ACHTERGRONDSTUDIES EN VERKENNINGEN 28

RFID

Veelbelovend of onverantwoord?

Bijdrage aan de maatschappelijke discussie over RFID

R. Beugelsdijk

COLLEGE BESCHERMING PERSOONSGEGEVENS

ACHTERGRONDSTUDIES EN VERKENNINGEN 29

RFID

Veelbelovend of onverantwoord?

Bijdrage aan de maatschappelijke discussie over RFID

R. Beugelsdijk

COLLEGE BESCHERMING PERSOONSGEGEVENS

Publicaties in de serie achtergrondstudies en verkenningen zijn het resultaat van onderzoeken uitgevoerd door of in opdracht van het College bescherming persoonsgegevens (CBP). Met het uitbrengen van deze publicaties beoogt het CBP de discussie en de meningsvorming te stimuleren over ontwikkelingen in de samenleving waarbij de persoonlijke levenssfeer van de burger in het geding is. In veel gevallen wordt in de publicaties het normatieve kader zoveel mogelijk praktisch uitgewerkt voor het onderwerp van de studie. Het CBP wil hiermee een handreiking geven voor het realiseren van de eigen verantwoordelijkheid die de wet een ieder geeft voor de bescherming van persoonsgegevens.

COLOFON

RFID. Veelbelovend of onverantwoord? Bijdrage aan de maatschappelijke discussie over RFID.
College bescherming persoonsgegevens, Den Haag, oktober 2006.
ISBN-10: 90-74087-36-1
ISBN-13: 978-90-74087-36-0

COLLEGE BESCHERMING
PERSOONSGEGEVENS

Juliana van Stolberglaan 4-10
Postbus 93374
2509 AJ Den Haag
TELEFOON 070 888 85 00
FAX 070 888 85 01
E-MAIL info@cbpweb.nl
INTERNET www.cbpweb.nl

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotocopie, microfilm of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het College bescherming persoonsgegevens.

Ontwerp en opmaak: Proforma en de Stal, M. Monster
Druk: Deltahage bv

Voorwoord

RFID-toepassingen maken al geruime tijd deel uit van het dagelijks leven. Ze zijn er in vele soorten en maten. Er zijn handige toepassingen, zoals elektronische sleutels om autodeuren mee te openen of chips waarmee weggelopen huisdieren kunnen worden opgespoord. Er zijn geaccepteerde beslissingen, zoals toegangsbadges voor op het werk. Er zijn toepassingen die levensreddend kunnen zijn, zoals identificatiearmbandjes van patiënten in operatiekamers. Er zijn toepassingen die geld besparen, zoals bij het verbeteren van voorraadbeheer in de detailhandel. Er zijn toepassingen die beogen de openbare veiligheid te verhogen. Er zijn exotische toepassingen, zoals het laten implanteren van een chip om een VIP-behandeling in een uitgaansgelegenheid te verwerven.
Er zijn toepassingen die geen noemenswaardige problemen opleveren. Er zijn er ook, die baden in een aura van onontkoombaarheid en tot intense discussie leiden, zoals bij het paspoort. Ten slotte zijn er ook toepassingen die vooral door hun onzichtbaarheid als bedreigend worden gezien en waartegen mensen heftig in het geweer komen, zoals het door middel van in kleding ingeweven chips volgen van klanten.

Het College bescherming persoonsgegevens acht het daarom van groot belang dat de vraag, hoe om te gaan met ontwikkeling en toepassing van RFID, vooral met het oog op de implicaties van RFID-toepassing voor de persoonlijke levenssfeer, voorwerp is van studie en overleg in verscheidene fora, internationaal en nationaal. In Nederland zijn op dit terrein verschillende partijen actief. Een ECP.NL-werkgroep waarin marktpartijen, beleidsmakers, wetenschappers en belangenbehartigers vertegenwoordigd waren, heeft in 2005 de publicatie 'Privacyrechtelijke aspecten van RFID' uitgebracht.
Vanuit zijn specifieke rol als toezichthouder wil het CBP bijdragen aan de verdere voortgang van het debat.

refs

Op internationaal vlak heeft het CBP bijgedragen aan de meningsvorming over RFID door onderschrijving van het Sydney Statement, uitgebracht tijdens de conferentie in 2003 van privacytoezichthouders en door deelname aan de EU Artikel 29-werkgroep van toezichthouders. Deze werkgroep heeft de RFID-gerelateerde problematiek geïnventariseerd en geanalyseerd en buigt zich thans over begripsbepalingen die behulpzaam kunnen zijn bij het nader interpreteren van regelgeving.

Op nationaal vlak beoogt het CBP vanuit zijn toezichthoudende rol met het uitbrengen van deze publicatie aan te geven welke aspecten van RFID naar de mening van het CBP uit het oogpunt van gegevensbescherming aandacht, nadere studie en debat verdienen. Het gaat daarbij niet om het toetsen hoe 'RFID-proof' de Wet bescherming persoonsgegevens is of om het bepleiten van een nieuw of aangepast wettelijk kader. De nadruk in deze inbreng ligt op het onderkennen van de maatschappelijke voor- en nadelen van de techniek en het geven van aanzetten tot normontwikkeling. Is RFID veelbelovend of onverantwoord? Welke toepassingen kunnen wel, welke niet? Hoe moeten we verder met RFID?
Door te onderzoeken welke maatregelen kunnen leiden tot een verantwoorde omgang met RFID en welke van de betrokken partijen - of dat consumenten zijn of bedrijven, systeemontwerpers of de overheid - deze maatregelen het beste kunnen treffen, hoopt het CBP de discussie over RFID en persoonsgegevens verder te stimuleren.

Inhoud

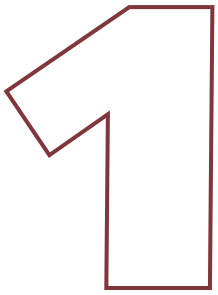
Samenvatting

De ontwikkeling van Radio Frequency Identification – RFID – is de afgelopen tijd in een stroomversnelling geraakt. De techniek maakt het mogelijk ongekend grote hoeveelheden data, waaronder persoonsgegevens, te genereren, op te slaan of anderszins te verwerken.
RFID heeft aanzienlijke implicaties voor de privacy en de privacybeleving en is daarom voorwerp van maatschappelijk debat. Met het uitbrengen van dit rapport wil het College bescherming persoonsgegevens de discussie over maatschappelijk verantwoord RFID-gebruik verder stimuleren.

De belangrijkste punten uit het rapport zijn:

- Samenwerking en kennisdeling tussen betrokken partijen – ontwerpers, toepassers, overheid en consumenten – is essentieel, nationaal en internationaal.
- Zet geen RFID in als dat niet hoeft. Als onvoldoende waarborgen bestaan tegen mogelijk nadelige effecten op de persoonlijke levenssfeer is RFID-gebruik af te raden.
- De drijfveer voor het huidige gebruik van RFID is vooral logistiek. De nadelen ontstaan doordat via de verkregen gegevens personen beoordeeld kunnen worden, vaak buiten hun medeweten. De belangrijkste waarborg om deze risico's te voorkomen of te verzachten moet worden gezocht in Privacy by Design. Bij het ontwerpen van applicaties en van infrastructuren dient van meet af aan rekening te worden gehouden met privacyrisico's.
- Voor zover RFID-toepassingen persoonsgegevens betreffen, is het bestaande juridisch kader van toepassing. Er zijn echter ook schemergebieden waarvoor normontwikkeling nodig kan blijken te zijn.
  Het te vroeg inzetten van nieuwe beperkende middelen kan verstikkend werken voor innovaties, het te laat inzetten daarvan tot onomkeerbare maatschappelijke nadelen.
  Gezien de snelheid waarmee RFID zich ontwikkelt, lijkt het voor het ontwikkelen van evenwichtige standpunten over de inzet van de techniek op dit moment verstandig vooral de nadruk te leggen op de mogelijkheden die Privacy by Design kan bieden voor het inbouwen van garanties voor verantwoorde toepassing.
- Alle partijen moeten weten waar zij goed aan doen in omgevingen waar RFID wordt ingezet en welke rechten, plichten en mogelijkheden voor hen gelden.
- Burgers hebben recht op informatie over toepassing van RFID en zouden waar redelijk over mogelijkheden moeten kunnen beschikken om al dan niet betrokken te worden bij RFID-verwerkingen. Hierbij valt te denken aan het kunnen kiezen voor een alternatief waarbij geen RFID wordt gebruikt of aan het kunnen verwijderen van tags.
  Zij dienen altijd inzage te kunnen krijgen in de met behulp van RFID over hen verzamelde gegevens. Voor misbruik of oneigenlijk gebruik van RFID moeten zij beschikken over een goede klachtregeling.
- Toepassers moeten bij het inzetten van RFID vooral aandacht besteden aan het uitsluiten van (privacy)risico's, zichtbaarheid, beveiliging en informatieverstrekking. Audits, gedragscodes en best practices kunnen hieraan bijdragen.
  Gewaakt moet worden voor cumulatie van gegevens. Datamininalisatie in de backoffice heeft een preventief belang.
- Overheden moeten er niet op uit zijn middels RFID over steeds meer gegevens te kunnen beschikken. De burger moet vertrouwen hebben in verantwoord RFID-gebruik door de overheid. De overheid moet zich als bijzondere toepasser bij uitstek verzekeren van optimale beveiligingsmogelijkheden. Zij heeft voorts een rol bij het stimuleren van kennisdeling en onderzoek, nationaal en internationaal, en bij publieksvoorlichting.
- Systeemontwikkelaars en ontwerpers van ICT-middelen moeten RFID-toepassingen niet alleen op technische aspecten toetsen maar ook op privacybestendigheid.

Maatschappelijke aspecten van RFID



RFID, een technologie die het mogelijk maakt om op afstand gegevens te lezen, neemt een grote vlucht. In dit hoofdstuk wordt kort ingegaan op de implicaties daarvan voor zowel de samenleving als geheel als voor individuen.

Radio Frequency IDentification is geen nieuw technisch snufje. De snel toegenomen toepassingsmogelijkheden ervan worden echter door velen met argusogen gevolgd. Waarom was die brede aandacht er niet toen de barcode zijn intree deed? Waarom stonden data-intensieve verwerkingen via draadloze communicatie niet in de schijnwerpers? Wat maakt RFID zo bijzonder? En vooral: waarom houden privacytoezichthouders zich ermee bezig?

RFID is de aanduiding van een technologie waarmee het mogelijk is om op afstand gegevens te lezen. De daarbij gebruikte gegevensdragers worden vastgemaakt aan het object waar de gegevens bijhoren. Dragers en hun antennes worden samen 'tags' genoemd. Zij kunnen zo klein worden uitgevoerd dat ze niet of nauwelijks meer te zien zijn.
Als het opgeslagen gegeven uniek is voor het bijbehorende object, wordt dat object via dit gegeven geïdentificeerd.
Het uitlezen van gegevens gebeurt met behulp van radiosignalen. Om de gegevens te kunnen lezen hoeven de gegevensdragers zich niet in het zicht te bevinden: het lezen kan bijvoorbeeld door andere materialen heen.

De natuurkundige principes die ten grondslag liggen aan RFID-systemen worden al decennialang toegepast. Wijdverbreid is het gebruik van een simpele vorm van de technologie in detectiepoortjes voor toegangscontroles en diefstalbeveiliging. De laatste jaren neemt de belangstelling voor toepassing van RFID op allerlei andere gebieden en in vele maatschappelijke sectoren sterk toe, aangejaagd door onder meer technologische veranderingen (waaronder de effecten van miniaturisering), resultaten op het gebied van standaardisatie van nummersystemen, interessante prijs-prestatieverhoudingen en het economisch succes van eerdere toepassingen. Belangstelling voor de inzet van RFID is er echter niet alleen van de zijde van toepassers. Ook partijen die zich richten op maatschappelijke en ethische aspecten van die toepassingen zijn geïnteresseerd.

1.1 Toepassingsgebieden

Een typisch gebruik van RFID ontstaat door afzonderlijke productexemplaren, bijvoorbeeld van consumentengoederen, via de gegevensdrager te voorzien van een uniek nummer ('itemized tagging'). Door dergelijke nummers op geschikte momenten van een afstand, desnoods groepsgewijs, uit te lezen, is het in beginsel mogelijk om deze productexemplaren gedurende hun gehele levenscyclus te volgen, van productie via voorraadbeheer tot verkoop en van gebruik tot destructie. Daardoor kunnen logistieke processen sterker worden geautomatiseerd en beter worden bewaakt, waarbij tevens garanties over herkomst en kwaliteit van elk product gegeven kunnen worden.

> "RFID has a lot of potential at the back end of retail operations to cut shrinkage, improve stock visibility and track shipments".
> *(Nick Gladding, senior onderzoeker bij detailhandelanalist Verdict, in IT Week, januari 2006)*

Het beheren van producten kan zelfs op huishoudelijk niveau gebeuren: apparaten kunnen besluiten nemen aan de hand van gegevens op tags. Een wasmachine kan het wasprogramma laten afhangen van gegevens die van tags in het wasgoed zijn gelezen. De opgeslagen gegevens kunnen ook anders worden gebruikt, bijvoorbeeld voor het geven van (product)-beschrijvingen ten behoeve van de consument. Voor zover gegevens horen bij verkochte producten kunnen ze, zeker als ze gerelateerd worden aan een gekende klant, gebruikt worden voor direct marketingdoeleinden.
RFID-toepassingen beperken zich niet tot de detailhandel. Ze kunnen branchespecifiek zijn, zoals het herkennen van boeken – per titel of per exemplaar - aan de hand van een RFID-

nummer. In openbare bibliotheken in Nederland worden RFID-tags al toegepast. Een ander voorbeeld is bagageafhandeling in luchthavens. Toepassingen kunnen ook algemeen van aard zijn, zoals het reguleren van toegang tot ruimtes.
Overheden kunnen gebruik maken van RFID-systemen, bijvoorbeeld om echtheidscontroles uit te voeren op bankbiljetten, of om voordeel te zoeken in het op afstand en gebruiksvriendelijk uitlezen van gegevens, bijvoorbeeld bij tolheffing.
RFID wordt niet alleen gebruikt voor producten of goederen. Ook de identificatie van personen – werknemers of uitgaanspubliek bijvoorbeeld – behoort tot de mogelijkheden.

Voorbeelden van RFID-toepassingen

Paspoort
Paspoorten en andere reisdocumenten worden op grond van een EU-verordening vanaf augustus 2006 voorzien van een beveiligd opslagmedium. Deze drager bevat biometrische en andere gegevens. Door in de toekomst het uitlezen van gegevens contactloos te laten plaatsvinden, ontstaan er geen problemen met het moeten afstemmen van de formaten van het paspoort en het leesapparaat en wordt slijtage voorkomen. Adequate beveiliging van de communicatie tussen het opslagmedium – de chip – en de lezer moet ervoor zorgen dat gegevens niet worden afgeluisterd.

Wal-Mart
Het Amerikaanse winkelbedrijf Wal-Mart Stores Inc. maakte in 2003 bekend dat het zijn honderd grootste toeleveranciers zou verplichten vanaf 2005 pallets en kratten die zijn bestemd voor distributiecentra, uit te rusten met RFID. Daardoor kan automatisch worden vastgesteld dat goederen (tijdig) zijn gearriveerd. Tevens is een beter voorraadbeheer mogelijk.

