#### *Variant I:*

In dit scenario bestaat er naast de mogelijkheid voor de bibliotheek om tags uit te lezen, ook de kans dat onbevoegde derden de tags uitlezen. Voor de werking van dit systeem is het 'killen' of anderszins uitschakelen van tags niet echt een optie, omdat dit de wer-

king van het systeem tenietdoet. Vanwege het feit dat de consument niet de keuze heeft de tag te 'killen', moeten er voldoende waarborgen in het systeem worden ingebouwd om ongeautoriseerd uitlezen door derden te voorkomen. Indien de tag informatie over de inhoud van het boek bevat zoals de titel, de schrijver, en/of het ISBN nummer, dan dient de tag beschermd te worden met behulp van encryptie. Gezien het feit dat de tag meerdere malen gebruikt kan worden lijkt dit de investering in een duurder tag te rechtvaardigen (zie hoofdstuk 7).

#### **Scenario 2:**

Auto's worden uitgerust met een passieve tag die functioneert als een digitaal nummerbord. De tag kan van vijf meter uitgelezen kunnen worden, zelfs bij een snelheid van 200 kilometer per uur. De tags kunnen gebruikt worden voor zaken als snelheidscontroles, tolheffing en parkeren.

*Variant I: Tankstations willen dit systeem gebruiken om 'wegrijden zonder te betalen' te voorkomen / bestrijden.*

Het probleem bij dit scenario (en de variant daarop) is de breedte van toepassingsmogelijkheden die zich zowel in het publieke als private domein bevinden en de verschillende bijbehorende verwerkingsgrondslagen. Een probleem dat zich hier kan gaan voordoen is het probleem van het hellend vlak: de ene toepassing ontlokt de andere toepassing. Het is juist om deze reden van het grootste belang dat bij RFID-systemen met brede toepassingsmogelijkheden altijd de juiste verwerkingsgrondslag wordt gehanteerd en gelet wordt op de doelbinding.

## **6.2 Veronderstelde risico's geanalyseerd**

Met de informatie verkregen uit de scenario's kunnen we nu bekijken hoe groot de risico's zijn van RFID voor de privacy, met andere woorden wat de kans op een inbreuk op de privacy is en hoe zwaar de gevolgen van de desbetreffende inbreuk zouden zijn.

### *6.2.1 Het op afstand heimelijk uitlezen van tags door readers*

De kans dat RFID-tags op afstand worden uitgelezen zonder dat de burger hier weten-

schap van heeft is aanwezig en vormt daarmee een potentieel risico voor de privacy. De gekozen RFID-technologie (met andere woorden het type RFID-tag) speelt bij dit vraagstuk een grote rol, omdat de gekozen technologie zaken zoals de maximale leesafstand en beveiligingsmogelijkheden van de tag bepaalt.

Het risico op een inbreuk op de privacy is het grootst wanneer de RFID-gegevens worden gekoppeld aan een geïdentificeerde of identificeerbare natuurlijke persoon. Omdat in dit geval de WBP van toepassing is, worden de privacyrisico's (in wettelijke zin) grotendeels ondervangen. Het blijft uiteraard wel de vraag in hoeverre invulling gegeven kan worden aan de handhaving van de WBP en andere regels omtrent de privacy en individuele vrijheid van de burger.

Maar ook wanneer er geen persoonsgegevens worden verwerkt, kan er afhankelijk van de toepassing, sprake zijn van een daadwerkelijk inbreuk op de privacy van de burger, of de privacybeleving van de burger. Om deze reden is kennisgeving en een algemene houding van openheid richting de consument omtrent de aanwezigheid van tags en readers van belang. Uit een analyse van wet- en regelgevende initiatieven op het gebied van RFID blijkt ook dat kennisgeving (met andere woorden duidelijkheid over waar, wat, hoe en waarom gescand wordt) wereldwijd gezien wordt als een belangrijke eis die aan RFID-toepassers wordt gesteld.

#### *6.2.2 Traceability door unieke identificatie*

Het vraagstuk over traceability (volgbaarheid) valt uiteen in twee segmenten: *de volgbaarheid in de publieke ruimte* (de angst dat door RFID personen overal volgbaar zijn) en *de volgbaarheid binnen een bepaald systeem* (de angst dat door RFID personen volgbaar zijn binnen een bepaalde omgeving). Deze twee risico's zullen afzonderlijk geanalyseerd worden.

##### *Volgbaarheid in de publieke ruimte*

Het is technisch mogelijk om de route die RFID-tags afleggen binnen een bepaalde keten of systeem te volgen. Indien een RFID-tag meegedragen wordt door een persoon, dan kan deze persoon in theorie dus ook gevolgd worden aan de hand van de tags die hij bij zich draagt. Een fijnmazig systeem van readers en achterliggende middleware kan in theorie de volgbaarheid van mensen bewerk-

stelligen. Een andere mogelijkheid is het plaatsen van RFID-readers op strategische knoep- c.q. knelpunten waar veel mensen langs (moeten) komen. Voorbeelden zijn ingangen van gebouwen, liften en trappen.

Het is echter maar zeer de vraag of dergelijke (fijnmazige) systemen gerealiseerd kunnen en zullen worden in de publieke ruimte. Het lijkt de Werkgroep zeer onwaarschijnlijk dat private ondernemingen alleen of in samenwerking met elkaar een dergelijk alomvattend volgsysteem gaan aanleggen voor commerciële doeleinden. Afgezien van de technische beperkingen en hoge kosten die een fijnmazig systeem van readers met zich meebrengt, zou een dergelijk systeem ook niet de toets van de WBP doorstaan. De kans dat een surveillancesysteem met een aanzienlijk dekkinggraad in de publieke ruimte door private partijen wordt aangelegd lijkt dus verwaarloosbaar klein.

Dit kan anders liggen als het de overheid is die personen wil volgen, bijvoorbeeld met het oog op de handhaving van de openbare orde of nationale veiligheid. In dat geval kan de overheid zelf een dergelijk RFID-systeem aanleggen of zichzelf toegang verschaffen tot individuele private RFID-surveillance-infrastructuren. Deze situatie is niet ondenkbaar, hoewel de maatschappelijke acceptatie van een dergelijk systeem naar verwachting erg laag zal zijn vanwege het hoge 'Big Brother' gehalte. Deze situatie is evenwel niet zozeer een RFID-specifiek probleem, maar dient in de bredere context van het debat over veiligheid, privacy en individuele vrijheid gevoerd te worden.

Uiteraard kunnen ook slechts beperkte delen van de publieke ruimte (een straat, een plein, een station) door middel van een RFID-systeem in de gaten gehouden worden. Een antwoord op de toelaatbaarheid van dergelijke toepassingen past ook binnen de bredere context van het debat over veiligheid, privacy en individuele vrijheid.

##### *Volgbaarheid binnen gesloten systemen*

Volgbaarheid binnen gesloten systeem zoals een winkel, school, of kantoor is geenszins ondenkbaar. Het is met de huidige stand van de techniek goed mogelijk om in een redelijk gesloten omgeving een RFID surveillance systeem te installeren met een afdoende dekkinggraad. Volgbaarheid van de burger/consument/werknemer in een gesloten systeem

kan een inbreuk vormen op de privacy en/of individuele vrijheid, zeker als dit heimelijk geschiedt.

De Werkgroep pleit daarom in het algemeen voor het betrachten van terughoudendheid bij de implementatie van dergelijke systemen. Het zal uiteindelijk aan de concrete toepassing, de doeleinden, en de context waarbinnen het RFID-surveillancesysteem gebruikt wordt liggen of er sprake is van een risico voor de privacy en/of individuele vrijheid van de burger, consument, of werknemer. Het is moeilijk om daar algemene uitspraken over te doen. Het gebruik van RFID-surveillancesystemen zal in ieder geval altijd aan de WBP getoetst dienen te worden indien met dergelijke systemen persoonsgegevens worden verwerkt.

Naar het zich laat aanzien zijn de meest waarschijnlijke toepassingen van RFID-surveillancesystemen binnen gesloten (private) omgevingen: *het analyseren van gedrag, het monitoren van werknemers, en het beveiligen van personeel en eigendommen.*

Voor het *analyseren van gedrag* geldt dat daar waar bedrijven of organisaties RFID willen toepassen om een beter inzicht te krijgen in het gedrag van hun doelgroep zij dit geanonimiseerd dienen te doen. Indien toch persoonlijke profielen aangemaakt worden, dan dient dit met wetenschap en toestemming van de klant te gebeuren en in overeenstemming van de WBP.

Voor het *monitoren van werknemers* kan aansluiting worden gezocht bij de huidige regels omtrent toezicht op werknemers welke grofweg zijn:

- Er dient sprake te zijn van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
- Er dient sprake te zijn van een gerechtvaardigd belang van de werkgever.
- Controlemaatregelen dienen beperkt te zijn en er dienen geen onnodige gegevens te worden vastgelegd.
- Er dient sprake te zijn van transparantie richting de werknemers.
- Tenslotte geldt natuurlijk de algemene eis van goed werkgeverschap.

Voor het *beveiligen van personeel en eigendommen* kan wellicht aansluiting worden gezocht bij de regels die gelden voor het gebruik van camera's in winkels.<sup>29</sup> In principe is dit toegestaan zolang de klant van het cameratoezicht op de hoogte is gebracht. Gebeurt dit niet, dan is de winkelier strafbaar. Dit zou naar analogie ook voor RFID-surveillancesystemen kunnen gelden. Uiteraard dient het belang van de winkelier afgewogen te worden tegen het recht op privacy van de klant en moet gekeken worden of minder ingrijpende middelen niet hetzelfde resultaat kunnen bewerkstelligen.