Medicijnen
Door medicijnen te voorzien van RFID-tags kunnen logistieke voordelen worden behaald en kan worden geborgd dat medicijnen de juiste bestemming bereiken. Mogelijkheden voor het vaststellen van de herkomst van een medicijn en voor betere controle van de houdbaarheid ervan leiden tot voordelen voor de patiënt. Die voordelen zijn alleen haalbaar als er een geschikte infrastructuur is voor het schrijven en lezen van tags.

Baja Beach
Bezoekers van de Baja Beach Club kunnen onderhuids een VIP-chip, een RFID-tag die is ondergebracht in een glazen capsule, laten aanbrengen, waardoor zij automatisch worden herkend. Door die herkenning krijgen deze bezoekers toegang tot VIP-ruimtes en kunnen zij hun consumpties afrekenen.

1.2 Invalshoeken

Er zijn verschillende benaderingen om RFID en RFID-toepassingen te bespreken.
Bij een *economische* invalshoek bijvoorbeeld kunnen kosten van implementatie, voordelen op het gebied van lokaliseerbaarheid van goederen of snelheid van distributie aan de orde komen. Wie vooral let op *gezondheid*saspecten van RFID-toepassingen kan niet alleen geïnteresseerd zijn in de effecten van de erdoor gebruikte radiosignalen, maar ook in toepassingen die streven naar kwaliteitsbeheersing van etenswaren of medicijnen. *Milieu-aspecten* komen aan de orde als men de levenscyclus van de gegevensdragers wil bestuderen bij massaal gebruik, of bij het inzetten van RFID ter verbetering van recycling. Waar de technologie gebruikt wordt voor het aantonen van echtheid en herkomst bestaan er raakvlakken met *opsporing* en *bestrijding* van productvervalsing. In scenario's waarin apparaten aan de hand van RFID-gegevens beslissingen nemen, kunnen *aansprakelijkheid*skwesties spelen.
Ethiek is een invalshoek, bijvoorbeeld waar tags gebruikt worden als implantaat voor dieren, zoals al geruime tijd gebeurt, of voor mensen, of bij de beoordeling van de (on)oorbaarheid van het heimelijk gebruik van de technologie.

Voor het CBP is het relevant om te kijken naar de gegevensverwerkingen die met RFID samenhangen.

1.3 Maatschappelijke waarden

Grootschalige inzet van nieuwe technologische middelen leidt vaak tot maatschappelijk debat. De voordelen van de techniek worden afgezet tegen mogelijke aantasting van maatschappelijke waarden en verworvenheden of sterker, tegen mogelijke schending van fundamentele rechten zoals het recht op privacy.
Bij RFID gaat het vooral om het ontstaan van een veelheid van gegevens. Ongerustheid over de privacy-implicaties van RFID-toepassingen kan in de weg staan aan geaccepteerd gebruik van de techniek, ook waar gepast vertrouwen op zijn plaats is.
Dat vertrouwen kan anderzijds ook ontstaan door op sommige gebieden RFID uitdrukkelijk niet toe te passen. Of zoals CBP-voorzitter J. Kohnstamm het in een interview verwoordde: "De samenleving bepaalt de grenzen, niet de techniek" (Automatisering Gids, 18 november 2005).

In deze studie wordt het woord *risico* gebruikt ter aanduiding van (dreigend) gevaar voor aantasting van rechten, verworvenheden en maatschappelijke waarden. Daarbij zal in belangrijke mate, maar niet uitsluitend, worden gedoeld op risico's die de technologie meebrengt voor de persoonlijke levenssfeer.

De mate waarin men effecten als nadelen beschouwt is geen constante in de tijd. Het gebruik van implantaten voor het kunnen herkennen van mensen was tien jaar geleden bijvoorbeeld nog ondenkbaar en zou daarnaast waarschijnlijk abject zijn gevonden. Tegenwoordig gebeurt het, zoals het Baja Beach Club-voorbeeld aantoont. Ook vergeetachtige personen die afhankelijk zijn van zorg en die bijvoorbeeld menen een reëel risico te lopen te verdwalen, kunnen besluiten zich te laten voorzien van een tag.
Voorts hangen oordelen over het gebruik van RFID af van de context. Het scannen van gedetineerden via enkelbandjes of van patiënten die uit de operatiekamer komen op mogelijk in hun lichaam achtergebleven operatie-instrumenten, levert doorgaans andere reacties op dan het via RFID verregaand controleren door de werkgever van zijn personeel.
Eenzijdige toetsing van RFID aan maatschappelijke waarden moet worden vermeden. Met (dezelfde) maatschappelijke waarden als norm zullen RFID-toepassingen zowel negatieve als positieve effecten hebben, direct of indirect.

1.4 Wolken van gegevens

Om aan te geven dat er in administraties veel gegevens zijn vastgelegd over personen, is wel het beeld gebruikt dat ieder van ons is omgeven door een wolk van gegevens.
Dit beeld wordt sterker nu RFID in steeds meer producten zal worden verwerkt, ook in kleding, zodat men ook letterlijk in toenemende mate is omgeven door gegevens, die door een ander kunnen worden uitgelezen.

De drijfveer voor het huidige gebruik van RFID is vooral logistiek. De nadelen van RFID-gebruik ontstaan doordat via de gegevens personen beoordeeld kunnen worden.
Bij het benoemen van risico's en het bespreken van mogelijkheden voor het beperken daarvan zal in deze studie de zorgvuldige omgang met (persoons)gegevens centraal staan. Dat gebeurt niet vanuit een juridische invalshoek. In deze fase van meningsvorming ligt het meer voor de hand de maatschappelijke effecten van RFID-gebruik als uitgangspunt te nemen.

dus geen discussie
over wat een persoonsgegeven is

1.5 Bedreigingen

Toepassing van RFID kan dankzij - of ondanks - de eenvoud ervan, leiden tot breed optredende voordelen en nadelen. Hoe een weging van voor- en nadelen in een concreet geval uitpakt, hangt in sterke mate van de context af.

Bij de verwerking van gegevens over meegedragen (consumenten)goederen is de vraag aan de orde of dit uitsluitend gebeurt door daartoe bevoegde partijen *(wie)*. Tevens moet worden nagegaan of partijen het lezen beperken tot de gegevens die voor hen bestemd zijn *(wat)*, of dit uitsluitend gebeurt onder omstandigheden waarin het kennisnemen van die gegevens passend is *(wanneer)* en om welke redenen het gebeurt *(waarom)*.

Zelfs als voldaan is aan de wettelijke vereisten voor de bescherming van persoonsgegevens, kunnen zich nadelen voordoen voor de persoonlijke levenssfeer. Niet altijd zijn er passende antwoorden op onderkende risico's. Daarnaast blijken technologieën *altijd* onvoorziene gebruiksmogelijkheden te genereren die tot eveneens onvoorziene risico's leiden. Voorts is misbruik niet uit te sluiten.

- RFID kan leiden tot mogelijk unfaire of onjuiste *beoordeling* (en navenante bejegening) van personen via de *door deze personen meegedragen goederen*. De aard van die goederen kan worden vastgesteld aan de hand van gelezen gegevens, zowel door organisaties (bijvoorbeeld een concurrerend warenhuis), door medeburgers (die daardoor bijvoorbeeld inzicht kunnen krijgen in gezondheid of maatschappelijke positie), als door overvallers (ten behoeve van 'slachtofferselectie').

algemeen = profiling/discriminatie (+ én -) aspect van privacy

> Hoe RFID-gebruik kan leiden tot ongelijke behandeling blijkt bijvoorbeeld uit het experiment van Gillette met RFID in de Britse supermarktketen Tesco in 2003. Klanten die een pakje scheermesjes oppakten, werden – als reactie op een signaal afgegeven door een in het pakje ingelijmde tag – gefotografeerd door een verborgen camera. Bij het afrekenen werd van hen opnieuw automatisch een foto gemaakt. Het beveiligingspersoneel kon met behulp van beide foto's potentiële winkeldieven scheiden van andere consumenten, zonder dat van diefstal sprake hoefde te zijn.

  Dergelijke beoordelingen vinden ook plaats in RFID-loze omstandigheden. Bijzonder aan de nieuwe technologie is onder meer dat er nieuwe mogelijkheden ontstaan ter identificatie, dat beoordelingen geautomatiseerd kunnen plaatsvinden en dat gegevens ook meegedragen goederen kunnen betreffen die normaliter aan het oog onttrokken zijn.

- Bij massale toepassing van de technologie kunnen, los van het ter plekke uitlezen van gegevens, bedreigingen ontstaan als gevolg van groei van de aantallen gegevensverwerkingen en hun omvang. Het koppelen van veel (product)gegevens aan een persoon kan leiden tot *gedetailleerde profilering en intensieve datamining*.

Men zou kunnen menen dat gegevens die via het vehikel RFID in backoffices zijn verzameld zich niet onderscheiden van op andere wijzen vergaarde data. Enige aandacht is toch gerechtvaardigd, omdat:

- producttype-informatie die afgeleid kan worden uit RFID-gegevens makkelijker kan worden verzameld, wat kan leiden tot gedetailleerde kennis over smaken en voorkeuren;
- informatie over aangeschafte productexemplaren (in tegenstelling tot producttypen) beschikbaar kan komen. Dit kan leiden tot gedetailleerdere kennis over smaken en voorkeuren, terwijl er ook nieuwe mogelijkheden tot identificatie bestaan, inclusief nieuwe mogelijkheden voor het relateren van productgebonden gegevens aan personen;
- het verzamelen van gegevens massaler zal plaatsvinden, waarbij door het standaardiseren van werkwijzen, productcodes en nummersystemen tevens meer informatie beschikbaar komt;
- het verzamelen van informatie heimelijk kan gebeuren.

→ tags zijn gelinkt via fysieke locatie / persoon!!

'Getting people to accept RFID was not going to be easy.
Did they take that as a sign to stop? Of course not. Rather than rethinking their spychipping plans, they did what powerful corporations do: They threw money at the problem. (.....) They conducted focus group research in North America, Europe and Asia for insights to help them manipulate public opinion and prevent a consumer revolt.
And what did the people they surveyed say? Not surprisingly, the studies reported that their "biggest concern" was abuse. Consumers feared they could be tracked through their clothing, spied on by corporations and governments monitoring their purchases, and taken advantage of by thieves secretly frisking them. (.....)
"I'd feel naked if people know what I'm wearing."
"I could be tracked by the clothes I'm wearing."
"Companies or the government will be able to monitor everything I buy and spy on me."
"Someone could see everything I buy by reading my trash."
"Muggers could know what is in my shopping bag or if I'm wearing a Rolex."
"The technology will improve to allow people to read through walls"'.
Uit: 'Spychips. How major corporations and government plan to track your every move with RFID' door Katherine Albrecht & Liz McIntyre, Nelson Current 2005, ISBN 1595550208

- *Onverwachte identificatie* kan ontstaan via het op afstand uitlezen van RFID-gegevens die een persoon bij zich draagt – bijvoorbeeld via een van een uniek nummer voorzien horloge – en die, tezamen of apart, binnen de context van een omgeving (warenhuis, stad, land,...) een voor die persoon unieke combinatie vormen. Het is denkbaar dat strategisch, in de openbare ruimte of elders, opgestelde RFID-lezers in staat zijn te volgen bij welke locaties deze unieke combinatie voorbijkomt.

- Bij brede toepassing kunnen betrokkenen, juist door het kleine formaat van tags en door het gemak waarmee deze kunnen worden uitgelezen, *het overzicht verliezen* over gegevensverwerkingen en over uitleesacties, waaronder heimelijke of 'per ongeluk' op afstand plaatsvindende. Detectiepoortjes op een station zouden bijvoorbeeld kunnen denken dat iemand met een ov-kaart op zak een reiziger is, terwijl hij in werkelijkheid iemand anders naar de trein brengt. Bepaalde handelingen die nu bewust uitgevoerd moeten worden – het in een betaalautomaat steken van een bankpas – zouden overgenomen kunnen worden door apparaten die op afstand lezen, als iemand per ongeluk te dicht bij dat apparaat staat.

- RFID-tags hebben, als ze niet afhankelijk zijn van een eigen stroomvoorziening, een onbegrensde levensduur. Eenmaal ingezet is het gebruik ervan nauwelijks terug te draaien. De *nadelen* die aan het gebruik ervan kleven, kunnen dan ook *blijvend* zijn.

- Iemands *autonomie* en *keuzevrijheid* kunnen worden *aangetast* als gegevens die op hem betrekking hebben op een bepaalde manier worden ingezet. Een voorbeeld: een leverancier van goederen doet een aanbieding met al dan niet beperkte keuzemogelijkheden. De betrokken klant weet niet in welke mate aan hem gekoppelde gegevens zijn gebruikt bij het opstellen van dit aanbod. Hij lijkt over bepaalde keuzemogelijkheden te beschikken, terwijl deze in feite door de leverancier al zijn ingeperkt. Als een dergelijke situatie zich voordoet voor belangrijke producten of het merendeel van diensten, verdwijnt de autonomie van de consument.

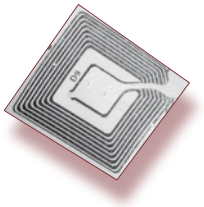
- De kans bestaat dat RFID-toepassing leidt tot *gevaar* – bijvoorbeeld als radiosignalen storingen veroorzaken in pacemakers of andere medische apparatuur.

Techniek en toepassingen

De maatschappelijke voordelen van RFID kunnen pas optimaal worden benut als de mogelijke nadelen van inzet van de technologie worden voorkomen of verzacht. Om een scherper beeld te krijgen van de aard en omvang van risico's van RFID wordt in dit hoofdstuk inzicht geboden in de daarvoor meest relevante aspecten van deze technologie en de toepassingen ervan.

RFID is een naam voor een technologie, of liever voor een verzameling technologieën, waarmee het mogelijk is om draadloze communicatie over korte afstand te realiseren.
Bij RFID-toepassingen worden gegevens vastgelegd op een tag. Een tag is een gecomputeriseerd 'identificatieplaatje'. Het is nauwkeuriger te spreken van een transponder, een hardware-elementje dat in staat is te *trans*mitten en te res*ponden* nadat het door een specifiek signaal is geactiveerd. Deze transponder bevat een halfgeleiderchip waarop de gegevens zijn opgeslagen en een, verhoudingsgewijs grote, antenne in de vorm van een spoel of strook metaal, waarmee via radiosignalen de communicatie met een leesapparaat tot stand wordt gebracht. Dit apparaat, de lezer *(reader)*, dat via radiogolven met de tag in verbinding staat, gebruikt men om gegevens op de tag uit te lezen of te veranderen. Het uitlezen van de tags kan *real time* en groepsgewijs. De gegevensuitwisseling verloopt zonder dat de tag in het zicht hoeft te zijn. Tags kunnen zeer klein zijn, niet groter dan tienden van een vierkante millimeter, en zeer dun, en zodanig verwerkt worden, in stof of in papier bijvoorbeeld, dat zij niet met het blote oog zichtbaar zijn. Nadat gegevens zijn uitgelezen kunnen ze met behulp van andere technologieën verder worden verwerkt of over grotere afstanden worden verzonden.

2.1 Soorten RFID-tags



Langdurig geldende uitspraken over RFID zullen niet moeten afhangen van technologische specificaties die op enig moment gelden. Het lijkt daarom nauwelijks zinvol om op de hoogte te zijn van de thans voorkomende soorten RFID-tags. Door het onderscheiden van soorten kan echter wel vanuit de optiek van de bescherming van persoonsgegevens een scherper beeld ontstaan van de aard en omvang van daaraan verbonden risico's. De volgende indelingen zijn daarvoor relevant.