De Werkgroep Privacy & RFID pleit voor nader onderzoek en (sector)specifieke regels voor de toepassing van RFID-surveillancesystemen.

### 6.2.3 Data aggregatie en profiling

Data aggregatie en profiling zijn middelen die nu reeds worden toegepast. Met de komst van RFID wordt de mogelijkheid tot het verzamelen van gegevens aanzienlijk groter en eenvoudiger. Indien profielen meer accuraat worden vergroot dit de mogelijkheden tot het identificeren, waardoor privacy-inbreuken kunnen ontstaan. Dit is uiteraard een omstandigheid waar rekening mee gehouden dient te worden bij de toepassing.

Bedrijven bewijzen hun klanten en zichzelf een grote dienst door gegevens waar mogelijk anoniem te verwerken. Indien het toch noodzakelijk is voor de bedrijfsvoering om profielen te maken van geïdentificeerde of identificeerbare personen, is de WBP van toepassing. Dit betekent onder meer dat er altijd een grondslag voor de verwerking moet zijn, zoals toestemming van de consument. Het risico op inbreuk op de privacy wordt dan ook grotendeels ondervangen door een goede handhaving van de WBP.

### 6.2.4 Taggen van mensen

Het taggen van mensen brengt aanzienlijke privacyrisico's met zich mee. Met name het plaatsen van een tag in het menselijk lichaam vormt een aanzienlijke privacyinbreuk en is daarnaast een aantasting van de lichamelijke integriteit. Met het taggen van mensen dient dus zeer zorgvuldig om te worden gegaan.

Het spreekt voor zich dat een individu toestemming moet geven voor het bevestigen

van een tag op, of het plaatsen van een tag in zijn lichaam. Voor hij zijn toestemming geeft dient hij goed geïnformeerd te worden en moet ook aan de andere bepalingen uit de WBP worden voldaan. Ook hier geldt weer dat het privacyrisico ondervangen kan worden wanneer de WBP goed wordt nageleefd.

Bij een tag die op het lichaam gedragen wordt in plaats van in het lichaam, is het mogelijke privacyrisico afhankelijk van de toepassing. Een armbandje dat consumenten moeten dragen bij het bezoeken van een concert in verband met toegangscontrole en na afloop weer af kunnen doen, is natuurlijk iets heel anders dan een armbandje met medische gegevens dat iemand continu dient te dragen. Ook hier speelt de wil c.q. toestemming van de consument, burger, patiënt et cetera uiteraard een belangrijke rol.

Bij het taggen van mensen dient de beveiliging van de RFID-tag prioriteit te hebben, zeker als deze persoonsgegevens bevat. De Werkgroep acht het bijzonder onverstandig om (zeker bij implantaten) toepassingen die samenhangen met het taggen van mensen een RFID-tag te nemen zonder een afdoende hoog beveiligingsniveau.

#### *6.2.5 Illegaal gebruik*

Misbruik van technologische vooruitgang door kwaadwillenden is een niet uitsluitbaar risico in iedere maatschappij. Zo is het bijvoorbeeld mogelijk dat een potentiële overvaller aan de hand van de tags die een persoon bij zich draagt een beter inzicht kan krijgen in de producten die deze persoon bij zich heeft. Dit is echter niet zozeer een privacyprobleem maar eerder een probleem van openbare orde en veiligheid.

Ook is het, zoals reeds in paragraaf 6.2.3 is aangehaald, mogelijk om in strijd met de bepalingen uit de WBP omvangrijke gepersonaliseerde profielen aan te leggen. Dit probleem dient onder andere door middel van verscherpte handhaving geadresseerd te worden.

Voor elk mogelijk misbruikscenario met betrekking tot nieuwe technologie geldt dat de maatschappij een afweging moet maken tussen de voordelen van de technologie enerzijds en de negatieve aspecten (mogelijk misbruik) die daar tegenover staan anderzijds. Dit geldt ook voor RFID, het is daarom verstandig nader onderzoek te doen naar de mogelijk-

heden die RFID-toepassingen bieden tot misbruik. Al naar gelang het risico dient gezocht te worden naar effectieve methoden om misbruik te voorkomen dan wel tegen te gaan.

#### *6.2.6 Systeemintegratie*

De analyse van het risico van systeemintegratie hangt nauw samen met de analyse van het probleem van traceability (volgbaarheid) door unieke identificatie. Systeemintegratie bevat echter een belangrijk aanvullend privacyrisico: de effectiviteit van een geïntegreerd surveillancesysteem opgebouwd uit diverse surveillance-infrastructuren (bijvoorbeeld het koppelen van RFID-systemen aan CCTV-systemen en GPS-systemen) is vele malen groter dan een enkelvoudige surveillance-infrastructuur zoals een RFID-systeem. Bij het probleem van systeemintegratie kan wederom een onderscheid worden gemaakt tussen de publieke ruimte en gesloten systemen.

#### *Systeemintegratie in de publieke ruimte*

Het risico op een vergaande systeemintegratie wordt in de private sector naast technische en organisatorische belemmeringen ondervangen door de bepalingen uit de WBP. Zoals reeds aangegeven in paragraaf 6.2.2 lijkt de inrichting van een fijnmazige surveillance-infrastructuur in de publieke ruimte ter behartiging van een privaat belang onrealistisch.

Uiteraard kan de overheid wel met het oog op de handhaving van de openbare orde, de bescherming van de nationale veiligheid en het opsporen van strafbare feiten bepaalde surveillance-infrastructuren inrichten. De volgbaarheid van personen in de publieke ruimte als gevolg van systeemintegratie blijft daarom een punt van aandacht dat in nader onderzoek en maatschappelijk debat geadresseerd dient te worden.

#### *Systeemintegratie binnen gesloten systemen*

Bij systeemintegratie binnen gesloten systemen geldt hetzelfde als voor de toepassing van een enkelvoudig surveillancesysteem zoals cameratoezicht of controle op emailverkeer (zie paragraaf 6.2.2). De toepasser dient er rekening mee te houden dat gezien de combinatie van verschillende surveillance-infrastructuren het risico op een inbreuk op de privacy en/of individuele vrijheid van de burger groter is dan bij een enkelvoudig surveillancesysteem, hetgeen betekent dat aanvullende zorgvuldigheid en terughoudendheid gepast is.

### **6.3 Toereikendheid bestaande wet- en regelgeving**

Door haar techniekafhankelijke redactie is de WBP volledig van toepassing op het verwerken van persoonsgegevens met behulp van RFID-systemen. De analyse van de wet- en regelgeving aan de hand van de scenario's wijst verder uit dat het huidige wettelijk kader toereikend is en er momenteel in Nederland geen reden is om te streven naar RFID-specifieke wetgeving.

Een vraag die verder rijst is de concrete invulling van de wetgeving in de dagelijkse praktijk van een RFID-systeem. Er moet nadere invulling gegeven worden aan de abstracte bepalingen uit de WBP wil de wet nageleefd kunnen worden door de toepassers van RFID.

Uit de bespreking van de scenario's komt naar voren dat mogelijke risico's voor de privacy voortvloeien uit *het onbewust niet naleven van de WBP of het misbruik van RFID-toepassingen*.

#### *Het onbewust niet naleven van de WBP*

Bij deze categorie zal het met name gaan om het onbewust onverantwoord toepassen van RFID binnen een organisatie. Hieronder valt bijvoorbeeld het niet treffen van afdoende beveiligingsmaatregelen, het niet informeren van de betrokkene, of het handelen in strijd met de doelbinding. Er zal per toepassing gekeken moeten worden of het gebruik van RFID in overeenstemming is met de bepalingen uit de wet. Hiervoor kunnen naast eventuele sectorspecifieke RFID-eisen de bestaande toetsingsmechanismen worden gebruikt. Uiteindelijk zal in de praktijk moeten blijken welke toepassingen wel en welke toepassingen niet door de beugel kunnen. De keuze en acceptatie van de consument zullen bij deze beslissing ook meewegen.

Om het probleem van het onbewust niet naleven van de WBP te adresseren dienen de mogelijke toepassers van RFID-technologie op de hoogte te worden gebracht van de regels uit de WBP, eventuele (nog op te stellen) sectorspecifieke gedragsregels, alsmede van de technische mogelijkheden en onmogelijkheden van RFID. Alleen met deze informatie zullen mogelijke toepassers in staat zijn een genuanceerde keuze te maken met betrekking tot de implementatie van RFID in hun bedrijfsvoering. Hier ligt duidelijk een

gezamenlijke taak voor de markt (met name de aanbieders) en de overheid.

#### *Het misbruik van RFID-toepassingen*

Onder deze categorie valt onder andere het bewust handelen in strijd met de WBP, het ongeautoriseerd lezen van RFID-tags, het manipuleren van RFID-gegevens, en het inbreken in geautomatiseerde werken die persoonsgegevens bevatten. De toekomst zal moeten uitwijzen hoe groot het gevaar is van misbruik. Het lijkt onverstandig in dit stadium reeds bepaalde RFID-toepassingen op voorhand te verbieden met het oog op mogelijk misbruik.

Uiteindelijk is het met het oog op RFID niet zozeer een kwestie van het verder versterken van het recht op privacy door middel van formele wetgeving, maar veeleer het ontwikkelen van mechanismen die onverantwoord gebruik helpen voorkomen alsmede maatregelen die misbruik helpen bestrijden. Met name in het geval van misbruik zijn de mogelijke risico's voor inbreuken op de privacy, maar ook de persoonlijke veiligheid, aanwezig en de gevolgen voor de betrokkenen potentieel ernstig. Het is dus zaak om in de nabije toekomst aanvullend onderzoek te doen naar de mogelijkheden tot misbruik en de manieren om dit te voorkomen.

## 7 Technische voorzieningen

Tijdens het bespreken van de scenario's en de bijbehorende risicoanalyse is een aantal malen het belang van beveiliging en de vrije keuze van de consument aan de orde gekomen. Deze en andere vereisten kunnen weliswaar in wet- en regelgeving worden vastgelegd, maar voor de uiteindelijke invulling zijn daarenboven organisatorische en technische voorzieningen noodzakelijk. Met name de technische voorzieningen zullen in de nabije toekomst een belangrijke rol gaan spelen daar zij invulling kunnen geven aan de bepalingen uit wet- en regelgeving en de consument een hogere mate van controle over zijn persoonsgegevens kunnen geven, bijvoorbeeld door te voorkomen dat RFID-tags uitgelezen kunnen worden. Hieronder staan de belangrijkste technische voorzieningen opgesomd.

### 7.1.1 RFID-detectie

Het radiosignaal dat RFID-lezers uitzenden kan worden opgevangen door radioapparatuur die op dezelfde frequentie opereert. Het is dus in principe mogelijk om 'RFID-reader-detectoren' te bouwen die de aanwezigheid van een RFID-reader kunnen waarnemen.<sup>30</sup> Dergelijke apparaten zouden meer duidelijkheid verschaffen aan de consument over de vraag waar en wanneer hun RFID-tags worden uitgelezen, hetgeen de transparantie verhoogt.

### 7.1.2 Kooi van Faraday

Een eerste technische voorziening die de werking van RFID-systemen verhindert is de zogenaamde 'Kooi van Faraday'. Door het creëren van een barrière die radiostraling tegenhoudt kan het uitlezen van RFID-tags voorkomen worden. Het plaatsen van RFID-tags in een metalen kooi (bijvoorbeeld een boodschappentas met een voering van aluminiumfolie) is hiervoor een methode. Deze lowtech oplossing stuit echter op praktische bezwaren: het is immers niet mogelijk om een persoon non-stop te hullen in een Kooi van Faraday.

### 7.1.3 Verwijderen antenne

Een tweede voorziening die het ongeautoriseerd uitlezen van RFID-tags tegengaat is het verwijderen van de antenne. Op deze manier

kan de RFID-tag geen signaal meer ontvangen of uitzenden. Deze oplossing stuit op twee praktische bezwaren: 1) het is veelal niet mogelijk om de tag te lokaliseren omdat deze verwerkt is in bijvoorbeeld verpakkingen of kleding, 2) de functionaliteit van de tag wordt voor altijd tenietgedaan. Met name dit laatste bezwaar is met het oog op diefstalpreventie en after sales services uiteraard bijzonder relevant.

### 7.1.4 Encryptie

De belangrijkste technische voorziening is ongetwijfeld encryptie. Met behulp van encryptie kan voorkomen worden dat onbevoegde derden toegang krijgen tot informatie die is vastgelegd in de RFID-tag. Dit is van belang omdat RFID-tags zich over het algemeen automatisch laten uitlezen als zij binnen het stralingsveld van een reader komen.<sup>31</sup> Zonder encryptie geeft een RFID-tag dus in principe altijd informatie bloot, ook aan 'onbevoegde' readers. Er is dus geen sprake van authenticatie tussen reader en tag. Door een RFID-tag van encryptie te voorzien kan er gezorgd worden voor reader-tag authenticatie waardoor het mogelijk wordt gemaakt de tag alleen uit te lezen op die plaatsen waar dit noodzakelijk en toegestaan is.

Belangrijkste nadeel van encryptie is het feit dat de prijs van de RFID-tag een stuk hoger wordt, omdat de chip 'intelligenter' moet worden gemaakt. Dit betekent dat encryptie voor veel toepassingen (waaronder het gebruik in de detailhandel) vanuit kostenoverwegingen veelal geen optie is. Daar waar persoonsgegevens op de RFID-tag vastgelegd worden, zoals in de gezondheidszorg, het openbaar vervoer, en het gebruik van RFID in paspoorten, is encryptie uiteraard wel een noodzakelijkheid. Gelukkig speelt hier het kostenargument een minder grote rol omdat de tags een langere levensduur hebben.

### 7.1.5 KILL Commando

In de EPCglobal specificaties is een zogenaamd 'KILL' commando opgenomen voor smart labels. Omdat smart labels gezien het toepassingsgebied (dat met name in de *fast moving consumer goods* sector ligt) een geringe prijs moeten hebben is er vanuit kostenoverwegingen geen ruimte voor encryptie

30 Zo zijn er bijvoorbeeld apparaatjes die de aanwezigheid van een draadloos netwerk kunnen detecteren.

31 Hierbij past de kanttekening dat indien readers en tags niet werken op basis van dezelfde frequenties of protocollen, of geen gebruik maken van dezelfde dataformaten, het uitlezen niet automatisch mogelijk is.

op de RFID-tag. Het alternatief is dan om als de RFID-tag de winkel verlaat deze voorgoed uit te schakelen door middel van het commando KILL. Wanneer het KILL commando wordt gegeven aan een tag, dan zal deze permanent niet meer reageren op signalen van readers. Met andere woorden, de chip vernietigt zichzelf, weliswaar niet fysiek, maar wel softwarematig. Om van deze mogelijkheid gebruik te maken dienen consumenten hun producten door speciale apparatuur te laten scannen.

Probleem bij het uitschakelen van tags is dat het aanbieden van value added diensten en after sales services (zoals het automatisch opzoeken van de bereidingswijze van een kant en klaar maaltijd, of de eenvoudige afhandeling van garantie) bemoeilijkt wordt. Hoewel het KILL commando een waardevol instrument is voor de bescherming van de privacy in het kader van RFID bestaat er bij tegenstanders van RFID nog wel enige scepsis over de toegevoegde waarde van de 'KILL switch'. De voornaamste bezwaren zijn:

- De KILL switch adresseert niet het vraagstuk van volgbaarheid binnen een gesloten omgeving zoals een winkel.
- Bedrijven kunnen het uitschakelen van de tag onaantrekkelijk maken voor de consument door prijsdifferentiatie, of door niet te voorkomen dat er bij het uitschakelen wachtrijen ontstaan.

Een ander probleem betreft het feit dat het niet altijd mogelijk is om tags uit te schakelen omdat dit de werking van het RFID-systeem zou frustreren. Een goed voorbeeld is het gebruik van RFID in bibliotheekboeken. Hier is het uiteraard niet de bedoeling dat de RFID-tag gekilled wordt, omdat het gebruiken van het KILL commando de werking van het systeem tenietdoet.

#### *7.1.6 RFID Deep Sleep mode*

Een aan het KILL commando gerelateerde methode om tags onleesbaar te maken is de 'deep sleep mode'. Wanneer een RFID-tag in deep sleep mode wordt gebracht gaat deze als het ware in een 'standby' modus: alle activiteit van de RFID-tag wordt gestaakt en alleen de mogelijkheid om weer te ontwaken blijft als functionaliteit over. Een reader zou in dit geval een speciaal 'ontwaak commando' moeten geven waardoor de tag weer ontwaakt. Omdat de RFID-tag in het geval van een deep sleep commando in tegenstelling

tot een KILL commando niet blijvend onklaar gemaakt wordt, biedt het meer mogelijkheden voor consumenten om zelf te bepalen waar en wanneer zij hun RFID-tags actief willen maken.

Hoewel de deep sleep mode als methode veelbelovend klinkt dient wel nader onderzoek naar deze mogelijkheid verricht te worden omdat vooralsnog weinig bekend is over de deep sleep mode en de werkbaarheid ervan.

#### *7.1.7 RFID Blocker tags*

RSA ontwikkelt momenteel een tag, de blocker tag, waarmee voorkomen kan worden dat readers RFID-tags in de nabijheid van de blocker tag kunnen lezen (Juels 2004). De blocker tag misleidt de reader door een vals signaal uit te zenden waardoor het lijkt of er een enorm groot aantal EPC's aanwezig is (2 tot de macht 64 in de simpelste systemen). Hiermee worden niet geautoriseerde readers als het ware 'gespammed' met een overvloed aan EPC's die de EPC's van de echte tags maskeren. Omdat de blocker tags selectief kunnen worden gemaakt hoeven zij geen bedreiging te vormen voor de normale werking van RFID-systemen.

#### *7.1.8 Informatiefiltering*

Hoewel readers grote hoeveelheden informatie kunnen verzamelen over RFID-tags en de omgeving waarin deze zich bevinden, bestaat niet altijd de noodzaak tot het verwerken en opslaan van al deze data. Om deze reden is (in het EPCglobal Network althans) de mogelijkheid tot het filteren van data in het leven geroepen. De mogelijkheid tot het filteren van RFID data wordt voornamelijk gebruikt om de enorme stroom aan data enigszins in te dammen, maar het is natuurlijk ook denkbaar om zogenaamde 'privacyfilters' in te bouwen. De mogelijkheden voor dergelijke filtering dienen nader onderzocht te worden.