Actieve en passieve tags onderscheiden zich door de energievoorziening.
Passieve tags hebben geen eigen energiebron. Zij verkrijgen hun energie uit de radiogolven waarmee ze uitgelezen worden Het signaal overbrugt een afstand variërend van enkele centimeters tot enkele meters. Als op passieve tags meer data moeten worden verwerkt, kost dat ook meer energie, wat ten koste gaat van de leesafstand. Dit soort tags kan bijvoorbeeld aan kledingstukken worden gehecht.
Actieve tags hebben een eigen energiebron in de vorm van een batterij en kunnen daardoor, zonder dat een lezer daarom vraagt, 'initiatieven nemen' tot het verzenden van gegevens. Hierbij kan men denken aan het doorgeven van voorraadinformatie aan een bedrijfsleider. Het bereik van actieve tags varieert van zo'n honderd meter tot enkele kilometers.
Er bestaan ook semi-actieve tags, maar deze vergen voor dit discussiestuk geen afzonderlijke aandacht.

Verder is er verschil te maken naar de *lees- en schrijfmogelijkheden* van de tag. Hier worden onderscheiden

- alleen lezen (*Read Only*): de tag is tijdens de fabricage voorzien van een niet te wijzigen code. Dit type tags wordt in detailhandelketens gebruikt;
- eenmalig schrijven (*WORM,* oftewel *Write Once Read Many*): het geheugen van de tag kan door de toepasser eenmalig voorzien worden van gegevens (of van een programma) en kan daarna niet meer worden gewijzigd. Toepassingen zijn bijvoorbeeld verwerking in toegangskaarten, bibliotheken, toegangscontrolesystemen of bagageafhandelingssystemen;
- herschrijfbaar *(ReadWrite)*: het geheugen van de tag kan herhaaldelijk beschreven worden, steeds met andere waarden.

Herschrijfbare tags vragen om een andere behandeling en vergen andere waarborgen dan alleen lezen-tags, zeker wanneer gegevens zoals naam of nationaliteit op de tag worden vastgelegd. Bij het ontwerpen van waarborgen moet erop worden gelet dat de partij die op de tag

mag schrijven de mogelijkheid moet hebben gegevens op de tag bij te werken of gegevens toe te voegen, maar ook, dat gegevens op de tag niet door onbevoegden kunnen worden veranderd.

Een ander onderscheid valt te maken naar de *intelligentie* van de tag. Tags kunnen behalve van data ook worden voorzien van programma's. Het begrip 'smart label' wordt gebruikt voor een tag die niet meer kan dan een onveranderbare code opslaan en deze op verzoek vrijgeven aan een lezer, te vergelijken met een barcodelabel die is voorzien van een RFID-transponder. De kwalificatie *smart* duidt dan op het vermogen om een code op te slaan en om te communiceren met de lezer.
Naarmate de tag intelligenter is, heeft hij in de regel een grotere opslagcapaciteit en ruimere mogelijkheden om berekeningen uit te voeren. De rekenkracht kan dan bijvoorbeeld worden gebruikt voor het controleren van een biometrisch gegeven of het ontsleutelen van gegevens, die versleuteld zijn vastgelegd om te voorkomen dat iedereen er kennis van kan nemen. Zo'n intelligentere tag krijgt dan de eigenschappen van een 'smart card'. Dergelijke kaarten kennen wij nu in de vorm van bankpasjes of SIM-kaarten. Daarvan bepaalt de houder echter zelf of hij die gebruikt of niet. Bij een tag kan het aflezen ook onverwacht van een afstand gebeuren.

2.2 Gegevens

De gegevens op de tag kunnen dienen als (sleutel tot) informatie over het object waar de tag aan is bevestigd of in is verwerkt. Toepassers zijn vrij hun eigen codes te gebruiken. Sommige RFID-toepassingen ontlenen hun kracht aan de totstandkoming van een verregaande standaardisering van artikelnummers. Als nummers gestandaardiseerd zijn, kan iedere groothandel, afnemer en klant aan de hand van zo'n door de fabrikant aangebracht nummer voor hem relevante informatie over het product ophalen. Een groothandel wil bijvoorbeeld weten waar en wanneer het product is gemaakt, een afnemer wil informatie over de fabrikant en over de nog beschikbare voorraad en een klant in de winkel kan belangstelling hebben voor beschikbaarheid van maten, een kleurbeschrijving of wasinstructie. Fabrikanten kunnen met behulp van tags die informatie in één keer wereldwijd verstrekken. Bij het taggen van goederen zal echter niet in alle gevallen gebruik worden gemaakt van wereldwijd unieke productcodes.

Bijzondere aandacht in het kader van standaardisatie verdient de Elektronische Productcode (EPC), ontwikkeld door het EPCglobal Network, een organisatie die ten behoeve van fabrikanten werkt. De EPC biedt een standaard voor het nummeren van productexemplaren. Hoe deze coderingsstandaard er in detail uit komt te zien is minder van belang, wel is relevant dat door de standaardisering op zichzelf al risico's kunnen ontstaan:

- Door de standaardisatie kan aan productcodes een vaste betekenis worden toegekend. Via raadpleging van – breed toegankelijke – catalogi van fabrikanten of groothandelaren waarin die betekenis van nummers is vastgesteld, ontstaat uit de gegevens op de tag informatie, die overal ter wereld ingezet kan worden, eventueel bij het – commercieel – beoordelen van personen in een niet voorziene context. Stel dat iemand een luxe-artikel heeft gekocht dat blijvend is voorzien van een RFID-tag. In beginsel kan door het uitlezen van de code op een tag via de catalogi worden vastgesteld in welke mate het bijbehorende artikel een luxe-artikel is. Daaruit kunnen, ook in andere winkels, conclusies worden getrokken over de welstand van de drager. Lees voor 'luxe-artikel' in deze context 'bankbiljet' en het wordt duidelijk waarom het voorzien van bankbiljetten van slecht beveiligde tags in het voordeel kan zijn van straatrovers die met een RFID-lezer op zoek zijn naar slachtoffers.
- De standaardisatie zorgt ervoor dat nummers ongeacht de context wereldwijd hun unieke, identificerende karakter behouden. Via de identificatie van goederen kunnen identificaties van personen ontstaan. Een persoon die voortdurend een artikel meedraagt, zoals een polshorloge dat is voorzien van een makkelijk uitleesbaar wereldwijd uniek nummer, is in beginsel wereldwijd herkenbaar aan dat nummer. Daardoor kan deze persoon worden gevolgd en kunnen te pas en te onpas gegevens aan hem worden gerelateerd op basis waarvan hij kan worden beoordeeld.

tag zegt iets over drager, bijvoorbeeld smaak of levensstandaard

Gegevens kunnen worden onderscheiden in *objectgebonden gegevens* en *persoonsgebonden gegevens*. Objectgebonden gegevens hebben als doel om, binnen een bepaalde context, een object (of product) te identificeren. Daarbij kan het gaan om gegevens die door een fabrikant aan zijn producten worden gekoppeld, zonder dat er nog sprake is van een koppeling naar een persoon. Objectgebonden gegevens kunnen evenwel 'verworden' tot gegevens die iets zeggen over een persoon. Een voorbeeld: een fabrikant heeft door zijn producten van een RFID-tag te voorzien louter de intentie die producten te beschrijven. Voor de koper van dat product kan de aanwezigheid van zo'n tag invloed hebben op de manier waarop hij in het maatschappelijk verkeer wordt beoordeeld door een partij die de tag heeft uitgelezen.
Iedereen die beschikt over de technische middelen om tags te lezen kan proberen om de gegevens te lezen van tags die een persoon die voor hem staat bij zich draagt. Als deze gegevens onvoldoende zijn afgeschermd kan een uitlezende partij die weet wat codes op een RFID-tag betekenen daarmee bijvoorbeeld ontdekken dat die persoon een bepaald medicijn bij zich heeft, een artikel dat verkocht wordt door een concurrent bij zich draagt of liefhebber is van een specifiek literair genre. Deze kennis kan doorwerken in de bejegening of beoordeling van deze persoon.
In de categorie persoonsgebonden gegevens vallen gegevens die van meet af aan iets over een persoon zeggen, zoals gebruikt in bijvoorbeeld het paspoort of in betaalsystemen.
Een verdere opdeling naar direct identificerende gegevens en overige is niet zinvol. Of gegevens direct identificerend zijn, hangt sterk af van de context en van de mogelijkheden van de waarnemer.

Ook als we het gebruik van RFID bij dieren geheel buiten beschouwing laten, blijven er RFID-gegevens die in geen van beide categorieën vallen, zoals gegevens waaruit alleen typeinformatie kan worden afgeleid. Ook kunnen de soorten gegevens elkaar overlappen, bijvoorbeeld als RFID wordt ingezet voor het herkennen van een identificatiemiddel. Desondanks geeft het onderscheid objectgebonden – persoonsgebonden houvast bij het later benoemen van aandachtspunten.

2.3 Communicatietechnologie

In de eerste toepassingen van RFID, waaronder het merken van dieren of goederen voor transportdoeleinden, speelde privacy in het geheel geen rol. In de protocollen die daarvoor werden opgesteld, waren dan ook geen confidentialiteitswaarborgen ingebouwd. Alle gegevens konden door iedere langskomende lezer worden uitgelezen. Deze protocollen worden ook nu nog gebruikt.
De mogelijkheden om gegevens af te schermen, ontwikkelen zich. Om te voorkomen dat gegevens door iedereen kunnen worden uitgelezen, kunnen communicatieprotocollen worden voorzien van stappen voor authenticatie en voor ontsleuteling van gegevens. Of er in RFID-toepassingen voldoende aandacht wordt geschonken aan gegevensafscherming, wordt onder meer bepaald door economische motieven.
Bij het afschermen moet niet alleen worden gelet op het afschermen van gegevens op de tag, maar ook op het afschermen van het radioverkeer tussen lezer en tag en tussen tag en lezer.

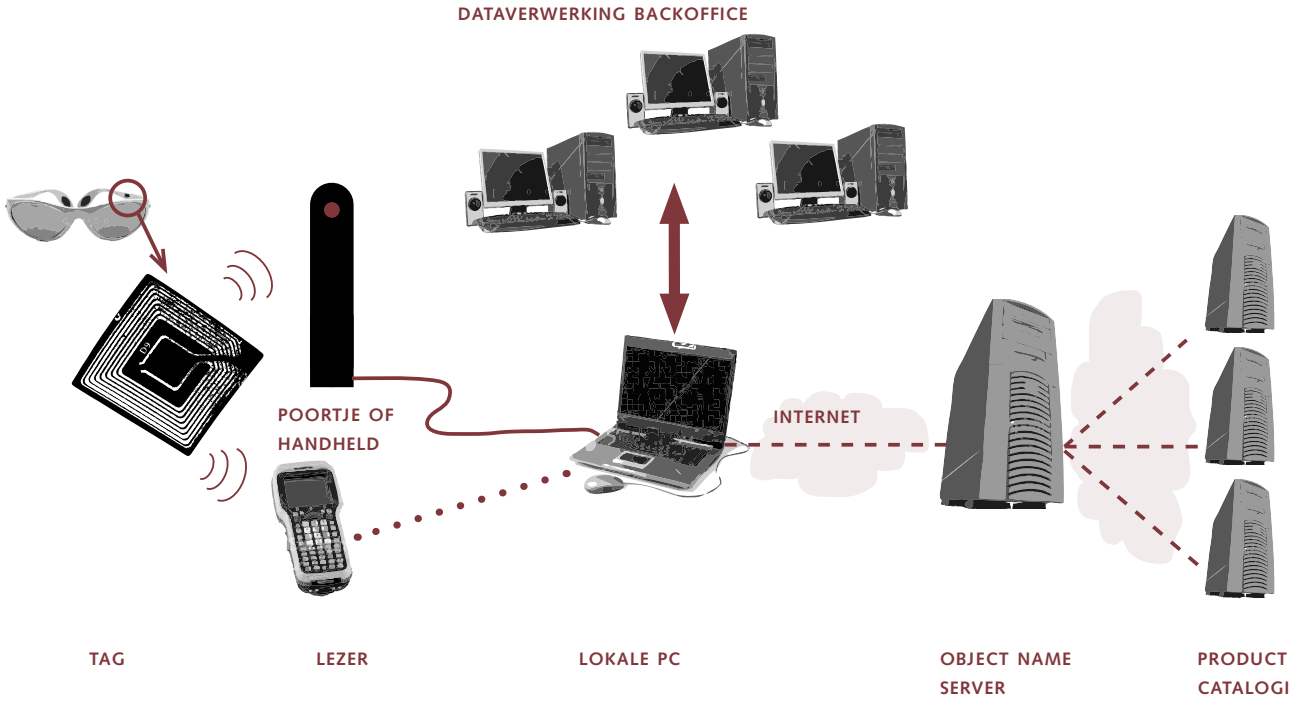
Zwaktes in de communicatietechnologie kunnen onbedoeld mogelijkheden bieden om gegevens op een tag te veranderen.

Risicobeheersing wordt zowel in positieve als in negatieve zin beïnvloed door standaardisering op het gebied van de protocollen die nodig zijn voor het uitwisselen van gegevens (gestreefd wordt naar interoperabiliteit). Positief omdat door standaardisering ook standaards voor adequate beveiliging kunnen ontstaan, negatief omdat ontdekte zwaktes zich breed zullen manifesteren.

Een ander relevant aspect voor het werken met radiosignalen is interferentie: radiosignalen kunnen elkaar verstoren. Hoewel RFID-toepassingen met zwakke signalen werken, kunnen bij massale toepassing personen via meerdere RFID-signalen worden bevraagd. Als het gaat om voor die personen vitale (zorg)toepassingen kunnen interferenties tot serieuze problemen leiden. Het zou denkbaar zijn dat juist op dit terrein wordt nagedacht over regulering.

2.4 Architectuur

Dit plaatje toont een typische RFID-verwerking op het gebied van consumentengoederen. Andere toepassingen, zoals paspoortverificatiesystemen, werken overigens op vergelijkbare wijze.



De catalogi kunnen aan de hand van een nummer op de tag, via het internet, informatie over het product verschaffen. Zij kunnen zich bevinden in de domeinen van fabrikanten, groothandelaren en zo meer.
Om aan de hand van een code op een tag te achterhalen welke informatie bij de code hoort is standaardisatie nodig. Deze standaardisatie betreft codes, systemen om gegevens op te slaan en protocollen om de bij een RFID-nummer behorende informatie te achterhalen. In het door EPCglobal Network ontwikkelde stelsel van afspraken is voorzien in een Object Name Server, die tot taak heeft om aan de hand van een EPC-nummer te achterhalen wáár op het netwerk zich de informatie bevindt die hoort bij het door het nummer aangegeven product.