## 8 Conclusies

RFID is een technologie die van wezenlijke invloed gaat zijn op de Nederlandse maatschappij en economie. Bij de toepassing van nagenoeg alle technologieën die grote gevolgen hebben voor de maatschappij ontstaan er vragen omtrent mogelijke negatieve effecten. Dit gold voor de boekdrukkunst (angst voor verschuiving van de machtsbalans), de stoommachine (angst voor verdwijnen van menselijke arbeid), de trein (angst voor invloed op de landbouw en veeteelt), en de auto (angst voor dodelijke ongelukken). Voor RFID is dit niet anders. Hoewel een groot-schalige toepassing van RFID nog net achter de horizon ligt bestaan er nu reeds zorgen over het effect dat RFID heeft op de privacy en de individuele vrijheid van de burger. Dergelijke zorgen komen natuurlijk niet uit de lucht vallen, maar vloeien voort uit de specifieke kenmerken van RFID die bij onverantwoord gebruik of misbruik de mogelijkheid tot inbreuken op de privacy van de burger openen.

Het wettelijk kader voor de bescherming van de (informationele) privacy zoals vastgelegd in de WBP is volledig van toepassing op RFID-systemen waarmee persoonsgegevens worden verwerkt. Dit betekent dat RFID-toepassers gebonden zijn aan de regels voor de rechtmatige verwerking van persoonsgegevens die voortvloeien uit de WBP. Het beschermingsniveau dat hiermee geboden wordt lijkt in het kader van RFID-toepassingen toereikend. Het is dus vooralsnog niet noodzakelijk om RFID specifieke aanvullingen te maken op de WBP. Uiteindelijk zal de ervaring moeten leren of deze conclusie houdbaar is.

Aanvullende RFID-wetgeving is naast niet noodzakelijk naar alle waarschijnlijkheid in dit stadium van de ontwikkeling ook contra-productief. Omdat de concrete implementatie van de techniek op veel punten nog niet volledig uitgekristalliseerd is en per sector en toepassing zal verschillen, bestaat de kans dat het huidig technisch en theoretisch kader dat gebruikt zal worden als uitgangspunt voor RFID-wetgeving te algemeen is en niet in overeenstemming met de uiteindelijke praktijk. Dergelijke premature wetgeving zal de verdere ontwikkeling en toepassing van deze veelbelovende en voor Nederland zeer belangrijke technologie nodeloos vertragen

c.q. frustreren en niet noodzakelijkerwijs bijdragen aan de bescherming van de privacy.

Hoewel het wettelijk beschermingsniveau adequaat is, lijkt het gezien het bijzondere karakter van RFID verstandig nadere invulling te geven aan de abstracte formuleringen van de WBP in de vorm van aanvullende (sector-specifieke) gedragsregels die de inhoud van de WBP helderder uiteenzetten. Het is met name van belang in deze gedragsregels duidelijke afspraken te maken over de invulling van bepalingen uit de WBP zoals de informatieverplichtingen (artikelen 33 en 34 WBP), overige voorlichting aan de consument, en regels omtrent toegang tot en beveiliging van gegevens. Daarnaast lijkt het opstellen van gedragsregels verstandig aangezien niet bij alle privacyrisico's noodzakelijkerwijs sprake is van het verwerken van persoonsgegevens en de privacybeleving van de burger ook niet per definitie gekoppeld is aan de idee van het verwerken van gegevens.

Gezien het feit dat inbreuken op de privacy bij RFID reëel zijn en in potentie ingrijpend, is met het oog op de bescherming van de consument handhaving van wet- en regelgeving en sanctionering een vereiste. Het bedrijfsleven is ook gebaat bij strenge handhaving en sanctionering van (zelf)regulering. Incidenten buiten Nederland hebben geleerd dat het sentiment van de consument door de mistappen van één enkel bedrijf om kan slaan. Het zou er bedrijven veel aan gelegen moeten zijn om dergelijk negatief sentiment (en mogelijke stringente wetgeving die daarop volgt) te voorkomen.

Voor de RFID-toepassingen waarbij persoonsgegevens worden opgeslagen op de tag dienen adequate beveiligingsmaatregelen te worden genomen om te voorkomen dat de tag wordt uitgelezen door onbevoegde derden. Bij de RFID-toepassingen die enkel een uniek nummer bevatten dient met name gekeken te worden naar de inrichting van de achterliggende bedrijfsprocessen en systemen. Dit is echter niet een RFID-specifieke kwestie maar maakt deel uit van de algemene procedure rondom de bescherming van persoonsgegevens en informatiebeveiliging. Belangrijk punt van aandacht voor de toekomst blijft wel de mogelijke schaalvergroting (meer en eenvoudigere data aggregatie) die zal optreden door het gebruik van RFID.

Uit de analyse van de risico's blijkt dat gevaren voor de privacy tot een minimum beperkt kunnen worden indien de regels uit de WBP worden nageleefd door RFID-toepassers. Bij het niet naleven van de WBP kunnen er wel degelijk aanzienlijke risico's voor de privacy van de burger/consument ontstaan. In onze huidige maatschappij (zonder vergaande toepassing van RFID) bestaan reeds vele mogelijkheden om (heimelijk) persoonsgegevens te verzamelen, RFID vormt daarom niet zozeer een kwalitatief verschil met bestaande technologieën maar veeleer een kwantitatief verschil. De schaal, het gemak en de fijnmazigheid waarmee gegevens verzameld kunnen worden in een RFID-omgeving is vele malen groter dan met de huidige stand van de techniek, hetgeen noopt tot extra zorgvuldigheid. Privacyrisico's zijn reëel, maar vloeien hoofdzakelijk voort uit onverantwoord gebruik (het onbewust niet voldoen aan de regels van de WBP) of misbruik (het bewust niet voldoen aan de regels van de WBP) van RFID-systemen.

Het eerste probleem (onverantwoord gebruik) kan met behulp van de hiervoor reeds genoemde gedragsregels en communicatie richting toepassers van RFID grotendeels worden ondervangen. Bij de toepassers van RFID moet het bewustzijn groeien dat RFID een technologie is die 'privacygevoelig' kan zijn indien niet is gezorgd voor de juiste beveiligingsmaatregelen en geen rekening wordt gehouden met de bepalingen uit de WBP.

Bij het tweede probleem (misbruik) is het niet een kwestie van het uitbreiden van de wettelijke bescherming van het recht op privacy, maar een kwestie van het verhogen van de transparantie van het bestaande regime en het versterken van de handhaving. In dit kader moet afgezien van de economische invalshoek (misbruik van persoonsgegevens door bedrijven) ook gekeken worden naar mogelijk misbruik door criminelen. Voor die scenario's waar de kans op misbruik groter is en/of de impact daarvan hoger kan gekeken worden naar sanctionering via bestuurlijke boeten, het financieel economisch strafrecht (Wet Economische Delicten), of als *ultimum remedium* het commune strafrecht (Wetboek van Strafrecht).

Tot slot heeft de consument ook een eigen verantwoordelijkheid met betrekking tot het

beschermen dan wel ter beschikking stellen van zijn persoonsgegevens. Om deze verantwoordelijkheid echter goed te kunnen nemen dient de consument over voldoende informatie te beschikken alsmede de (technische) middelen om invulling te geven aan zijn rechten. Het voorlichten van consumenten en het hanteren van een algemene houding van openheid met betrekking tot het verwerken van gegevens is in veel gevallen reeds een wettelijke plicht, maar ook een noodzakelijke voorwaarde om de rechten van de consument te waarborgen en de acceptatie van RFID te stimuleren.

Met betrekking tot het uitoefenen van zijn rechten dient de consument bovenal keuzevrijheid te hebben als het aankomt op het gebruik van RFID. De consument moet dus de mogelijkheid worden geboden om een RFID-tag te verwijderen dan wel uit te schakelen, tenzij deze mogelijkheid niet bestaat, omdat uitschakeling of verwijdering de werking van het RFID-systeem negatief beïnvloedt. Het is in dit stadium nog te vroeg om een concreet antwoord te formuleren op de vraag of RFID-tags (met name EPC smart labels) na het verlaten van de winkel standaard geactiveerd blijven, per definitie gedeactiveerd moeten worden, of gedeactiveerd moeten *kunnen* worden. De discussie omtrent keuzevrijheid voor de consument zal zich dan ook in de nabije toekomst naar alle waarschijnlijkheid toespitsen op de vraag of een EPC smart label standaard actief blijft bij het verlaten van de winkel en de consument het recht heeft het smart label te deactiveren (opt-out), of dat de EPC smart label bij het verlaten van de winkel standaard gedeactiveerd wordt en de consument de keuze heeft om de smart label te activeren (opt-in).

Om misbruik door derden te voorkomen zou ook de mogelijkheid tot het afschermen van RFID-tags nader onderzocht moeten worden. In dit kader is het onderzoek naar technische voorzieningen zoals bijvoorbeeld encryptie en blocker tags van wezenlijk belang.

Deze studie vormt een eerste tentatieve aanzet tot het analyseren van de privacyrisico's van RFID. Er bestaat echter nog veel onduidelijkheid over de technische mogelijkheden van RFID, de toepassing ervan in onze maatschappij, en de gevolgen daarvan. Het blijft dus bij het analyseren van de risico's en het formuleren van mogelijke beleid tot op zeke-

re hoogte 'schieten op een bewegend doel'.  
Bij het doen van aanbevelingen wordt dit in  
ogenschouw genomen.

ECP.NL blijft zich in 2005 inzetten voor het  
adresseren en oplossen van maatschappelij-  
ke vraagstukken die met RFID samenhangen.

## 9 Aanbevelingen

Op basis van dit rapport en de daaraan verbonden conclusies doet de Werkgroep Privacy & RFID de volgende aanbevelingen richting overheid en bedrijfsleven:

### Voorlichting

In dit rapport is meermalen het belang van voorlichting en openheid in het kader van RFID onderstreept. De Werkgroep ziet voorlichting over RFID en de privacyrechtelijke aspecten van RFID als het belangrijkste hulpmiddel voor een gecoördineerde en verantwoorde toepassing van RFID.

- Geef duidelijke voorlichting over RFID in zijn algemeenheid en de privacyrechtelijke aspecten ervan in het bijzonder. Deze voorlichting moet gericht worden tot gebruikers van RFID en tot consumenten, burgers, patiënten et cetera.
- Overheid en bedrijfsleven dienen richting consument, burger, patiënt et cetera een open houding aan te nemen met betrekking tot de toepassing van RFID. Kennisgeving is hierbij een eerste voorwaarde, maar het is ook raadzaam aanvullende informatie ter beschikking te stellen.
- Kennisdeling op het gebied van RFID en privacy (bijvoorbeeld in de vorm van best practices) dient gestimuleerd te worden.

### Helderheid implementatie juridisch kader

Er kan geconcludeerd worden dat hoewel de huidige privacywetgeving in het kader van RFID zowel toepasselijk als toereikend is, de concrete toepassing ervan soms nog onduidelijk is. Aanbieders en gebruikers van RFID alsmede consumenten, burgers, patiënten et cetera zijn daarom gebaat bij het verhelderen van de abstracte bepalingen uit de wet.

- De WBP kan in het kader van RFID verhelderd worden door middel van een 'Model Code Privacy & RFID'. Een dergelijke Code kan als richtsnoer dienen voor de implementatie van het huidig wet- en regelgevend kader in onder andere branchespecifieke gedragscodes. De Code dient door partijen (aanbieders, gebruikers, consumenten/burgers en de overheid) in samenspraak opgesteld te worden.

- Om het probleem van het onbewust niet naleven van de WBP te adresseren dienen de mogelijke toepassers van RFID-technologie op de hoogte te worden gebracht van de regels uit de WBP, alsmede van de technische mogelijkheden en onmogelijkheden van RFID. Alleen met deze informatie zullen mogelijke toepassers in staat zijn een genuanceerde keuze te maken met betrekking tot de implementatie van RFID in hun bedrijfsvoering. Hier ligt duidelijk een gezamenlijke taak voor de markt en de overheid.
- Er dient rekening te worden gehouden met een ophanden zijnde 'opt-in, opt-out discussie' in het kader van RFID.

### Aanvullend onderzoek

Doordat ontwikkelingen op het gebied van RFID zich momenteel in een stroomversnelling bevinden is het op veel punten nog moeilijk om de economische en maatschappelijke effecten van RFID te beoordelen. Om deze reden is het raadzaam om aanvullend onderzoek op dit gebied te stimuleren.

- Er dient aanvullend onderzoek te worden gedaan naar mogelijk misbruik van RFID en de maatschappelijke impact van dergelijk misbruik.
- Er dient aanvullend onderzoek te worden gedaan naar de kansen die RFID biedt voor de handhaving van de openbare orde en de opsporing van strafbare feiten. Hierbij dient echter ook onderzoek te worden gedaan naar de mogelijke gevolgen die dit heeft voor de privacy en individuele vrijheid van de burger.
- Het onderzoek naar technische voorzieningen die de privacy helpen beschermen (privacy enhancing technologies) dient gestimuleerd te worden door zowel het bedrijfsleven als de overheid.
- Er moet gezocht worden naar mechanismen die de burger helpen meer controle te krijgen over de verwerking van zijn persoonsgegevens in het kader van RFID. Hierbij kan gedacht worden aan technische maatregelen zoals privacy enhancing technologies, maar ook aan mechanismen om meer invulling te geven aan de rechten die een betrokkene vanuit de WBP heeft (zoals het recht op verzet en het recht op inzage).

### **Internationale dimensie**

Het is van belang dat Nederland internationaal gezien geen 'eiland' wordt met betrekking tot wet- en regelgeving op het gebied van RFID en privacy. Er dient daarom rekening te worden gehouden met internationale ontwikkelingen. De volgende aanbevelingen kunnen worden gedaan:

- Overheid en bedrijfsleven dienen waar mogelijk aansluiting te zoeken bij internationale initiatieven.
- Nederland dient waar nodig invloed uit te oefenen op de ontwikkelingen via internationale gremia.

# 10 Literatuurlijst

## **Agrawal 2003**

Agrawal D, Archambeault B, Chari S, Rao J.R, Rothatgi P, Advances in Side-Channel Cryptanalysis, Electromagnetic Analysis and Template Attacks, in: *RSA Laboratories Cryptobytes Volume 6, No1--Spring 2003*

## **Alok Jha 2003**

Alok Jha (2003). Tesco tests spy chip technology: Tags in packs of razor blades used to track buyers, in: *The Guardian, Saturday July 19, 2003*

## **Artikel 29 Werkgroep 2005**

Artikel 29 Werkgroep (2005). *Working Document on Data Protection Issues Related to RFID Technology*. 10107/05/EN WP 105

## **Artz 1999**

Artz, M. J. T. (1999), Koning Klant, het gebruik van klantgegevens voor marketingdoeleinden, *Achtergrondstudies en Verkenningen 14*, Den Haag: Registratiekamer

## **Ashton 2003a**

Ashton, K (2003). Testimony of Kevin Ashton (Executive Director, Auto-ID Center), *California State Senate Subcommittee on New technologies Hearing on RFID and Privacy*, August 18, 2003

## **Ashton 2003b**

Ashton, K. (2003), *Options for Regulation of the EPCglobal Network*, Auto ID Center, MIT-AUTOID-EB-006

## **Auto ID Center 2002**

Anoniem, *860MHz-930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1*, Auto ID Center 14 november 2002

## **Big Research & Artafact 2004**

Big Research & Artafact (2004). *RFID Consumer Buzz Report*  
<<http://www.bigresearch.com/rfid>>

## **Blok 2002**

Blok, P. (2002). *Het Recht op Privacy*, Boom Juridische Uitgevers.

## **Cantwell 2003**

Cantwel B. (2003). *Why Technical Breakthroughs Fail: A History of Public Concern with Emerging Technologies*, Auto ID Center, MIT-AUTOID-WH-016

## **Capgemini 2005a**

Capgemini (2005). *RFID and Consumers, What European Consumers Think About Radio Frequency Identification*, februari 2005

## **Capgemini 2005b**

Capgemini (2005). *RFID in de praktijk*, Capgemini Nederland BV, februari 2005

## **Cavoukian 2004**

Cavoukian, A. (2004). *Tag, You're it: Privacy Implications of Radio Frequency (RFID) Technology*, Toronto: Information and Privacy Commissioner/Ontario.

## **Duce 2003**

Duce H. (2003). *Public Policy: Understanding Public Opinion*, Auto ID Center, CAM-AUTOID-EB-002

## **Etzioni 1999**

Etzioni, A. (1999). *The Limits of Privacy*, New York: Basic Books

## **Franken 2000**

Franken, H. et al. (2000), *Commissie Grondrechten in het Digitale Tijdperk 2000*

## **Frost & Sullivan 2004**

Frost & Sullivan 2004, *World RFID Based Applications Market*,  
<<http://www.autoid.frost.com>>

## **Gagné 2003**

Gagné M. (2003). Identity-Based Encryption: a Survey, in: *RSA Laboratories Cryptobytes Volume 6, No1--Spring 2003*

## **Gandy 1993**

Gandy, O. *The Panoptic Sort: a Political Economy of Personal Information*, Westview Boulder 1993

## **Garfinkel 2002**

Garfinkel S. (2002), An RFID Bill of Rights, in: *Technologie Review, october 2002*

## **Givens 2003**

Givens B. (2003). RFID and the Public Policy Void, in: *Joint Committee on Preparing California for the 21st Century*, 2003

**Gordon 2003**

Gordon L. (2003). *Tracked By Your Clothes*, The Globe; A quarterly newsletter of LawExchange International, zomer 2003

**Gutwirth 1998**

Gutwirth, S. (1998). *Privacyvrijheid! De vrijheid om zichzelf te zijn*. Otto Cramwinckel Uitgevers.

**Hines 2004**

Hines M. (2004). Roadblocks could slow RFID, in: *CNET News.com*, 2004

**IBM 2003**

IBM (2003). *Global Commerce Initiative EPC Roadmap*

**Juels 2003**

Juels, A., Rivest R. L., Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID-tags for Consumer Privacy, RSA, in: *8th ACM Conference on Computer and Communications Security* (ed. V. Atluri), pp. 103-111. ACM Press. 2003

**Kosto 1992**

Kosto A. (1992). Complementaire verhoudingen bij de wetgeving, in: N.J.H. Huls en H.D Stout (red.), *Reflecties op reflexief recht*, 1992

**Koops 2000**

Koops, B. J., Prins C., Schellekens. M., Gijrath, S., Schreuders, E. (2000). *Overheden over internationalisering en ICT*, ITER 39, Kluwer: Deventer

**Meloan 2003**

Meloan, S. (2003). *Toward a Global "Internet of Things"*, Sun Microsystems

**Natsui, 2004**

Natsui, T. (2004). *Traceability System using RFID and Legal Issues*, at WHOLES conference, Stockholm, januari 2004

**OECD 1980**

OECD (1980), *Guidelines governing the protection of privacy and transborder flows of personal data*.