2.5 Karakteristieken

De groeiende aandacht voor de maatschappelijke effecten die RFID kan hebben, wordt veroorzaakt door een samenloop van karakteristieken. Inzicht erin kan helpen bij het aangeven van voor een context typische bedreigingen en bij het vinden van tegenmaatregelen.

	karakteristiek	door	kan leiden tot	opmerkingen
1	massaal toegepast	functionele baten, prijsstelling en implementatiegemak	intensieve gegevensverwerkingen	goedkope RFID-tags hebben minder mogelijkheden tot data-afscherming
2	minuscuul	technologische verbeteringen	onzichtbaarheid en ongemerkt gebruik	tags kunnen in materialen verwerkt worden
3	interoperabel	standaardisatie van codes, protocollen en apparatuur	uitgebreidere mogelijkheden tot het verzamelen en vergelijken van gegevens	- standaardisatie in het bijzonder van (unieke) productnummers - verregaande standaardisatie zal leiden tot dalende productiekosten en daardoor tot een nog breder gebruik van tags
4	contactloos uitleesbaar, over afstanden groter dan enige decimeters	technische verbeteringen (ook waar het uitleesapparatuur betreft)	afluisteren	leesafstand sterk afhankelijk van gebruikte technologie
5	uitleesbaar zonder in zicht te zijn	gebruik radiogolven	stiekem uitlezen en moeizamer afscherming	
6	groepsgewijs uitleesbaar	technologische opzet	snelle gegevensverwerking	
7	lange levensduur	externe energievoorziening	blijvende risico's	levensduur is in theorie onbeperkt

Nog niet alle tags kunnen met eenzelfde lezer worden gelezen en verder zijn er uitleesbeperkingen, niet alleen door afstand, maar ook omdat RFID-systemen elkaar kunnen storen en omdat lezers bij het uitlezen van gegevens over een grotere afstand wel degelijk een bepaalde positionering ten opzichte van de tag moeten hebben. Maar de voordelen die de techniek nu al biedt, zorgen voor steeds meer toepassingen in allerlei branches en voor allerlei doeleinden. Risicoverhogende omstandigheden zijn er ook: doordat zowel de tag als de lezer zo geplaatst kunnen worden dat ze niet of nauwelijks te zien zijn, is het mogelijk tags ongemerkt te laten uitlezen.

Het is duidelijk dat het bij RFID om méér gaat dan om digitalisering van de streepjescode. Vooral door de combinatie van karakteristieken is de aandacht voor privacyaspecten nu ook groter dan bij toepassingen van andere technologieën om op afstand gegevens uit te lezen.

Een blik in de toekomst: het Internet der Dingen
Bij wijze van intermezzo kijken wij vooruit. Door initiatieven van grote detailhandelaren zullen RFID-toepassingen in logistieke processen en voorraadbeheer gemeengoed worden. Daarbij zal meer behoefte ontstaan aan interoperabiliteit en standaardisatie. Door grootschaliger gebruik zullen er technische aanpassingen aan systemen nodig zijn, zowel in technische als in organisatorische zin. Te verwachten is dat daarbij RFID-data in toenemende mate geïntegreerd worden met andere data.

Ook in andere sectoren, op het werk en thuis zal van RFID gebruik gemaakt worden, bijvoorbeeld voor het monitoren van de kwaliteit van producten of in toepassingen voor zorg op afstand. Daarbij zal het steeds vaker mogelijk worden actieve tags in te zetten.
Gebruiksomgevingen van RFID zullen steeds moeilijker van elkaar zijn te scheiden. De grens tussen een thuisomgeving en een werkomgeving zal steeds diffuser worden. Ook zullen RFID-applicaties hun taken steeds meer autonoom uitvoeren en zal er minder controle mogelijk zijn over de gegevens.

Het idee dat maatschappelijke effecten van RFID in steeds sterkere mate voelbaar zullen zijn, wordt versterkt door de verwachting dat zich een Internet der Dingen zal ontwikkelen, waardoor niet alleen logistieke stromen steeds zelfstandiger worden, maar waarin ook de omgeving van de mens in sterke mate kan worden geautomatiseerd. Dit Internet der Dingen staat daarbij voor de toekomst van communicatie en gegevensverwerking: het (via RFID) identificeren van objecten gecombineerd met het inzetten van bewegingssensoren en het via zeer kleine computersystemen verwerken van gegevens over die objecten, leidt in deze visie tot een omgeving waarin objecten zelf acties ondernemen, variërend van het aangeven van een vervangingsmoment tot het kiezen van een route in een logistiek systeem en het verzenden van berichten aan de ontvanger. Als bijvoorbeeld het laatste pak melk uit de ijskast is gehaald, dan kan die ijskast zelf nieuwe pakken melk 'bestellen'. In een verdergaande vorm wordt massale toepassing voorzien van micro-elektronische sensoren die allerlei veranderingen (bijvoorbeeld in temperatuur, positie, vochtigheid etc.) kunnen detecteren en die via radiosignalen kunnen communiceren met andere sensoren en apparaten, bijvoorbeeld om informatie over de veranderingen door te geven. In een scenario waarin zulk 'smart dust' de hoofdrol speelt, is sprake van een omgeving waarin ook mensen bij voortduring door hun omgeving – een 'smart environment' – gemonitord worden.

2.6 Hoe alert moeten we zijn?

Ook nu wij nog niet in een 'smart environment' vertoeven, geven publicaties over 'RFID en privacy' blijk van zorg. Hoe terecht die zorg is zou men kunnen afmeten aan scenario's waarin *denkbare* bedreigingen geschetst worden. Een andere weging ontstaat als men let op het *actualiteitsgehalte* van toepassingen en het (technisch/organisatorische) *realiteitsgehalte* van geschetste bedreigingen. Bedreigingen kunnen ontstaan wanneer RFID-toepassingen juist beogen inbreuk te maken op een maatschappelijke waarde, maar ook kan er, gelet op de beperkte ervaring met de technologie, sprake zijn van 'onbewust verkeerd' gebruik.

Zelfs verantwoorde toepassingen, uitgevoerd op verantwoorde wijze, kunnen leiden tot ongerustheid, bijvoorbeeld vanwege de vrees dat in de loop der tijd 'creatief ' (buitencontextueel) gebruik van gegevens zal ontstaan, hetzij van gegevens waarover een RFID-toepasser 'toch al' beschikt, hetzij van gegevens die deze al te gemakkelijk kan verkrijgen door het uitlezen van tags.
Vertrouwen in de technologie moet daarom niet alleen ontleend worden aan maatregelen tegen ongepast gebruik van de technologie, maar ook aan maatregelen tegen nevengebruik van gegevens.

RFID en bedreigingen gaan niet hand in hand

Het gebruik van RFID voor het op afstand uitlezen van gegevens is staande praktijk, ook waar het persoonsgegevens betreft. Toch doen bedreigingen voor de persoonlijke levenssfeer zich niet bij alle RFID-toepassingen voor. RFID kan bijvoorbeeld ingezet worden voor routering, kwaliteits- of echtheidscontrole zonder dat een relatie met een persoon is te leggen. Ook als zo een relatie wel bestaat – bijvoorbeeld bij de echtheidscontrole van een bankbiljet dat door een gekend persoon wordt overhandigd - is niet per definitie sprake van een inbreuk op de privacy. Wie een analyse wil maken van de voor- en nadelen van RFID-toepassingen, moet zich realiseren dat er verschil is tussen het beoordelen van een toepassing en van het beoordelen van de (privacy)effecten van RFID-gebruik.

Niet alle nadelen die zich voor kunnen doen bij RFID-toepassingen hebben hun oorzaak in die technologie:

- sommige bedreigingen zijn helemaal niet specifiek voor de RFID-technologie en doen zich ook voor als men een andere technologie zou hebben gebruikt, zoals barcodes, magneetstrips of smart cards;
- sommige bedreigingen ontstaan niet zozeer door de RFID-technologie *op zichzelf* maar eerder door de erdoor aangejaagde productexemplaarnummering;
- sommige bedreigingen ontstaan door het intensieve gebruik van RFID-gegenereerde gegevens in backoffices.

Commentatoren maken niet steeds duidelijk welke aan RFID toegeschreven risico's inderdaad in verband staan met specifieke (en zo ja welke) karakteristieken van deze technologie.
De observatie bijvoorbeeld dat alleen gebruikers van een klantenkaart met RFID in aanmerking komen voor het genieten van bepaalde voordelen, zoals het krijgen van korting, waardoor het afzien van gebruik van een dergelijke kaart geld kost, geldt ook voor een RFID-loze klantenkaart.
In andere gevallen richten bezwaren zich tegen het op afstand uitlezen van gegevens in het algemeen, wat een veel breder (beveiligings)onderwerp is, of tegen de nadelen van het centraal verzamelen van persoonsgegevens.
Wie RFID wil becommentariëren, zal dus bij de bespreking van de oorzaak van bedreigingen onderscheid maken naar soorten toepassingen.

Dat de aantrekkingskracht van RFID er toe kan leiden dat er voor toepassing van die technologie gekozen wordt, terwijl er vanuit maatschappelijk oogpunt, maar soms ook voor degene die de technologie aanwendt, betere alternatieven voorhanden zijn, is nauwelijks meer een eigenschap van RFID te noemen.

Bovenstaande opmerkingen laten onverlet dat toepassingen van de technologie leiden tot ongerustheid, niet alleen gericht op het heden, maar vooral gericht op de toekomst, bij een verdere robotisering van onze omgeving.

Realiteitsgehalte van bedreigingen
Sommige handelwijzen die als bedreiging worden gezien zijn theoretisch denkbaar, maar praktisch moeilijk uitvoerbaar. Om te voorkomen dat er bij het beoordelen van risico's wordt uitgegaan van onrealistische scenario's, moet men een beeld hebben van de (technisch/organisatorische) realiteitswaarde van bedreigingen (er wordt bijvoorbeeld verschillend gedacht over de mogelijkheden personen te volgen via de gegevens die verkregen worden uit RFID-tags die zij bij zich dragen) en evenzeer van voorgestelde technische en organisatorische beschermingsmaatregelen.
Het vergroten van publieke kennis over de (on)mogelijkheden van RFID-toepassingen kan bijdragen aan het vertrouwen in verantwoorde toepassingen en tegelijkertijd aan het tijdig treffen van maatregelen ter voorkoming van nadelige effecten.

Actualiteitsgehalte van bedreigingen
Zelfs als men de aandacht richt op realistische, technisch duidelijke, specifieke applicaties zoals het itemized taggen in detailhandelketens, blijkt het moeilijk te zijn het actualiteitsgehalte van scenario's te schatten. Lag tot voor kort de nadruk op tagging van pallets, nu lijkt de focus te verschuiven naar itemized tagging. Het zal nog enige jaren duren voordat itemized tagging betaalbaar is.

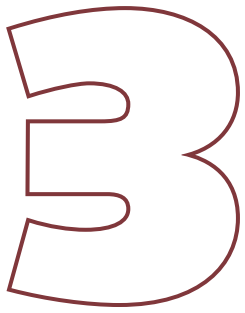
> Despite the high percentage growth rate, "item-level tagging will be rolled out slowly", says VDC's Michael Liard. "Current implementation costs - particularly tag prices - are simply too high for widespread adoption".
> *Onderzoeksgroep VDC,USA, www.mmh.com/article/CA6332917.html*

Er zijn daarbij organisatorische barrières, zoals het realiseren van een wereldwijd vernieuwd productnummersysteem of het tot stand brengen van samenwerking en economische barrières – waar de barcode goed voldoet en RFID geen meetbare meerwaarde heeft, zal invoering trager verlopen. Wanneer deze barrières, die aan een brede toepassing in de weg staan, opgeheven zullen worden, is nog niet te zeggen. Evenmin valt te zeggen in welke mate veronderstelde risico's zich daadwerkelijk zullen voordoen en in welke mate er in dat geval beschermingsmaatregelen nodig zullen zijn.
Dat neemt niet weg dat RFID in rap tempo aan populariteit wint. Thans nog niet haalbare toepassingen zullen binnen korte tijd realiteit blijken te zijn. Sommige bedreigingen manifesteren zich ook nu al.

"Already profitable for most suppliers, item-level tags and systems will be the world's largest RFID market by value from 2007 forwards. The market for item-level RFID tagging is forecast to rocket from $ 0.16 billion in 2006 to $ 13 billion in 2016 for systems including tags. In 2006, 0.2 billion items will be RFID tagged worldwide. In 2016, 550 billion items may be RFID tagged."
Dr Peter Harrop, in de nieuwsbrief Medical Technology Business Europe, augustus 2006.
www.mbteurope.info/content/ft608001.htm

Zichtbaarheid van bedreigingen
Stiekeme toepassing van RFID is een bron van zorg. Bij het leveren van commentaar op gebruik van RFID moet niet alleen aandacht worden geschonken aan de door de toepassers van de technologie beoogde verantwoorde effecten. Er moet ook aandacht worden besteed aan RFID-applicaties waarin geen rekening is gehouden met maatschappelijk nadelige effecten of het inbreuk maken op grondrechten, zoals privacy, of aan applicaties waarbij het maken van die inbreuken de opzet is.

Typen RFID-toepassingen

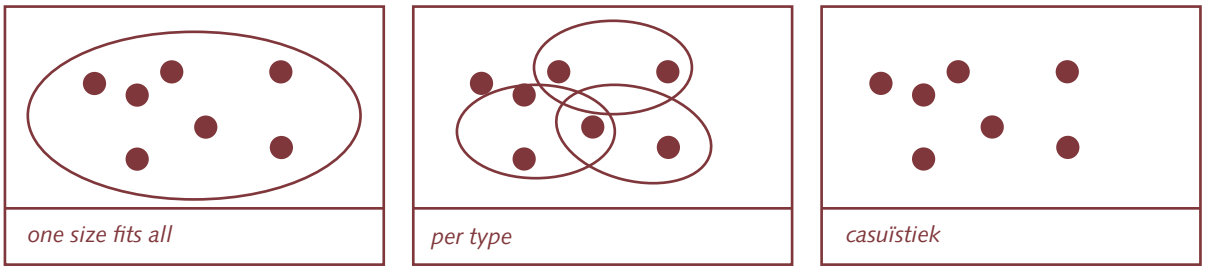


Het onderkennen en becommentariëren van privacyaspecten van RFID-systemen dwingen tot het hanteren van een typologie van systemen. Anders zou, gelet op de grote verscheidenheid van verschijningsvormen van de technologie en van RFID-toepassingen, een schier eindeloze reeks van besprekingen nodig zijn.

Er zijn verschillende uitgangspunten mogelijk bij het typeren van RFID-gebruik. De nadruk kan bijvoorbeeld liggen op de technische karakteristieken, op de soorten RFID-toepassingen, op de omgeving waarin de technologie functioneert, of op de mate waarin zij een directe relatie heeft met de persoonlijke levenssfeer. Het benoemen van verschillende kenmerken kan houvast bieden bij het onderkennen van bedreigingen die RFID meebrengt en bij het treffen van maatregelen.