**Roberti 2004**

Roberti, M. (2004). The Law of the Land, in: *RFID Journal*, March 2004

**Sarma 2003**

Sarma, S. E., Weis, S. A., Engels, D. W. (2003). Radio-Frequency Identification: Security Risks and Challenges, in: *RSA Laboratories Cryptobytes* Volume 6, No1--Spring 2003

**Sarma 2002a**

Sarma, S. E., Weis S. A., Engels D. W. (2002). *RFID Systems, Security & Privacy Implications*, Auto ID Center Cambridge Massachusetts

**Sauerwein 2002b**

Sauerwein L.B., Linnemann, J.J. (2002). *Handleiding voor verwerkers van Persoonsgegevens*, Den Haag: Ministerie van Justitie

**Schermer 2004**

Schermer, B. W. (2004). RFID: Big Brother in een kleine chip?, in: *JAVI*, Jaargang 3 nummer 4, oktober 2004

**Rietdijk 2004**

Rietdijk, J. W., Trier, van, M. (2004). *Innoveren met RFID, op de golven van verbetering*, tenHagenStam Uitgevers

**US Dept. Health 1973**

U.S. Dep't. of Health, Education and Welfare(1973). *Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens*.

**Ustaran 2004**

Ustaran E. (2004). *Data Protection and RFID Systems*, Privacy & Data Protection, Volume3, Issue 6, 2004

**Verhaegh 2004**

Verhaegh, S. (2004). *Bits of Freedom Dossier Privacy & RFID*. <<http://www.bof.nl/rfid>>

**Westin 1967**

Westin, A. F. (1967). *Privacy and Freedom*, New York: Atheneum Press.

**Kamerstukken**

Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 1-2

Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3

Wijziging van de Telecommunicatiewet en enkele andere wetten, Tweede Kamer, vergaderjaar 2002-2003, 28 851, nr. 1-2

Wijziging van de Telecommunicatiewet en enkele andere wetten, Tweede Kamer, vergaderjaar 2002-2003, 28 851, nr. 3

### Internetsites

#### Emerce

VIP-chips in Rotterdamse Baja Beach Club <<http://www.emerce.nl/nieuws.jsp?id=277589>> (geraadpleegd 12 mei 2004)

#### EPIC RFID 2004

EPIC RFID Privacy Page, *Radio Frequency Identification (RFID) Systems*, WWW <<http://www.epic.org/privacy/rfid/>> (geraadpleegd 17 februari 2004)

#### PML 2003

Institute for pervasive computing (department of science), *Physical Mark-Up Language (PML)*, WWW <<http://www2.inf.ethz.ch/~floerkem/>> (bijgewerkt 2 januari 2003)

#### Recommended Safeguards

*Recommended Safeguards for Administrative Personal Data Systems Chapter IV*, WWW <<http://aspe.os.dhhs.gov/datacncl/1973privacy/c4.htm>> (geraadpleegd 26 februari 2004)

#### RFID Journal 2004

<http://www.rfidjournal.com>

#### RFID Position Statement 2003

RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, *Position Statement on the Use of RFID on Consumer Products*, WWW <<http://www.privacyrights.org/ar/RFIDposition.htm>> (geraadpleegd 17 februari 2004).

#### RFID Right to Know Act 2003

Consumers Against Supermarket Privacy Invasion And Numbering (CASPIAN), *Right to Know Act*, WWW <<http://www.nocards.org/rfid/rfidbill.shtml>> (geraadpleegd 17 februari 2004)

#### RFID Right to Know Act Summary 2003

Consumers Against Supermarket Privacy Invasion And Numbering (CASPIAN), *Right to Know Act(summary)*, WWW <<http://www.nocards.org/rfid/rfidbillsummary.shtml>> (geraadpleegd 17 februari 2004)

#### RFID Wizards

*RFID Wizards*, WWW <<http://www.rfidwizards.com/>>, bijgewerkt 2003.

#### Safeguards voor privacy

Records, Computers and the Right of Citizens (1973), *Safeguards voor privacy*, WWW <<http://aspe.os.dhhs.gov/datacncl/1973privacy/c3.htm>> (geraadpleegd 26 februari 2004)

#### Marktonderzoek:

Capgemini (2005). *RFID and Consumers, What European Consumers Think About Radio Frequency Identification*, februari 2005

Contact voor nadere informatie in Nederland: [marc.spronk@capgemini.com](mailto:marc.spronk@capgemini.com)  
Contact voor nadere informatie Internationaal: [ardjan.vethman@capgemini.com](mailto:ardjan.vethman@capgemini.com)

Big Research & Artafact (2004). *RFID Consumer Buzz Report* < <http://www.bigresearch.com/rfid> >

# 11 Bijlagen

## 11.1 Bijlage I: Internationale wetgeving (algemeen)

Het recht op bescherming van de persoonlijke levenssfeer wordt in de rechtsorde van nagenoeg alle landen in de westerse wereld impliciet of expliciet als grondrecht erkend.<sup>32</sup> Op internationaal niveau zijn er diverse verdragen waarin het recht op privacy is vastgelegd. De belangrijkste zijn de Universele Verklaring van de Rechten van de Mens, het Internationale Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) en het Verdrag tot de Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Hoewel er kleine tekstuele verschillen tussen de verdragen bestaan, komen de formuleringen van het recht op bescherming van de persoonlijke levenssfeer grotendeels overeen.

Naast wetgeving zijn er diverse regelgevende initiatieven op het gebied van privacy in het algemeen en RFID in het bijzonder. Hoewel deze initiatieven niet de status hebben van wetgeving kunnen ze wel van groot belang zijn. Belangrijke regelgeving met betrekking tot privacy zijn de Fair Information Practice Principles en de OECD Privacy Guidelines. De OECD Guidelines bevatten belangrijke beginselen aangaande kwaliteit, doelspecificatie, doelbinding, beveiligingswaarborgen, transparantie, aansprakelijkheid en recht op inzage, correctie en verzet. Deze beginselen zijn van grote invloed geweest op de ontwikkeling van privacywetgeving met name binnen de Europese Unie.

Enkele regelgevende initiatieven op het gebied van RFID die kunnen worden genoemd zijn de EPC Guidelines, de RFID Bill of Rights en ICDPPC Resolution on Radio-Frequency Identification. Omdat specifieke wetgeving op het gebied van RFID uitvoerig wordt behandeld, wordt voor een nadere uitwerking van RFID-regelgeving verwezen naar Bijlage III.

### 11.1.1 Universele Verklaring van de Rechten van de Mens<sup>33</sup>

Op 10 december 1948 is door de Algemene

Vergadering van de Verenigde Naties de Universele Verklaring van de Rechten van de Mens aangenomen. De lidstaten van de Verenigde Naties verplichten zich door middel van het aannemen van de Verklaring de rechten van de mens zo goed mogelijk te waarborgen.

De Universele Verklaring is niet bindend, met andere woorden de Verklaring kent geen speciaal handhavingsmechanisme. Het is veeleer een intentieverklaring van de deelnemende landen om binnen hun territorium de mensenrechten te respecteren en op internationaal niveau te streven naar een betere waarborging van deze rechten.

Artikel 12 van de Verklaring ziet op de bescherming van de persoonlijke levenssfeer:

*“Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.”*

### 11.1.2 Het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR)<sup>34</sup>

Het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) werd op 16 december 1966 aangenomen door de Algemene Vergadering van de Verenigde Naties en werd op 23 maart 1976 officieel van kracht. Het IVBPR betreft een uitwerking van de rechten opgesomd in de Universele Verklaring van de Rechten van de Mens. In tegenstelling tot de Universele Verklaring is het IVBPR wel bindend. Een Comité ziet toe op de naleving van de in het verdrag opgesomde rechten en plichten.<sup>35</sup> Artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten stelt dat:

*“Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.”*

32 Zo is er in de Amerikaanse Constitutie geen expliciet grondrecht op bescherming van de persoonlijke levenssfeer, maar wordt dit in de Fourth Amendment (search and seizure) gelezen.

33 Universele Verklaring van de Rechten van de Mens, 10 december 1948

34 New York, 19 december 1966, Tractatenblad 1969 nr. 99,

35 Zie hiervoor artikel 28 IVBPR

en dat een ieder recht heeft op bescherming door de wet tegen zodanige inmenging of aantasting.

### 11.1.3 EVRM<sup>36</sup>

Het voor Nederland belangrijkste verdrag op het gebied van de bescherming van de mensenrechten is het Verdrag tot de Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Op 4 november 1950 is dit verdrag aangenomen door de Raad van Europa.

Artikel 8 EVRM ziet op de bescherming van de persoonlijke levenssfeer. Het is de Europese tegenhanger van artikel 10 Grondwet. De artikelen lijken sterk op elkaar en zijn beide techniekonafhankelijk. Artikel 8 EVRM luidt als volgt:

1. Een ieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economische welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

## 11.2 Bijlage II: regelgeving informatiele privacy

In de laatste dertig jaar hebben als gevolg van de ontwikkeling van informatie- en communicatie technologie grote veranderingen plaatsgevonden op het gebied van privacy. De nadruk bij de bescherming van de privacy ligt nu grotendeels bij persoonsgegevens, een ontwikkeling die ingezet is met de publicatie van de Fair Information Practice Principles.

### 11.2.1 Fair Information Practice Principles

De Fair Information Practice Principles gepubliceerd door de US Department of Health, Education and Welfare zijn:<sup>37</sup>

- Er mogen geen systemen zijn voor de verwerking van persoonsgegevens waarvan

het bestaan geheim is.

- Het moet voor een persoon mogelijk zijn om kennis te nemen van de informatie die over hem of haar verzameld is en hoe deze informatie verwerkt wordt.
- Het moet voor een persoon mogelijk zijn om te voorkomen dat informatie betreffende zijn/haar persoon zonder toestemming aangewend of verstrekt wordt voor een doel anders dan de oorspronkelijke verwerking.
- Het moet voor een persoon mogelijk zijn om zijn/haar persoonsgegevens te verbeteren of aan te vullen.
- Elke organisatie die verantwoordelijk is voor het genereren, onderhouden, gebruiken, verstrekken of anderszins verwerken van persoonsgegevens moet zorg dragen voor de betrouwbaarheid van deze persoonsgegevens, voor het doel van de verwerking en maatregelen nemen om misbruik van deze persoonsgegevens te voorkomen.

### 11.2.2 OECD Privacy Guidelines<sup>38</sup>

De OECD Privacy Guidelines zijn in 1980 binnen de OECD (OESO) opgesteld. De Guidelines vormen een belangrijk richtsnoer voor de verwerking van persoonsgegevens en staan aan de basis van diverse internationale wetgevingsinitiatieven. De Guidelines leggen een aantal principes neer welke hieronder opgesomd staan:

- *Collection limitation principle*

Deze bepaling stelt dat er een limiet is aan de hoeveelheid gegevens die over een persoon verzameld mogen worden en dat deze data op rechtmatige en eerlijke wijze verkregen moet worden, waar noodzakelijk met de wetenschap of toestemming van de betrokkene.

- *Data quality principle*

Deze bepaling stelt dat persoonsgegevens noodzakelijk moeten zijn voor het doel waartoe ze verwerkt worden en voor dit doel compleet, nauwkeurig en up-to-date moeten zijn.

- *Purpose Specification principle*

Deze bepaling stelt dat het doel waartoe persoonsgegevens verzameld worden niet later vermeld dient te worden dan het moment van verkrijging, en dat de persoonsgegevens

36 Verdrag van 4 november 1950, Trb. 1951, 154

37 US Dept. Health 1973

38 *OECD Guidelines governing the protection of privacy and transborder flows of personal data*, 1980.

enkel en alleen mogen worden verwerkt ten behoeve van dit doel, of doelen die met het oorspronkelijke doel verenigbaar zijn.

- *Use limitation principle*

Deze bepaling stelt dat persoonsgegevens niet openbaar mogen worden gemaakt, verstrekt of anderszins gebruikt anders dan in overeenstemming met het purpose specification principle (doelbindingscriterium). Een uitzondering op deze regel is enkel mogelijk met de toestemming van de betrokkene of bij de wet voorzien.

- *Security safeguards principle*

Deze bepaling stelt dat er adequate veiligheidsmaatregelen genomen dienen te worden om persoonsgegevens te beschermen tegen ongeoorloofde toegang, vernietiging, gebruik, aanpassing of openbaring.

- *Openness principle*

Deze bepaling stelt dat er een algemeen beleid van openheid dient te zijn met betrekking tot ontwikkelingen, toepassingen en beleidsvorming op het gebied van de verwerking van persoonsgegevens. Het moet in voldoende mate mogelijk zijn om het bestaan en de aard van persoonsgegevens vast te stellen, alsmede de doelen voor het gebruik van persoonsgegevens. Verder moet het mogelijk zijn om de vestigingsplaats en de identiteit van de verantwoordelijke voor de verwerking vast te stellen.

- *Individual participation principle*

Deze bepaling geeft de betrokkene een aantal rechten te weten:

- a) Het recht om van een verantwoordelijke te vernemen of deze persoonsgegevens over de betrokkene heeft.
- b) Het recht om informatie te krijgen over zijn persoonsgegevens:
  - i) binnen een redelijke termijn;
  - ii) -indien niet gratis- tegen een redelijk bedrag;
  - iii) op een redelijke manier;
  - iv) in een formaat dat duidelijk te begrijpen is.
- c) Het recht op motivatie indien de rechten onder a) en b) niet gehonoreerd kunnen worden en de mogelijkheid om zich tegen deze weigering te verzetten.

- d) Het recht om in verzet te gaan tegen de verwerking van zijn persoonsgegevens en indien dit verzet gegrond wordt geacht het recht om de persoonsgegevens te wissen, rectificeren, aanvullen of completeren.

- *Accountability principle*

Deze bepaling stelt dat de verantwoordelijke aansprakelijk is voor het naleven van alle voorgaande bepalingen.

### **11.3 Bijlage III: RFID specifieke (zelf)regulering**

Naast algemene wet- en regelgeving op het gebied van informatieprivacy wordt er ook hard gewerkt aan RFID specifieke regulering. Hieronder worden de belangrijkste initiatieven opgesomd.

#### *11.3.1 EPC guidelines*

Als beheerder van de EPC standaard heeft EPCGlobal een aantal richtlijnen voor het gebruik van EPC opgesteld. Deze richtlijnen dienen als aanvulling op reeds bestaande nationale en internationale wet- en regelgeving. De EPC Guidelines moeten het vertrouwen in het gebruik van de EPC en het EPC netwerk stimuleren. De Guidelines bevatten vier kernpunten:

- *Consumer Notice*

Consumenten moeten op de hoogte worden gesteld van de aanwezigheid van EPC RFID-tags. Hiertoe dient een vermelding te worden opgenomen op het product of de verpakking.

- *Consumer Choice*

Consumenten moeten geïnformeerd worden over de mogelijkheden om EPC RFID-tags te verwijderen of uit te schakelen wanneer deze gekocht worden.

- *Consumer Education*

Consumenten moet de mogelijkheid worden geboden om snel en makkelijk duidelijke informatie te krijgen over EPC, de toepassingen ervan en toekomstige ontwikkelingen op het gebied van EPC.

- *Record Use, Retention and Security*

Het verwerken van (persoons)gegevens gegenereerd door het EPC-systeem dient in overeenstemming te zijn met alle toepasselijke wet- en regelgeving. Bedrijven die gebruik maken van EPC dienen kenbaar te maken (bijvoorbeeld door publicatie op de

website) wat hun beleid is met betrekking tot de verwerking en bescherming van persoonsgegevens, met name die (persoons)gegevens die gegenereerd en/of verwerkt worden door het EPC-systeem.

### 11.3.2 RFID Bill of Rights

In oktober 2002 verscheen in Technology Review van de hand van Simson Garfinkel het artikel 'An RFID Bill of Rights'. In dit artikel schetste Garfinkel de mogelijke gevaren voor de privacy van burgers als gevolg van het gebruik van RFID. Hij stelt een 'Bill of Rights' voor waarin een aantal consumentenrechten is vastgelegd. Het gaat om de volgende rechten:

- het recht om te weten of een product een RFID-tag bevat;
- het recht om RFID-tags uit te schakelen of te verwijderen wanneer een product gekocht wordt;
- het recht om van diensten gebruik te maken zonder RFID-tags, daar waar deze normaliter wel van RFID gebruik maken.
- het recht om kennis te nemen van de in een tag opgeslagen informatie;
- het recht om te weten wanneer, waar en waarom tags gelezen worden.

De RFID Bill of Rights is opgesteld als een raamwerk voor zelfregulerende initiatieven vanuit het bedrijfsleven.

### 11.3.3 ICDPPC Resolution on Radio-Frequency Identification

Op 20 november 2003 is door de International Conference of Data Protection & Privacy Commissioners een resolutie aangenomen met betrekking tot het verantwoord gebruik van RFID. De resolutie bevat de volgende punten:

- Elke verantwoordelijke moet, alvorens over te gaan tot de introductie van een RFID-systeem dat persoonsgegevens verwerkt, alle mogelijke alternatieven overwegen waarmee hetzelfde doel kan worden bereikt zonder de verwerking van persoonsgegevens.
- Als de verantwoordelijke kan aantonen dat de verwerking van persoonsgegevens door middel van een RFID-systeem noodzakelijk is, dan dient deze verwerking open en transparant te geschieden.
- Persoonsgegevens mogen alleen verwerkt worden voor het doel waartoe ze verkregen zijn en mogen alleen bewaard worden zolang dit noodzakelijk is voor het doel

waartoe de persoonsgegevens verkregen zijn.

- Wanneer een RFID-tag in het bezit van een individu komt, dan moet deze de mogelijkheid worden geboden de tag onschadelijk te maken en/of de daarop vastgelegde data te vernietigen.

### 11.3.4 ICC Principles on EPC deployment and operation

In maart 2005 hebben de International Chambers of Commerce (ICC) een aantal principes opgesteld aangaande de verantwoorde toepassing van EPC systemen. Het document kent een zevental artikelen:

#### • Artikel 1: Algemene bepalingen

Bevat algemene uitgangspunten over eerlijk en verantwoord gebruik, voorlichting en vrije keuze.

#### • Artikel 2: Informatie en keuze

Geeft regels omtrent de informatievoorziening aan consumenten, etikettering en keuzemechanismen voor de consument.