Het belang van een typologie

Een 'one size fits all' beoordeling dicht aan iedere RFID-applicatie dezelfde maatschappelijke risico's toe. Die benadering ziet over het hoofd dat de mate waarin risico's zich voordoen van geval tot geval verschilt. Risico's hangen niet alleen af van gegevens op de tag, maar ook van ontwerpbeslissingen – bijvoorbeeld over de uitleesbaarheid van gegevens – evenals van waarborgen die bijvoorbeeld voortvloeien uit voorlichting.
Een ander uiterste zou zijn een casuïstische benadering, waarin per toepassing een risicobeoordeling wordt gegeven. Uit de gevallen wordt dan lering getrokken voor een volgende beoordeling.



a Technische karakteristieken alleen onvoldoende

RFID-tags bestaan in vele soorten, elk met zijn eigen mogelijkheden op het gebied van opslagcapaciteit, gebruikte uitleesfrequentie, de geschiktheid om in een bepaalde omgeving te functioneren, de afstand waarop gegevens uitleesbaar zijn, en zo meer. Zoals in het vorige hoofdstuk al ter sprake kwam, is het gelet op de snelle technologische ontwikkelingen nauwelijks zinvol om bij besprekingen van risico's de (ontwikkelingen in de) technische karakteristieken van de tag, bijvoorbeeld de afstand waarop gegevens uitleesbaar zijn, als uitgangspunt te nemen. Bovendien worden bedreigingen die worden veroorzaakt door een karakteristiek van een individuele tag soms afgezwakt door (andere) karakteristieken of door de aanwezigheid van meerdere tags. Het is bijvoorbeeld niet gemakkelijk om een tag van een specifiek individu in een groep van RFID-bezitters uit te lezen. Ook is het lastig te bepalen bij welke persoon een gelezen tag hoort.
Het risico van het aldoor uitlezen van tags door verschillende partijen wordt verkleind doordat RFID-systemen kunnen interfereren, zowel als er één RFID-systeem is dat met (te veel) tags moet werken als wanneer lezers met tags van verschillende RFID-systemen geconfronteerd worden. Tegen sommige bedreigingen vormt massale toepassing van RFID in zekere mate een bescherming.

is dit wel zo ? ⇒

Het lijkt beter om in plaats van naar de technische karakteristieken te kijken naar de omgeving waarin een RFID-systeem zou moeten functioneren. Afhankelijk van de omstandigheden kunnen eisen worden gesteld aan de architectuur van en de middelen waarmee het systeem gerealiseerd wordt, onder meer via de specificaties van de in te zetten tags, waarvoor kan gelden dat ze uitgeschakeld moeten kunnen worden.

b Andere indelingen succesvoller

Een typologie kan ook gevonden worden via het benoemen van de partijen die betrokken zijn bij een RFID-toepassing. Op die wijze komt tot uitdrukking dat maatschappelijke effecten van een technologie een relatie hebben met machtsverhoudingen.
Men kan dan kijken naar toepassingen waarin de verhouding overheid-burger speelt, of zorgverlener-patiënt, werkgever-werknemer of 'gewone' burgers onderling, bijvoorbeeld door te bespreken welke mogelijkheden een individu nog heeft bij de keuze om wel of niet mee te doen aan het gebruik van de technologie. Het belang van die keuze wordt beïnvloed door het vertrouwen dat er in het verantwoorde gebruik van RFID bestaat.

Een indeling die gebaseerd is op soorten toepassingen is een gelijkwaardig alternatief, omdat er een sterke relatie is tussen soorten toepassingen en de partijen/betrokkenen die daarvan gebruik maken. Daarbij kunnen zich interessante situaties voordoen: waar in de verhouding bedrijfsleven-consument normaliter keuzevrijheid bestaat, is deze de facto niet meer aanwezig als bedrijven zich op dezelfde manier opstellen.

> Stel, in een boekwinkel zijn de boeken zodanig voorzien van niet verwijderbare RFID-tags, dat daarmee voor iedereen eenvoudig is na te gaan om wat voor soort boek het gaat. Een deel van het boekenkopend publiek zal het bezwaarlijk vinden dat zijn leesvoorkeuren niet privé gehouden kunnen worden. Als alle boekenverkopers, bijvoorbeeld om logistieke redenen, uitsluitend aldus getagde boeken aanbieden, dan hebben kopers niet meer de vrijheid boeken aan te schaffen waaraan het genoemde nadeel niet kleeft. Hetzelfde geldt voor situaties waarin een bedrijf nagenoeg een monopoliepositie heeft, zoals in het openbaar vervoer per trein.

Het ligt voor de hand om te streven naar een typologie waarin toepassingen met vergelijkbare gegevensverwerkingen en omgevingen samen genomen worden.
Deze typologie is zinvol als men wil komen tot een toets van kansen en bedreigingen, tot uitspraken over de verhouding van verwerkingen tot regelgeving en tot richtsnoeren voor goed gebruik, voor ontwerp en tot waarborgen. Afdoende is zij echter niet: de maatschappelijke effecten van RFID zijn zodanig dat men ook rekening moet houden met al dan niet opzettelijk incorrecte implementatie van toepassingen.

c Een voorstel voor een typologie: de omgeving

Een typering die helpt bij het begrijpen en terugdringen van risico's ontstaat door onderscheid te maken naar de soort van omgeving waarin een RFID-tag functioneert en naar de soort gegevens op de tag. Op die manier kan tot uitdrukking komen dat het bij het beoordelen van toepassingen niet zozeer gaat om de intentie van de toepassing, maar om het werkelijke gebruik, waarin ook partijen met andere oogmerken dan de toepasser een rol spelen.

Voor wat betreft de omgeving kan men daarbij gesloten omgevingen en open omgevingen onderscheiden. Een gesloten omgeving is alleen toegankelijk voor de deelnemers aan de toepassing: degene die gegevens verwerkt kent de deelnemers en de betekenis van gegevens. Voorbeelden zijn toepassingen met werknemerspasjes en bibliotheekpasjes.
Door tevens onderscheid te maken naar soorten gegevens die op de tag staan, ontstaan kwadranten, waarbij per kwadrant bezien kan worden welke risico's en maatregelen er bestaan en welke onderwerpen eventueel nog nadere aandacht verdienen:

soort gegevens soort omgeving	productgebonden gegevens dit is subtiel, vooral waar het gaat om het aangrijpingspunt van de WBP	persoonsgebonden gegevens hier is de WBP van toepassing
Open	speciaal letten op: het moment waarop gegevens in het consumenten-/ burgerbereik komen, c.q. persoonsgegevens worden.	speciaal letten op: toergang tot direct identificerende gegevens (eisen rond authenticatie en afscherming).
	betrokkenen zijn niet steeds bekend met gebruik van RFID. bedreigingen komen van *wie, wanneer.*	betrokkenen zijn niet steeds bekend met gebruik van RFID. bedreigingen komen van *wie, wat, wanneer.*
	of er sprake is van inbreuken wordt mede bepaald door het *waarom* van leesacties.	vooral moet worden gemotiveerd waarom er persoonsgebonden gegevens op een tag zouden moeten.
Gesloten	hier is in elk geval duidelijk wie er betrokkenen zijn en wie verantwoordelijke(n).	hier is in elk geval duidelijk wie er betrokkenen zijn en wie verantwoordelijke(n).
	speciaal letten op: gegevens die ook betekenis hebben buiten de gesloten omgeving.	speciaal letten op: koppeling met achterliggende databases.
	betrokkenen zijn bekend met gebruik van RFID. Bedreigingen komen vooral van *wanneer*.	betrokkenen zijn bekend met gebruik van RFID. Bedreigingen komen vooral van *wanneer*.
		in de regel zal duidelijk zijn *waarom* gegevens worden gelezen.

In de kwadranten waarin de tag persoonsgebonden gegevens bevat, bijvoorbeeld, zijn verwerkingen onderworpen aan de Wet bescherming persoonsgegevens. Voor die kwadranten zou de aandacht vooral uit kunnen gaan naar interpretatievraagstukken. In gesloten omgevingen zou men zich ongeacht het van toepassing zijn van de WBP vooral kunnen richten op de inspanningen die een verantwoordelijke kan plegen om de informatiewaarde van gegevens te minimaliseren en op het nadrukkelijk informeren van betrokkenen.
In hoofdstuk 4 wordt onder 'Juridische middelen' ingegaan op de vraag in hoeverre productgebonden gegevens gelden als persoonsgebonden gegevens in de zin van de WBP.

Typen waarborgen

Met welke middelen kunnen bedreigingen die RFID kan meebrengen worden tegengegaan? Technische voorzieningen lijken vooralsnog de meeste waarborgen te geven voor verantwoord RFID-gebruik. Daarnaast moet worden bezien of additionele juridische waarborgen nodig zijn en of flankerende instrumenten zoals gedragscodes een rol kunnen vervullen.

RFID-ontwikkelingen gaan zo snel, dat het lijkt of zij ons overkomen. Deze ontwikkelingen voltrekken zich echter niet in een vacuüm: systemen worden door mensenhanden gebouwd en functioneren in een door mensen bepaalde omgeving.
Waarborgen voor correct RFID-gebruik moeten in eerste instantie worden gezocht in het goed ontwerpen van systemen. Een goed ontwerp biedt echter niet in alle gevallen uitkomst. Ook als het uitlezen van gegevens volkomen wordt beheerst, zullen onbedoelde verwerkingen van gegevens plaatsvinden en blijven verdere verwerkingen soms ten onrechte mogelijk, bijvoorbeeld het combineren van gegevens in backoffices.
Door het onderkennen van wederzijdse belangen kunnen actoren uit alle sectoren werken aan een situatie waarin de maatschappelijke baten van RFID tot hun recht komen. Als betrokkenen inzien op welke bescherming zij aanspraak willen en kunnen maken als hun gegevens via RFID-systemen worden verwerkt, kan dat leiden tot een vraag naar juridische en technologische waarborgen. Een aanbod van geschikte technologieën kan weer leiden tot een vraag om de passende inzet van die middelen bij betrokkenen. Toepassers van de technologie zijn ook geholpen met een duidelijke uitleg over (juridische) randvoorwaarden.

4.1 Privacy by Design

Probleemloos gebruik van RFID moet vooral tot stand komen via ontwerpen van applicaties en van infrastructuren waarin vanuit verschillende invalshoeken aandacht is geschonken aan bestaande en mogelijke risico's, waaronder privacyrisico's, en die met de inzet van de juiste technologische maatregelen worden geïmplementeerd. Daarbij spelen niet alleen juridische randvoorwaarden een rol, bijvoorbeeld over het frequentiespectrumgebruik, maar ook technische, bijvoorbeeld over de standaardisatie van hard- en software ten behoeve van internationale operabiliteit.
Zeker bij toepassingen waarbij meer gegevens op een chip staan dan alleen een (product)-identificerend nummer, zoals bij paspoorten en OV-chipkaarten, komt het er op aan daarvoor een zodanige tagtechnologie te selecteren dat het gevaar van het weglekken van data zoveel mogelijk wordt beperkt. Ook bij andere onderdelen van het ontwerp speelt het belang van 'Privacy by Design'. Dit houdt in dat in alle fasen van de systeemontwikkeling rekening moet worden gehouden met de (juridische) eisen die samenhangen met de bescherming van persoonsgegevens.
Ongeacht de intenties die organisaties kunnen hebben met betrekking tot de zorgvuldige omgang met gegevens, kan het vertrouwen in die zorgvuldige omgang worden verhoogd door het inbedden van privacyverhogende maatregelen (Privacy-Enhancing Technologies of PET) in systeemprocessen, omdat dat een effectieve manier is om die zorgvuldigheid technisch af te dwingen.

> Voorbeelden van ontwerpbeslissingen zijn het verwijderbaar maken van tags, het (kunnen) weglaten van gegevensonderdelen bij het opslaan van RFID-gegevens in het backoffice systeem of het laten uitschakelen van tags zodra zij het consumentendomein bereiken.

Voorkomen moet worden dat tags worden ingezet voor typen toepassingen waarvoor ze niet geschikt zijn. Bij het bepalen van geschiktheid spelen niet alleen de uitleesafstand en het passen bij de omgevingsfactoren een rol, maar moet ook rekening worden gehouden met de mogelijkheid om gegevens op de tag te veranderen en met eventueel uitlezen van de gegevens door derden.

Omdat de geheugenruimte op RFID-tags beperkt is, nam iedereen tot nu toe aan dat deze niet geïnfecteerd konden worden met een computervirus. Onderzoekers aan de Vrije Universiteit hebben echter ontdekt dat dit wel degelijk mogelijk is. Op 15 maart 2006 hebben Melanie Rieback en haar promotor prof. dr. Andrew Tanenbaum op de jaarlijkse conferentie van het Institute of Electrical and Electronics Engineers over Pervasive Computing and Communications te Pisa een demonstratie gegeven van het plaatsen van een computervirus op een tag. Eén geïnfecteerde RFID-tag kan een heel systeem ontregelen, met catastrofale gevolgen. In het persbericht dat de Vrije Universiteit over deze ontdekking deed uitgaan, wordt het volgend voorbeeld gegeven.
'Stelt u zich bijvoorbeeld het vliegveld van Las Vegas voor, dat maandelijks twee miljoen stuks bagage verwerkt. Vanaf mei 2006 willen ze daar RFID-tags bevestigen aan koffers om de bagageafhandeling te versnellen. Als iemand met kwade bedoelingen een geïnfecteerde RFID-tag aan zijn koffer bevestigt, kan hij de boel aardig in de war schoppen. Zodra zijn koffer wordt gescand kan de besmette tag de hele bagagedatabase van het vliegveld aantasten en raakt alle daarna ingecheckte bagage eveneens besmet. Bij aankomst op andere vliegvelden scant men deze koffers opnieuw, waardoor binnen 24 uur honderden vliegvelden, overal ter wereld, kunnen worden besmet.'
Verdachte bagage zou op deze manier ongezien de wereld over kunnen worden gestuurd.
Zie voor het paper www.rfidvirus.org/papers/percom.06.pdf

Ook het bepalen met wie de informatie gedeeld mag worden, bijvoorbeeld via autorisatie, is niet alleen onderworpen aan regulering maar is ook een ontwerpvraagstuk.

4.2 Vaste aspecten van Privacy by Design

Elke techniek zou uiteindelijk zonder onnodige beslommeringen gebruikt moeten kunnen worden. Dat kan soms bereikt worden door zodanige, niet per se ingewikkelde, technische voorzieningen te treffen, dat het succes van de toepassing niet onnodig afhangt van menselijk gedrag, procedures en/of van de betekenis en naleving van regelgeving. Verder kunnen bewustwording en (technologisch) begrip van (on)mogelijkheden al voor een betere omgang met de technologie zorgen en voor een groter vertrouwen erin.

Het succes van Privacy by Design hangt in belangrijke mate af van de deskundigheid en creativiteit van ontwerpers. Denkbaar is dat er per type RFID-toepassing ontwerpvoorstellen worden gedaan.
RFID-technologie en de toepassing ervan zijn te veelsoortig om op deze plaats specifieke maatregelen te kunnen noemen die met het oog op de verwerking van persoonsgegevens genomen moeten worden. Het is aan de verantwoordelijken om die maatregelen, gegeven een applicatie, wel te noemen en te nemen. Verder kunnen ontwikkelingen in de technologie ertoe leiden dat systemen die ooit met inachtneming van Privacy by Design zijn ontworpen naderhand aangepast moeten worden om probleemloos gebruik te garanderen. Een grotere leesafstand bijvoorbeeld en een groter aantal gegevens dat kan worden uitgelezen, zouden aanleiding kunnen zijn voor scherpere beveiliging.

Desondanks kan wel worden aangegeven langs welke weg selectie van de juiste maatregelen tot stand kan komen.

Twee onderwerpen verdienen daarbij altijd de aandacht: technische middelen en beveiliging.

Technische middelen
Bij het in het ontwerp inbouwen van waarborgen voor een goed gebruik van de technologie spelen vele factoren een rol. Veel vragen moeten worden beantwoord, zowel op organisatorisch terrein – wie mag, in gevallen waarin data zijn versleuteld, waarvoor gegevens ontsleutelen, wie mag sleutels gebruiken en beheren – als op het technisch vlak – hoe moeten de infrastructuur, bandbreedte, opslag- en rekencapaciteit van chips zijn en zijn hiervoor standaards beschikbaar? Bij toepassingen waarbij versleuteling essentieel is, zoals RFID-

uitleesbare paspoorten, is het ontwikkelen van een infrastructuur voor het (geautoriseerd) uitlezen en ontsleutelen van data een technologische en organisatorische uitdaging.
Met het oog op de verwachte gegevensexplosie moeten middelen worden bedacht voor de opslag en verwerkingscapaciteit van systemen. Ook hier is de technische uitdaging aanzienlijk.

Bij het ontwerpen van systemen moet uiteraard in de eerste plaats aandacht worden besteed aan de beoogde functionaliteit, waarbij de specificaties voor de te hanteren technologie moeten passen bij de gebruiksomgeving. Tevens moeten de ontwerpers onbedoeld gebruik van de technologie tegengaan. Systemen moeten bestand zijn tegen onverwachte situaties – men moet voorzichtig zijn met het soort gegevens dat men op een tag wil vastleggen – en verhinderen dat nadelen optreden wanneer partijen zich bewust of onbewust niet houden aan (formele of informele) regels voor de omgang met de applicatie.

Beveiliging
Waar gegevens niet verwijderd kunnen worden, zoals door het wissen, het uitschakelen of verwijderen van tags, komt de nadruk te liggen op beveiliging. Maatregelen hiervoor zijn gedeeltelijk gericht op het garanderen van de continuïteit van een applicatie. Vanuit het oogpunt van gegevensbescherming kunnen daarop nog verscherpingen nodig zijn, bijvoorbeeld wanneer gegevens niet zonder meer uitleesbaar mogen zijn, zoals bij

- gegevens die van meet af aan gekoppeld worden aan een persoon (bijvoorbeeld als het gaat om het plaatsen van direct identificerende gegevens op tags);
- de verwerking van bijzondere gegevens die aan een persoon zijn te relateren (bijvoorbeeld RFID's op medicijnverpakkingen).

Ook waar het niet gaat om de aanwezigheid van persoonsgebonden gegevens, zijn aan RFID gerelateerde risico's doorgaans te wijten aan slechte beveiliging van een specifiek onderdeel van een RFID-systeem, namelijk de tag, of aan communicatie met de tag. Het minimaliseren van uitleesafstanden is een vorm van beveiliging tegen afluisterpraktijken. Als deze minimalisatie leidt tot uitleesafstand nul, dan is er geen reden meer om voor die verwerking RFID in te zetten.
Soms is het verstandig om met het oog op risico's RFID helemaal niet in te zetten voor bepaalde toepassingen. Analyse van de tekortkomingen die kleven aan bijvoorbeeld het digitale paspoort zou tot het inzicht kunnen leiden dat het helemaal niet wenselijk is dat paspoorten contactloos worden uitgelezen.

In 2005 verscheen in de pers het bericht dat het kraken van de beveiliging van paspoorten mogelijk bleek, waardoor ongeautoriseerde partijen persoonsgegevens, zoals vingerafdruk en digitale gelaatsscan, van de pas konden kopiëren.
Algemeen Dagblad 28 juli 2005
Ook een implanteerbare chip is al gekraakt.
(www.spychips.com)

Nog beter dan het goed beveiligen van overbodige gegevens is het niet genereren ervan.

Drie aspecten van beveiliging
Aspecten van beveiliging zijn confidentialiteit, integriteit en continuïteit.
Bij confidentialiteit en integriteit gaat het om aspecten van de data, niet van de systemen.
Bij continuïteit gaat het om systemen.
Gelet op de technische mogelijkheden van RFID-systemen kan de neiging bestaan tot 'security by obscurity'. Om vertrouwen in de technologie en in de toepassingen te bereiken, is het beter om uit te gaan van transparantie.

Confidentialiteit
Gegevens, zowel 'in ruste' als 'in transit', dienen alleen uitgelezen te kunnen worden door daartoe geautoriseerde partijen. Voor situaties waarin confidentialiteit een rol speelt, moeten

daarom protocollen zijn voor authenticatie en voor encryptie. Het gebruik van mechanismen hiervoor brengt eisen, en daarmee kosten, mee voor de verwerkingsmogelijkheden. Bij het ontwerpen van RFID-toepassingen is een belangrijke vraag welk type toepassingen welke soort authenticatie en/of versleuteling vergt.

Het is niet altijd gemakkelijk om confidentialiteit te waarborgen, onder meer vanwege:
- organisatorische redenen (gebruik van encryptie vergt bijvoorbeeld voorzieningen en sleutelbeheer);
- technische redenen (de tijd die bij het uitlezen nodig is voor dataversleuteling en -ontsleuteling is bijvoorbeeld niet steeds beschikbaar); en
- economische redenen (chips die voldoende intelligent zijn voor het afhandelen van protocollen, bijvoorbeeld voor authenticatie, zijn duurder dan vergelijkbare chips die deze intelligentie niet hebben).

Bij het verwerken van persoonsgebonden gegevens moet confidentialiteit worden gegarandeerd. Welke beveiligingsmaatregelen er op de tag nodig zijn bij toepassingen waarin tags productgebonden gegevens bevatten, is in sterke mate contextafhankelijk.
Als gegevens op de tag persoonsgegevens zijn, gelden specifieke beveiligingseisen, ontwikkeld door de Registratiekamer, de voorganger van het CBP, in het rapport 'Beveiliging van persoonsgegevens', reeks Achtergrondstudies en Verkenningen nr 23, 2001.

Gegevens op smart labels zullen openbaar zijn (evenals de bijbehorende gegevens uit de catalogi). Wat niet openbaar is of hoort te zijn is de koppeling tussen die gegevens en personen, de oorzaak van een deel van de risico's. Gelet op de zwakke beveiligingsmogelijkheden van smart labels is te verwachten dat het tegengaan van misbruik van gegevens eerder bereikt moet worden door vernietiging of uitschakeling van de tags of het wissen van de gegevens, dan van het beveiligen van de tag.

Bij overige voorzieningen die ter bevordering van de vertrouwelijkheid kunnen worden getroffen, kan men zich mechanismen voorstellen die het afgeven van informatie laten afhangen van de afstand tot de lezer, waarbij een lezer op onverwacht grote afstand niet wordt vertrouwd. Bij gesloten systemen als bibliotheken zou de beveiliging erop gericht moeten zijn dat gegevens niet bekend kunnen worden aan personen die geen deel uitmaken van het systeem.

Integriteit
De integriteit van gegevens op tags is niet alleen vanuit maatschappelijk en beschermingsoogpunt relevant, maar ook vanuit het oogpunt van de toepasser. Gelet op het belang van de juistheid van data mag worden verwacht dat toepassers steeds zelf zorgen voor een voor dit aspect optimale technologie. Helaas zal het dan nog steeds voorkomen dat gegevens ten onrechte worden veranderd. Vanuit het oogpunt van bescherming van persoonsgegevens mag daarom worden geëist, dat op tags geen persoonsgegevens mogen worden vastgelegd als deze zo kunnen worden veranderd dat zij, gelet op het doel van de verwerking, niet meer integer zijn.

> Het garanderen van data-integriteit op RFID-tags is niet eenvoudig. Lukas Grunwald, een Duitse beveiligingsconsultant, liet al in 2004 zien hoe gegevens op smart labels door winkelbezoekers kunnen worden veranderd.
> *CNET News.com, RFID tags become hacker target, by Robert Lemos, 28 juli 2004, http://news.com.com/RFID+tags+become+hacker+target/2100-1029_3-5287912.html*

Als gegevens toch veranderd moeten kunnen worden terwijl sprake is van een niet herschrijfbare tag, dan moet of de tag worden vervangen of moeten de wijzigbare gegevens elders, niet op de tag, worden opgeslagen.

Continuïteit
Applicaties zullen in het algemeen zo worden ingericht dat het in het ongerede raken van tags

geen problemen oplevert, ook niet voor de betrokkene. Voor RFID-systemen gelden enkele bijzondere omstandigheden:

- bij RFID-toepassingen kan het uitschakelen van tags juist het oogmerk van betrokkenen zijn in gevallen waarin er onvoldoende vertrouwen bestaat in de omgang met gegevens;
- inmiddels blijken tags ook via aanvallen onklaar te maken. Of een tag nog functioneert, is door een betrokkene nauwelijks na te gaan en het is de vraag in welke gevallen dragers van een tag een zorgplicht hebben voor het functioneren van de tag. Deze constatering geeft aan dat het onwenselijk is dat rechten gaan afhangen van het functioneren van de tag of van gegevens die zich op de tag bevinden.

Het is mede in het belang van de toepassers dat RFID-systemen robuust ontworpen worden en dat er tegelijk rekening wordt gehouden met de mogelijkheid dat tags die zich buiten het domein van een verantwoordelijke bevinden (per ongeluk of met opzet van enige partij) in het ongerede raken. Robuustheidseisen spelen te meer bij toepassingen in de zorg. De correcte en ononderbroken werking van RFID-systemen kan daar van levensbelang zijn.

4.3 Juridische middelen

Of het bestaande juridisch kader voor de bescherming van de persoonlijke levenssfeer voldoet voor het beteugelen van de risico's die RFID meebrengt, is nog niet te beoordelen. Over de reikwijdte van de regelgeving voor de bescherming van persoonsgegevens verschillen partijen van mening. Dit meningsverschil is onder meer te wijten aan verschillende opvattingen over de invulling van het begrip 'persoonsgegeven'. Daarbij speelt bijvoorbeeld de vraag onder welke omstandigheden een productgebonden gegeven een persoonsgegeven is.

RFID-toepassers zijn gebonden aan de wettelijke regels voor de rechtmatige verwerking van persoonsgegevens.
Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1 onder a van de WBP). Op RFID-systemen waarmee het de bedoeling is persoonsgebonden gegevens te verwerken, zoals bij toepassingen in paspoorten of andere documenten met direct identificerende persoonsgegevens, is de Wet bescherming persoonsgegevens vanzelfsprekend volledig van toepassing.

In andere gevallen is het niet steeds eenvoudig vast te stellen of gegevens op een tag aan te merken zijn als persoonsgegevens. Ook als niet het oogmerk bestaat om een gegeven aan een persoon te relateren, kunnen gegevens, bijvoorbeeld gegevens die louter bedoeld zijn om een product te beschrijven, worden gebruikt ter beoordeling van een persoon in het maatschappelijk verkeer. In zo'n geval zal in de regel wel sprake zijn van persoonsgegevens in de zin van de WBP.

Een voorbeeld ter verheldering. Zolang een getagd product zich in de logistieke keten bevindt en niet geassocieerd kan worden met een persoon, is een productgebonden nummer dat zich op de tag bevindt geen persoonsgegeven. Wanneer echter dat gegeven in een winkel wordt verwerkt samen met de identificerende gegevens van een gekende persoon, zoals betaalgegevens, of wordt gerelateerd aan de fysieke persoon die zich in die omgeving bevindt, is er doorgaans wel sprake van een persoonsgegeven. Daarbij doet het niet steeds ter zake of er betekenis kan worden gehecht aan het gegeven dat zich op de tag bevindt.
Ook het begrip 'identificeerbaar' behoeft aandacht. Men hoeft iemand niet met naam en toenaam te kennen om van een identificeerbaar persoon te spreken: voor het begeleiden of het volgen van een persoon in een winkel volstaat soms het uitlezen van een waarde die binnen de verwerkingscontext is gekoppeld aan een uniek persoon, ook als aan die waarde geen verdere betekenis kan worden toegekend. Gebruik van productgebonden gegevens die van tags gelezen worden met als doel de betrokkenen op de een of andere manier te bedienen, valt binnen de reikwijdte van de WBP.

cf: IP adres is persoonsgegeven (nl. door ISP herleidbaar tot persoon)
Maar waarom dan een OV chipkaart nummer niet?

Als geen sprake kàn zijn van risico's die samenhangen met een verwerking van een gegeven, dan heeft het weinig zin een RFID-gegeven als persoonsgegeven aan te duiden. De ervaring leert echter dat men niet te snel moet denken dat een risico niet bestaat.
Voor het treffen van maatregelen voor de zorgvuldige omgang met RFID-gegevens bieden het huidig wettelijk kader en jurisprudentie voorlopig voldoende aanknopingspunten. Voor het leveren van meer houvast wordt in Europees verband gewerkt aan de vaststelling van wettelijke RFID-kernbegrippen. Het is niet zinvol of gewenst om bij voorbaat voor iedere denkbare RFID-toepassing afzonderlijk te bezien of en zo ja in welke gevallen de WBP van toepassing zou kunnen zijn.

Om effectieve voortgang in RFID-specifieke regelgeving te bereiken, is het beter om per type toepassing van de technologie te inventariseren welke maatschappelijke knelpunten ontstaan als regelgeving ontbreekt of onvoldoende duidelijk is. Daarnaast kunnen zelfregulerende initiatieven, zoals het opstellen van gedragscodes, worden ontwikkeld door marktpartijen en consumentenorganisaties.

4.4 Overige waarborgen

Ook individuen kunnen zelf een bijdrage leveren aan het verminderen van mogelijke RFID-risico's. Onafhankelijk van regelgeving en technologische waarborgen kunnen zij hun gedrag afstemmen op het bestaan van RFID-toepassingen, zeker zolang de door Privacy by Design beoogde waarborgen niet worden bereikt of niet voldoende blijken. Daarbij kan het gaan om het tonen van alertheid ten aanzien van de aanwezigheid van tags of om het uitvoeren van handelingen waarmee men tags uitschakelt of afschermt. Om optimale omgangsvormen te bereiken is kennis van risico's en van beschermingsmiddelen nodig.

Daarom is het van groot belang dat inzetters van RFID-toepassingen betrokkenen over die inzet actief informeren. De informatievoorziening is vooral van belang om betrokkenen de juiste beslissingen te kunnen laten nemen, bijvoorbeeld over het uit- of inschakelen van de tag in gevallen waarin die keuze voor hen relevant kan zijn. De informatie zou moeten zien op de aanwezigheid van RFID, de momenten van het lezen van de gegevens van de tag, de data die op deze tag staan en de betekenis daarvan.

Er wordt verschillend gedacht over de risico's die RFID mee kan brengen. De situatie zal van soort tot soort applicatie verschillen en welke (rest)risico's bestaan, hangt verder af van waarborgen die voor een applicatie zijn getroffen. Waarborgen kunnen ook maatregelen betreffen die thans niet in de regelgeving zijn opgenomen. Hieronder vallen het inrichten van aanspreekpunten in de vorm van algemene loketten voor RFID-klachten of -vragen. Alleen al het bestaan van dergelijke loketten kan bijdragen tot het objectiveren van RFID-verwachtingen en tot het verminderen of wegnemen van ongerustheid.
Door open te zijn over de klachten en vragen, kunnen onder meer inzetters van de technologie initiatieven nemen om verbeteringen aan te brengen in applicaties. De loketten vormen ook een platform voor het geven van voorlichting en het delen van kennis.
Daarnaast kan gedacht worden aan het instellen van audits van systemen, die duidelijk kunnen maken of RFID verantwoord wordt ingezet en gebruikt, aan best practices bij het invullen van technische en organisatorische eisen en aan RFID-certificering. Het verdient overweging om auditresultaten openbaar te laten maken.

> TNO heeft in 2006 verkend of het mogelijk is om een 'privacy keurmerk' voor RFID te ontwikkelen. Belangrijke vragen hierbij zijn waarop het keurmerk precies betrekking heeft en hoe het zich zou verhouden tot andere certificaten. Bij een mogelijke toekenning van een keurmerk aan fabrikanten die RFID-tags op hun producten plaatsen is het van belang dat de privacyvriendelijke inzet die door de fabrikant wordt beoogd, ook daadwerkelijk wordt gerealiseerd in de gehele keten die het product doorloopt.

Hoe verder met RFID?

5

De voorgaande hoofdstukken hebben een beeld geschetst van wat RFID is en welke implicaties toepassing van deze technologie heeft. De stellingen en aanbevelingen die hieronder zijn verwoord beogen niet in eerste instantie 'oplossingen' te bieden voor de gesignaleerde bedreigingen. Zij hebben meer de bedoeling bij te dragen aan een verdergaand debat dat moet leiden tot nadere afspraken over een goede omgang met RFID. Daarbij moet steeds worden bedacht dat bedreigingen deels al worden ondervangen door aan de WBP te voldoen.