#### • Artikel 3: Openheid

Geeft regels over de openheid die bedrijven moeten betrachten met betrekking tot het gebruik van EPC, bijvoorbeeld via een privacy policy.

#### • Artikel 4: Rechtmatige en eerlijke gegevensverzameling

Stelt regels omtrent de gegevensverzameling en vormt als zodanig een uitwerking van beginselen zoals die onder andere in de WBP zijn verwoord.

#### • Artikel 5: Doelbinding

Stelt regels omtrent de doelbinding en vormt als zodanig een uitwerking van beginselen zoals die onder andere in de WBP zijn verwoord.

#### • Artikel 6: Beveiliging

Stelt regels omtrent de beveiliging en vormt als zodanig een uitwerking van beginselen zoals die onder andere in de WBP zijn verwoord. Ook wordt ingegaan op de beveiliging van gekoppelde systemen.

#### • Artikel 7: Recht op toegang

Stelt regels omtrent de rechten van de betrokkene op inzage, correctie en verzet en vormt als zodanig een uitwerking van beginselen zoals die onder andere in de WBP zijn verwoord.

## 11.4 Bijlage IV: Voorgestelde RFID specifieke wetgeving

In de Verenigde Staten (waar de toepassing van RFID verder gevorderd is dan in Europa) zijn reeds drie formele wetgevingsinitiatieven genomen om het gebruik van RFID in goede banen te leiden. De voorstellen zijn deels ingegeven door het werk van consumentenorganisatie CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) die voor dit doel zelfs een eigen model voor een wet hebben gemaakt: de CASPIAN RFID Right to Know Act.<sup>39</sup> Overigens zijn alle wetsvoorstellen tot op heden gestrand in het wetgevingstraject. De voornaamste reden hiervoor is dat beleidsmakers niet de ontwikkeling van een veelbelovende technologie nodeloos willen belemmeren door de introductie van starre, premature wetgeving.

### 11.4.1 CASPIAN RFID Right to Know Act

Naast zelfregulerende initiatieven geïnitieerd door marktpartijen die RFID willen gaan gebruiken, is in de Verenigde Staten door consumenten belangengroepering CASPIAN een model voor een wet opgesteld welke het gebruik van RFID moet reguleren.

De wet, welke de US Code zou moeten amenderen kent de volgende hoofdpunten:

- De verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat.
- Een bepaling die het aanbrengen van een onduidelijk label dat aangeeft dat een product een RFID-tag bevat bedreigt met sancties gelijk aan die gelden voor het verkeerd of niet labellen van producten.<sup>40</sup>
- Het verbod voor bedrijven om persoonsgegevens te koppelen aan informatie vastgelegd in individuele RFID-tags, anders dan hetgeen noodzakelijk is voor voorraadbeheer.
- Een verbod voor bedrijven om persoonsgegevens in samenhang met identificerende informatie uit een RFID-tag te verstrekken aan derden.

- Een aanwijzing aan de Federal Trade Commission om richtlijnen voor bedrijven op te stellen ter waarborging van de integriteit, vertrouwelijkheid en beveiliging van persoonsgegevens.
- Een aanwijzing aan de Federal Trade Commission om te waarborgen dat gegevens verkregen uit RFID-tags geen personen kunnen identificeren.
- Een aanwijzing aan de Federal Trade Commission om individuen te beschermen tegen mogelijke (toekomstige) bedreigingen voor de veiligheid van persoonsgegevens en negatieve gevolgen voor het individu die hier het gevolg van kunnen zijn.
- Een aanwijzing aan de Federal Trade Commission om burgers en bedrijven voor te lichten over het gebruik van RFID en de mogelijke negatieve gevolgen die dit kan hebben voor de privacy van de burger.

De RFID Right to Know Act of 2003 heeft als voorbeeld gediend voor de wetgevende initiatieven op deelstaat niveau. Deze wetsvoorstellen zijn minder vergaand dan het origineel.

### 11.4.2 RFID Right to Know Act 2004 (California)<sup>41</sup>

In februari 2004 is door Senator Bowen in California een wetsvoorstel ingediend dat het gebruik van RFID-systemen moet reguleren. In tegenstelling tot het wetsvoorstel van CASPIAN richt de aanpassing zich niet op federale wetgeving, maar op aanpassing van de wet in de deelstaat California. Inmiddels heeft het voorstel een aantal amendementen ondergaan en is het in april 2004 door de State Senate goedgekeurd. Eind juni 2004 is het wetsvoorstel echter verworpen in de State Assembly.

Het wetsvoorstel bevatte de volgende punten:<sup>42</sup>

Wanneer een RFID-systeem gebruik maakt van RFID-tags gekoppeld aan consumentenproducten of een reader die het mogelijk maakt om door het lezen van RFID-tags op consumentenproducten informatie te verzamelen, opslaan, gebruiken of delen die kan worden gebruikt om een persoon te identifi-

39 <<http://www.nocards.org>>

40 Vastgelegd in de Food, Drug and Cosmetic Act; US Code, title 21, chapter 9

41 State of California Senate Bill, No. 1384, 20 februari 2004

42 Opgenomen in Division 8, Section 1, Chapter 22.7 van de Business en Professions Code onder 22650, 22651, 22652, 22653, 22654, 22655 en 22656.

ceren, is voor een bedrijf niet toegestaan dit systeem te gebruiken tenzij:

- De reikwijdte van de verzamelde informatie niet verder gaat dan bij wet wordt toegestaan;
- De informatie door een klant aan het bedrijf wordt verstrekt om de afhandeling van een overeenkomst met betrekking tot het kopen of huren van een product met RFID-tag mogelijk te maken;
- De informatie niet verzameld wordt vóór het moment dat de klant daadwerkelijk de overeenkomst tot het kopen of huren van een product met RFID-tag aangaat en na het moment dat de overeenkomst is afgehandeld;
- De informatie alleen betrekking heeft op de klant die daadwerkelijk een product met RFID-tag wil kopen of huren en alleen met betrekking tot dat specifieke product.<sup>43</sup>

Voor een bibliotheek gelden dezelfde voorwaarden, maar dan met betrekking tot de boeken die worden geleend.

Een belangrijke omissie in dit wetsvoorstel is de afwezigheid van een definitie van het begrip RFID. Hoewel senator Bowen te kennen heeft gegeven dat de wetgeving alleen van toepassing is op die RFID-systemen waarmee persoonsgegevens verwerkt worden, betekent de afwezigheid van een definitie veel onzekerheid over de precieze reikwijdte en invulling van de wet.

#### *11.4.3 RFID Right to Know Act 2004 (Utah)<sup>44</sup>*

In Utah is ook een wetsvoorstel ingediend om het gebruik van RFID te reguleren, maar dat voorstel is vooralsnog van de baan. Nadat de wet goedgekeurd was door de Business and Labor Committee en het Huis van Afgevaardigden van Utah, verliep de indieningstermijn bij de Senaat van Utah. Waarschijnlijk zal het voorstel opnieuw worden ingediend op een later tijdstip. Het voorstel bevatte de volgende punten:

- De verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat, of indien dit niet mogelijk is, een waarschuwing nabij het product (bijvoorbeeld op het schap).
- De verplichting om RFID-tags uit te schakelen bij het verlaten van de winkel, tenzij een consument uitdrukkelijk aangeeft de tag actief te willen houden.

#### *11.4.4 RFID Right to Know Act 2004 (Missouri)<sup>45</sup>*

Ook in de staat Missouri is een RFID Right to Know Act ingediend. Het voorstel kent slechts één bepaling: de verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat. Ook dit voorstel is gestrand in het wetgevingstraject.

---

43 Dit houdt in dat er alleen informatie mag worden verzameld met betrekking tot het product dat daadwerkelijk bij de kassa wordt afgerekend, en niet met betrekking tot andere producten die de klant bij zich draagt of aan heeft. Ook mag er geen informatie worden verzameld met betrekking tot de producten die hij wel heeft bekeken of uit het schap gepakt, maar niet koopt of huurt.

44 State of Utah House Bill, No. 251, 27 januari 2004

45 State of Missouri Senate Bill, no. 867, 1 december 2003

## **11.5 Bijlage V: Werkgroep Privacy & RFID ECP.NL**

De onderstaande partijen zijn betrokken geweest bij de totstandkoming van dit rapport.  
De inhoud van dit rapport geeft niet noodzakelijkerwijs de individuele mening van partijen weer.

Bird & Bird  
Bits of Freedom  
Capgemini  
Centraal Bureau Levensmiddelenhandel  
College bescherming persoonsgegevens  
Consumentenbond  
DDMA  
eJure  
EPN, Platform voor de Informatiesamenleving  
Federatie Nederlandse Levensmiddelen Industrie  
Fox-IT  
GSI  
Houthoff Buruma  
IBM  
ICT~Office  
KPN  
Laurens  
M&I Partners  
Microsoft  
Ministerie van Economische Zaken  
Ministerie van Justitie  
Ministerie van Verkeer en Waterstaat  
National High Tech Crime Centre  
NEN  
NICTIZ  
Oracle  
Philips  
Raad Nederlandse Detailhandel  
Rabobank  
Radboud Universiteit Nijmegen  
RFID Society  
Safe Internet Foundation  
Sara Lee/DE  
SOLV Advocaten  
RFID Platform Nederland  
SURFnet  
Thuiswinkel.org  
TNO  
TPG POST  
Translink Systems  
Universiteit Leiden  
Universiteit Nyenrode  
Universiteit Tilburg  
Van Doorne  
VNO-NCW