In deze fase van het debat over RFID ligt het accent op de mogelijke maatschappelijke gevolgen van toepassing van de techniek: veelbelovend of onverantwoord? De ontwikkelingen gaan snel en het is zinnig aan te geven waarop moet worden gelet. Omwille van de inzichtelijkheid zijn de aandachtspunten per doelgroep gerangschikt. Dat wil niet zeggen dat sprake is van geïsoleerde taakgebieden. Alleen al omdat vertrouwen in de technologie vergroot kan worden door transparantie, gebruik van best practices, inzet van de juiste technologische middelen, gebruik van standaards, certificering en toezicht is duidelijk dat partijen zullen moeten samenwerken om risico's verbonden aan RFID-toepassing het hoofd te bieden en om maatschappelijk ongewenst gebruik en/of oneigenlijk gebruik door derden zoveel mogelijk te voorkomen.

5.1 Betrokkenen

- *Betrokkenen hebben recht op informatie over toepassing van RFID.*

Betrokkenen – burgers, consumenten – zouden geen zorgen moeten hebben over de eventueel aan RFID verbonden nadelen. Om RFID objectief te kunnen waarderen moeten zij over toereikende informatie beschikken. Dit kan bijvoorbeeld gebeuren door duidelijke en volledige etikettering van goederen.

- *Een kritische houding draagt bij aan goed gebruik van RFID.*

Betrokkenen kunnen al dan niet in georganiseerd verband, zoals in consumentenorganisaties, bijdragen leveren aan het maatschappelijk discours over RFID. Zij kunnen eventuele zorgpunten aangeven en stimuleren dat er voor hen voldoende kanalen beschikbaar zijn voor het ontvangen van informatie van overheden en branches en voor het naar voren brengen van vragen en opmerkingen.

- *Betrokkenen moeten zich kunnen verweren tegen RFID-gebruik.*

Voor zover zij aan zelfbescherming moeten doen is het voor betrokkenen van belang dat zij de mogelijkheden daartoe kennen, zodat zij hun gedrag kunnen aanpassen of middelen kunnen inzetten. Hierbij valt te denken aan het kunnen kiezen voor een alternatief waarbij geen RFID wordt gebruikt of aan het kunnen verwijderen van tags. Dit laatste brengt ook mee dat er geen algemeen verbod zou mogen komen op het verwijderen van tags.

- *Betrokkenen dienen inzage te kunnen verkrijgen in de met behulp van RFID over hen opgeslagen gegevens.*

Dit inzagerecht is geborgd in de WBP. Het is raadzaam het inzagerecht voor RFID-gegevens nader te specificeren, een taak voor de wetgever of de toezichthouder.

- *Er dient een goede klachtregeling te komen voor mogelijk misbruik of oneigenlijk gebruik van RFID.*

In eerste instantie dient de partij die verantwoordelijk is voor de inzet van RFID een aanspreekpunt in te richten.
Daarnaast kan worden bezien of het inrichten en onderhouden van een algemeen loket nodig en/of wenselijk is.
In alle gevallen is het wenselijk dat er openheid bestaat over de ontvangen klachten en dat de afhandeling van klachten transparant is.

5.2 Toepassers van de technologie

Toepassers van de technologie zouden dienen te letten op de effecten die partijen kunnen ondervinden door inzet van die technologie. De aandacht moet niet alleen gaan naar de positieve effecten – zekerheid over de herkomst van producten, betere serviceverlening, snellere afhandeling, betere bedrijfsresultaten – maar, met het oog op acceptatie van de technologie, ook naar negatieve.

- *Zet geen RFID in als dat niet hoeft.*

Het afzien van RFID-gebruik geldt in het bijzonder voor die gevallen waarin het gebruik van persoonsgegevens risico's meebrengt, bijvoorbeeld doordat gegevens door derden kunnen worden uitgelezen. Inzet is af te raden als niet voldoende duidelijk is dat toepassing geen onoverkomelijke complicaties kan meebrengen.
Ook overheden kunnen een slechte beurt maken door zonder grondige analyse over te gaan op het gebruik van RFID. Ook hier mogen risico's niet toevallen aan betrokkenen. Bijzonder is dat dezen vaak geen keuzevrijheid hebben.

- *Inzet van RFID moet proportioneel zijn.*

Stel, dat op alle kleding gegevens door middel van RFID worden vastgelegd die slechts relevant zijn voor een klein gedeelte van de populatie – bijvoorbeeld voor mensen met een uiterst luxueuze wasmachine die in staat is RFID-tags in kleren te lezen om aan de hand daarvan zelf haar wasprogramma's vast te stellen. Als deze tags niet goed beveiligd blijken te zijn, dan wordt de gehele bevolking met de mogelijke nadelen van verkeerd gebruik opgezadeld. Dit is buiten proportie.

- *Toepassers en organisaties van toepassers dienen zich een goed beeld te vormen van mogelijke en al gebleken risico's van de inzet van RFID, om aan de hand daarvan maatregelen te kunnen treffen om deze risico's te elimineren of te verminderen.*

Het overstappen naar een nieuwe technologie is niet altijd aangewezen. Bij innovatie moet ook worden gelet op maatschappelijke effecten. Elke nieuwe toepassing wint aan vertrouwen als deze precies daar wordt ingezet waar dat verantwoord is. Detailhandelaren zullen niet overgaan tot de inzet van RFID zolang deze geen meerwaarde heeft boven streepjescodesystemen, bijvoorbeeld omdat een voor RFID benodigd nummersysteem nog niet klaar is.
Indien het niet de bedoeling is dat tags verwijderd kunnen worden, zoals bij lidmaatschapskaarten, dan moeten verantwoordelijken de kaart voorzien van zodanige beveiligingsmaatregelen dat geen gegevens onbedoeld gelezen kunnen worden.

- *Uitgangspunt moet zijn dat actieve tags niet het consumentendomein bereiken.*

Het zou aanbeveling verdienen dat smart labels die alleen een functie hebben in het logistieke proces worden verwijderd, uitgeschakeld of gewist voordat zij in het consumentendomein komen.

- *De last die samenhangt met het opheffen van RFID-gerelateerde risico's moet niet worden verschoven naar de consument/betrokkene.*

Als verwijderbare tags worden ingezet, dan moeten die zo geplaatst worden dat zij ook daadwerkelijk te verwijderen zijn.
Consumenten moeten niet worden 'gestraft' met hogere prijzen of langere wachttijden als zij kiezen voor RFID-loze alternatieven of als zij kiezen voor het laten verwijderen van de tags voordat zij de winkel uit zijn.

Beveiliging

Toepassers van de RFID-technologie vervullen een spilfunctie bij het vinden van de beste manieren om deze in te zetten. Om Privacy by Design te kunnen bewerkstelligen, moeten zij feedback geven aan ontwerpers en ontwikkelaars van systemen. In het bijzonder geldt dit voor het ontwikkelen van beveiligingscriteria voor tags waarop zich persoonsgegevens bevinden.

- *Toepassers moeten expliciet kunnen aangeven welke afwegingen een rol hebben gespeeld bij de totstandkoming van beveiligingsmaatregelen.*

Speciale aandacht verdient de relatie met andere systemen: het is niet evident dat gegevens op een tag altijd en volledig worden overgenomen in andere systemen. Voor zover gegvens-

persoonsgegevens zijn moet het overnemen daarvan in overeenstemming zijn met de eisen die de WBP daar aan stelt. Dat wil ook zeggen dat het opslaan van data-elementen die gelet op het doel van een verwerking bovenmatig zijn, niet is toegestaan.
Hoewel het niet specifiek een RFID-aspect is, het is nuttig te wijzen op het preventief belang van dataminimalisatie in de backoffice.

- *De omstandigheid dat RFID-nummers in hun totaliteit worden gelezen rechtvaardigt nog niet dat deze ook in hun totaliteit worden opgeslagen in backofficesystemen.*

Ketens

Verwerking van gegevens in een branche is steeds meer ketengeoriënteerd. Deze tendens is ook zichtbaar bij de inzet van RFID. Door de ketenoriëntatie vervagen grenzen en verantwoordelijkheden. Bij toepassingen met een ketenbreed effect is een rol weggelegd voor samenwerkingsverbanden binnen branches, om te bezien waar in een keten risico's ontstaan, waar maatregelen kunnen worden getroffen en wie waarop aangesproken kan worden, indien daarover nog onduidelijkheid mocht bestaan. Ook voor partijen die niet in dezelfde keten opereren is samenwerking van belang. Dit is onderkend door het RFID Platform Nederland, een forum waar leveranciers en (potentiële) gebruikers van RFID elkaar kunnen ontmoeten, onder meer om kennis en ervaringen uit te wisselen en mogelijke barrières voor de toepassing van RFID te slechten.

- *Samenwerkingsverbanden kunnen gedragscodes en best practices ontwikkelen en scenario's voorkomen waarin de techniek aan partijen wordt 'opgedrongen'.*

Al eerder in deze studie is gewezen op het bestaan van 'schemergebieden' bij RFID-toepassingen, waarin het niet duidelijk is of het begrip 'persoonsgegeven' van toepassing is. In die gevallen is het voor toepassers onduidelijk welke verplichtingen zij hebben en voor betrokkenen onduidelijk welke bescherming zij genieten. Verheldering kan via wetsuitleg, maar ook via (branchegewijze) afspraken.
Belangrijke zelfreguleringsinitiatieven met betrekking tot RFID-gebruik zijn de richtlijnen van de Internationale Kamers van Koophandel, de ICC principles on EPC deployment and operation (www. iccwbo.org) en de EPCglobal Guidelines (www.epcglobalinc.org).

- *Het kan zinvol zijn, bijvoorbeeld om de acceptatie van RFID door het publiek te bevorderen, om bepaalde maatregelen gewoonweg te treffen, ook al zijn deze (nog) niet altijd afdwingbaar.*

Zichtbaarheid

Bij het verwerven van vertrouwen in de ontwikkeling en inzet van RFID zijn informatieverstrekking en transparantie trefwoorden voor toepassers.

- *Toepassers hebben de plicht RFID-gebruik zichtbaar en kenbaar te maken.*

Deze plicht kan worden gezien als tegenhanger van het recht van de consument op informatie over RFID-gebruik.
Het feit dat RFID wordt gebruikt, kan via algemene informatieverstrekking aan het publiek worden kenbaar gemaakt. Die informatie moet duidelijk maken welke data op een tag zijn vermeld, welke betekenis die hebben en welke doelen zij dienen. Ook moet duidelijk zijn waar en wanneer uitleesacties plaatsvinden, bijvoorbeeld door het aangeven van de plaats van lezers en door het zichtbaar en hoorbaar maken van uitleesacties.

5.3 De overheid als bijzondere toepasser

Ook overheden zijn of worden toepassers van RFID-technologie. Voorbeelden hiervan zijn het contactloos uitlezen van officiële documenten (paspoorten), het controleren van de echtheid van voorwerpen (geld, pasjes) en het oplossen van logistieke vraagstukken, zoals bijvoorbeeld in de Verenigde Staten ten behoeve van materiaalbeheer bij Defensie.

De overheid is een bijzondere partij. Zij heeft mogelijkheden om bepaalde systeemspecificaties voor bepaalde applicaties af te dwingen en de technisch best mogelijke beveiligingssystemen te eisen.

- *Juist vanwege haar monopoliepositie op een aantal terreinen mag worden verwacht dat de overheid RFID altijd verantwoord inzet, gebruikmakend van technologische en organisatorische maatregelen ter voorkoming van risico's.*

De overheid heeft een voorbeeldfunctie. Gelet op de negatieve reacties die zijn losgekomen op de manier waarop RFID in paspoorten zou worden gebruikt – de Verenigde Staten bijvoorbeeld overwogen een gemakkelijk afluisterbaar RFID-paspoort uit te geven, wat aanleiding was tot heftige reacties uit de samenleving – blijkt dat overheidsapplicaties die niet vertrouwenwekkend zijn het vertrouwen in de technologie kunnen ondermijnen. Eerdere versies van het Nederlandse RFID-paspoort zijn gekraakt.

- *Het bestaan van RFID zal van invloed zijn op het denken over toegang tot gegevens door overheden.*

Overheden zijn altijd geïnteresseerd in plaatsen waar veel gegevens over personen samenkomen. Die interesse bestaat ook bij andere partijen. De overheid echter is in staat om invloed uit te oefenen op de grenzen van het (juridisch) toelaatbare. De overheid moet er niet op uit zijn om RFID-gebruik aan te jagen om zodoende over steeds meer gegevens te kunnen beschikken. De samenleving moet erop kunnen vertrouwen dat datgene dat toelaatbaar is, past bij hetgeen maatschappelijk wenselijk is. Dit garandeert niet dat er geen spanning kan optreden ten aanzien van de omgang met privacygevoelige gegevens. Voorbeelden daarvan uit het recente verleden zijn de ophef over de Amerikaanse Patriot Act, de onderhandelingen over het verstrekken van passagiersgegevens door luchtvaartmaatschappijen aan de VS , of inzage in bibliotheekgegevens door de Amerikaanse overheid.

De intensivering van gegevensverwerkingen door RFID kan ook de belangstelling voor de daardoor gegenereerde gegevens aanwakkeren. Deze tendens kan voor organisaties juist weer aanleiding zijn om minder gegevens te willen vastleggen, bijvoorbeeld om te voorkomen dat deze organisaties zich later inspanningen moeten getroosten die geen verband meer hebben met de eigen doelstellingen.

cf. bewaar plicht & kosten beveiliging

Onderzoek en kennisdeling

Of de overheid ook als aanjager moet functioneren is bij innovatie een relevante vraag. Waar het gaat om het voorkomen van maatschappelijke risico's lijkt het eerder voor de hand te liggen dat overheden zich niet als eerste inlaten met technologieën waarvan de effecten nog niet zijn te overzien.

De overheid moet niet alleen inzicht hebben in de werking van haar eigen applicaties, maar ook in de mogelijkheden en onmogelijkheden van RFID en in de maatschappelijke effecten van de technologie.

- *De overheid heeft een rol bij het stimuleren van onderzoek en kennisdeling en het bevorderen van een goed gebruik van RFID.*

Overheden kunnen beleid ontwikkelen over RFID-gebruik en zich daarbij laten informeren door maatschappelijke instanties of andere organisaties zoals het Rathenau Instituut of ECP.NL. De overheid kan ook samenwerkingsverbanden van wetenschap, industrie, toepassers en toezichthouders in het leven roepen om goed RFID-gebruik te bevorderen.

Tevens kan de overheid wetenschappelijk onderzoek stimuleren en financieren en bevorderen dat ICT-fabrikanten specifieke hardware (tags, lezers), software (protocollen) en standaards ontwikkelen. De overheid kan tevens bevorderen dat RFID-toepassingen gebruikmaken van specifieke types RFID-technologie door het toewijzen van bandbreedtes voor te gebruiken radiofrequenties en dergelijke en het opleggen van authenticatieverplichtingen.

Tot slot kan de overheid het delen van kennis stimuleren, bijvoorbeeld over best practices. Daarbij kan het ook gaan om kennis die de overheid zelf heeft, of kennis die ontstaat via overleg met internationale (overheids)organisaties, waaronder toezichthouders.

- *De overheid heeft een rol in het informeren van burgers.*

Het onderzoek naar mogelijkheden voor RFID-toepassingen is sterk in ontwikkeling. Burgers zullen meer en meer met RFID geconfronteerd worden, zonder dat op alle (daardoor ontstane) vragen rond de bescherming van persoonsgegevens al antwoord gegeven kan worden. Verder brengt het 'verborgen karakter' van de technologie mee dat ongerustheid kan ontstaan bij per-

sonen over de vraag of hun gegevens wel of niet uitgelezen zijn en wel of niet goed worden gebruikt. Voor zover het toepassing van RFID door de overheid betreft ligt het voor de hand een informatiepunt in de trant van 'Postbus 51' in te richten.

- *Bij het nadenken over het gebruik van juridische middelen om eventuele RFID-risico's te voorkomen, kunnen ook de bezwaren aan de orde komen tegen bijvoorbeeld een verbod op apparaten waarmee men zich tegen uitlezen kan beschermen.*

Een voorbeeld van zo'n apparaat is de "guardian" die door onderzoekers aan de Vrije Universiteit wordt ontwikkeld.

> Zorg over RFID-toepassingen heeft geleid tot het ontwikkelen van apparaten waarmee consumenten zich kunnen wapenen tegen het ongewenst uitlezen van tags. In juli 2006 verscheen een bericht in de pers dat een "RFID Guardian" is ontwikkeld door een groep wetenschappers van de Vrije Universiteit. De onderzoeksleider, prof. Andrew Tanenbaum, stelde: "De industrie denkt niet na over het schenden van je privacy. Europese banken willen RFID in geld verwerken. Dat betekent dat een overvaller met een scanner de straten kan langsgaan om te zien hoeveel geld iemand bij zich draagt en wie het beste doelwit is".
> Een guardian is niet groter dan een Personal Digital Assistant en geeft een waarschuwing als er een RFID-lezer in de buurt is.
> *(Security.nl 21 juli 2006/Automatisering Gids 21 juli 2006)*

Er zou geen algemeen verbod mogen komen op het uitschakelen van tags. Voor specifieke gevallen kan het instellen van zo'n verbod wel zinvol zijn, bijvoorbeeld voor tags in paspoorten en op bankbiljetten.

5.4 Ontwikkelaars van systemen

De techniek kan bedreigingen voor de privacy meebrengen. Bij het vinden van beschermingsopties moet onderscheid worden gemaakt tussen de mogelijkheden van de basistechnologie (tags, readers, protocollen, nummersystemen etc.) en het systeemontwerp.

PEARL ⇒

- *Van de mogelijkheden die bestaan om risico's in te dammen, genieten technologische maatregelen doorgaans de voorkeur, omdat daarbij nadelen worden voorkomen onafhankelijk van het gedrag van gebruikers en onafhankelijk van het correct volgen van procedures.*

Het treffen van technologische maatregelen is vooral relevant in gevallen waarin de mogelijkheid bestaat dat andere partijen er juist op uit zijn om zwaktes in een ontwerp uit te buiten. Als risico's niet zijn te beteugelen door middel van de basistechnologie, kunnen bij het ontwerpen van de systemen alsnog maatregelen genomen worden, waarbij ook beveiligingsaspecten aan de orde komen.

- *Dataminimalisatie is een beschermingsstrategie.*

Er blijken altijd onbedoelde mogelijkheden voor gegevensgebruik te ontstaan als datastromen niet precies aansluiten bij een beoogde functionaliteit. Risico's kunnen worden voorkomen of verzacht door alleen noodzakelijke gegevens te verwerken.

- *Bij het opstellen van de systeemspecificaties zou de aandacht niet alleen moeten uitgaan naar functionele en technische aspecten, maar ook naar gebruikscriteria en naar maatschappelijke randvoorwaarden.*

Het CBP hanteert het begrip "Privacy by Design" om aan te geven dat het in het algemeen raadzaam is om in alle fasen van de systeemontwikkeling rekening te houden met de maatschappelijke en juridische eisen die samenhangen met de bescherming van persoonsgegevens. Organisaties willen zorgvuldig omgaan met de gegevens die hun ter beschikking staan. Het vertrouwen in die zorgvuldige omgang kan worden verhoogd door het inbedden van privacyverhogende maatregelen (Privacy Enhancing Technologies of PET) in systeemprocessen, omdat daarmee een effectieve manier bestaat om die zorgvuldigheid technisch af te dwingen.

In de regel worden bij de ontwikkeling van systemen kosten-batenanalyses uitgevoerd. Een dergelijke analyse kan ook worden uitgevoerd door niet een economisch perspectief te hanteren, maar een maatschappelijk. Daarbij kan gebruik worden gemaakt van een typologie van RFID-toepassingen (zie hoofdstuk 3). De analyse bestaat dan in het bepalen van de soort applicatie en het verfijnen van de voor die soort al beschikbare beschrijving.
Net zo goed als men per soort toepassing een inventarisatie van risico's kan maken, kan men zich een inventarisatie voorstellen van beschermingsmaatregelen. Die hoeven niet beperkt te zijn tot puur technische, maar kunnen ook tot uiting komen in bijvoorbeeld maatregelen die transparantie garanderen.

Vertrouwen

Bij toepassing van het concept Privacy by Design bij RFID-toepassingen bestaan de voordelen niet of nauwelijks in het besparen op ICT-middelen. De voordelen betreffen eerder het borgen van vertrouwen. Dit gebeurt door het voorkomen van verkeerd gegevensgebruik (door derden). Het gebruik van PET's wordt dan niet gebaseerd op de gedachte 'wie minder heeft hoeft minder te bewaken', of 'wie minder heeft kan makkelijk de kwaliteit ervan waarborgen!', maar eerder op 'waar minder is kan minder door derden misbruikt worden'. PET's kunnen bijdragen aan het voorkomen van imagoschade èn aan het behalen van bedrijfsvoordelen.
Over het algemeen geldt dat het kostenefficiënt is om in een zo vroeg mogelijk stadium van het ontwerp Privacy by Design toe te passen.
De eerste vraag daarbij is: 'Is het nodig RFID in te zetten?'.

> "A successful RFID-based solution needs to include a concerted effort to make sure that you're both taking the full potential and business process into consideration and laying the right kind of enterprise IT foundation"
> "When deploying RFID, make sure you think about the architecture issues, the scalability issues, and the security issues, besides looking at RFID readers and hardware."
> "Don't let the enterprise architecture get underfunded just because the hardware is sexy."
> *Jeff Woods van Gartner (Oracle magazine, mei/juni 2005)*

Aan deze woorden van Woods zoals geciteerd in het kader hierboven hadden ook 'privacy issues' toegevoegd kunnen worden. In gevallen waarin het onduidelijk is of de beoogde functionaliteit opweegt tegen maatschappelijke risico's is het afzien van RFID-inzet een relevante strategie. Als besloten is wel RFID in te zetten, worden aan de hand van onder meer de doelstelling van de toepassing en de inventarisatie van risico's ontwerpbeslissingen genomen en wordt een keuze gemaakt uit het aanbod van RFID-middelen.
Bij het ontwerpen komen onder meer aan de orde dataminimalisatie, het uitgangspunt dat persoonsgebonden gegevens niet op RFID-tags verwerkt moeten worden zolang daarbij geen afdoende beveiliging realiseerbaar is, doelbinding en beveiligingsmaatregelen.

5.5 Ontwikkelaars van de basistechnologie

Voor de ontwikkelaars van de basistechnologie is het inmiddels duidelijk dat het gebruik ervan privacyaspecten kent. Er zijn voldoende publicaties hierover voorhanden, niet alleen van de kant van privacyorganisaties maar ook van producenten van ICT-middelen. De ontstane kennis geeft aanleiding tot het doen van voorstellen om gesignaleerde bedreigingen het hoofd te bieden – ook op dit niveau is dus sprake van Privacy by Design - of om te komen tot de ontwikkeling van middelen waarmee betrokkenen zich kunnen beschermen tegen de nadelen van slordige implementaties. Hierbij kan men denken aan apparatuur om RFID-tags te detecteren, aan afschermmiddelen of aan maatregelen die ervoor zorgen dat betrokkenen een betere controle kunnen uitoefenen op het vrijgeven van gegevens. Ook kan worden gedacht aan het aanbrengen van vernietigingsmechanismen voor de tag, bijvoorbeeld door middel van 'kill switches', of aan mechanismen voor het wissen van de gegevens die er op staan.
Encryptie (van gegevens op de tag en/of van het communicatieverkeer) kan worden ingezet om te verhinderen dat derden kennisnemen van gegevens, en met authenticatie wordt toegang tot tag(gegeven)s door onbevoegden tegengegaan.

- *Naast het ontwerpen en produceren van ICT-middelen hebben ontwikkelaars, evenals wetenschappers, een rol bij het technisch en op privacybestendigheid beoordelen van systemen.*

Daarbij valt te denken aan het testen van de beveiliging van (infrastructurele) systemen of het controleren dat taggegevens niet kunnen worden gemanipuleerd.

Het CBP gaat verder niet in op technische mogelijkheden die er bestaan of zouden moeten bestaan voor het realiseren van doelen bij deze onderwerpen. Het volstaat met op te merken dat de Europese Commissie onderzoek naar optimale inzet van maatschappelijk relevante technologieën in het algemeen stimuleert, door fondsen beschikbaar te stellen.

Standaardisering

Zorgen over RFID-toepassing zijn deels te wijten aan standaardisering. Standaards bij RFID-gebruik betreffen niet alleen de via EPC te realiseren wereldwijde standaardisering van productcodes, waarmee een optimale besturing van wereldwijde goederenstromen bereikt kan worden. Er vindt ook technische standaardisatie plaats van hardwaremiddelen, software en protocollen, die onder meer nodig is om interoperabiliteit te kunnen bereiken.
Waar enerzijds standaardisatie kan zorgen voor een wereldwijd systeem van nummering, wat in enkele gevallen de oorzaak is van privacybedreigingen, kunnen anderzijds standaards die privacyvriendelijke inzet bevorderen, bijdragen aan het verzachten van nadelen, bijvoorbeeld via het ontwikkelen van standaards voor privacyvriendelijke chips, protocollen, beveiliging, of gedragscodes. Standaards kunnen natuurlijk ook worden gebruikt voor het kiezen van de middelen die moeten worden aangewend nadat via Privacy by Design is bepaald welke specificaties er bestaan.
Ook voor het vaststellen van de mate waarin technische oplossingen adequaat zijn, bestaan er standaards. Hierbij kan men denken aan de normering die bij het certificeren van producten of diensten gebruikt wordt.

5.6 Maatschappelijke partijen

De populariteit van RFID zorgt niet alleen voor activiteit bij potentiële toepassers en de ICT-industrie, maar ook bij wetenschappers en partijen in het 'privacyveld': burgerrechtenorganisaties, consumentenorganisaties, toezichthouders, bestuurders en politici. Deze partijen beperken zich niet tot het voor derden signaleren van hetgeen in hun ogen maatschappelijk onwenselijk is, maar zij delen ook kennis.

- *Onderling overleg en informatieoverdracht over RFID is van groot belang.*

De ontwikkelingen voltrekken zich niet in alle sectoren en in alle landen even snel. Ook hebben niet alle politieke en maatschappelijke instellingen de beschikking over dezelfde middelen, mogelijkheden en bevoegdheden. Het kennisarsenaal dat door middel van samenwerking en overleg wordt opgebouwd, kan niet alleen ingezet worden om risico's te signaleren, maar ook om deze te voorkomen of te verkleinen.
Door de technologie in het geheel niet in te zetten vermijdt men risico's, maar kunnen ook baten niet gerealiseerd worden.

5.7 De rol van het CBP

Grootschalige toepassing van RFID zal leiden tot een explosieve groei van het gebruik van gegevens. Voor zover het daarbij om persoonsgegevens gaat, zal de WBP van toepassing zijn, waarop het CBP de toezichthouder is. Het blijkt echter niet steeds eenvoudig te zijn om vast te stellen wanneer gegevens inderdaad zijn aan te merken als persoonsgegevens. Ook daarnaast zijn er de nodige interpretatievraagstukken die van invloed zijn op naleving van regelgeving en het toezicht daarop.
Het CBP rekent ook het leveren van bijdragen aan debat over privacygerelateerde ontwikkelingen tot zijn taak, om te voorkomen dat maatschappelijk ongewenste scenario's ontstaan. Gelet hierop ziet het voor zich een taak op de volgende terreinen.

Kennisdelen

- *Gezien de snelheid van RFID-ontwikkelingen en gelet op de vragen die gebruik van de RFID-technologie oproept, is samenwerking en kennisdeling met betrokken partijen essentieel, nationaal en internationaal.*

Het is nodig om een objectief beeld te hebben van de kansen en bedreigingen van de technologie, van het tempo waarin effecten zich voordoen en van de mate waarin middelen om risico's te voorkomen of te verzachten toereikend zijn. Onder meer is het van belang dat er een ook met toepassers gedeeld beeld is over definities en begripppen die essentieel zijn voor het reguleren van toepassingen waar dat noodzakelijk is. Daarbij zal onder andere de vraag moeten worden beantwoord wie de aangewezen partij is voor het voorkomen van door het publiek gepercipieerde bedreigingen en/of voor het voldoen aan verplichtingen.
Het ligt voor de hand om bij het agenderen van onderwerpen aansluiting te zoeken bij al bestaande initiatieven.

Technologie

- *Bij het voorkomen of verzachten van risico's die samenhangen met RFID-toepassing moet Privacy by Design uitdrukkelijk de aandacht hebben.*

Het CBP kan bijdragen aan voorstellen die per type toepassing aangeven op welke wijze kan worden geborgd dat gegevens op de juiste wijze worden verwerkt. De bijdrage kan bijvoorbeeld bestaan uit het aangeven van de aspecten van een verwerking die uit het oogpunt van gegevensbescherming relevant zijn of uit het toekennen van een voorbeeldfunctie aan toepassingen waarin RFID op verantwoorde wijze is ingezet.
Interessant is dat het hierbij ook om verwerkingen kan gaan waarvan niet a priori duidelijk is of zij formeel onder de WBP vallen.

Bewustwording

- *Alle partijen moeten weten waar ze goed aan doen in omgevingen waar RFID wordt ingezet en welke verplichtingen, rechten en mogelijkheden voor hen gelden.*

Er zijn vele publicaties verschenen waaruit een laag vertrouwen in de 'maatschappelijke veiligheid' van RFID-toepassingen spreekt. Dat vertrouwen kan toenemen als het publiek zich bewust is van de mogelijkheden en onmogelijkheden van de technologie en vertrouwen heeft in de middelen om risico's af te dekken. Het CBP speelt een rol in het vergroten van die bewustwording. Het CBP kan algemene voorlichting geven, in het bijzonder aan betrokkenen. Toepassers van RFID en ontwikkelaars van RFID-systemen verdienen ook de aandacht van het CBP. Zij kunnen worden geïnformeerd over verantwoorde inzet van RFID.

Normontwikkeling en handhaving

Het normenkader voor de goede omgang met persoonsgegevens wordt door RFID-toepassingen danig op de proef gesteld.

- *Alhoewel er in RFID-verband nog voldoende juridische vragen spelen over de reikwijdte en betekenis van de WBP, zijn er ook voldoende gevallen waarin geen twijfel bestaat over het onverkort van toepassing zijn van de wettelijke bepalingen.*

Voor zover de normen of definities in de WBP nog onduidelijk zijn, zal het CBP deze kunnen uitwerken. Bij normontwikkeling valt te denken aan het nader uitwerken van de nu al bestaande informatieplicht: er zijn inmiddels voldoende concrete voorstellen voor de inhoud van de informatie die verantwoordelijken moeten verstrekken als een RFID-toepassing eenmaal onder de reikwijdte van de WBP valt. In die voorstellen wordt bijvoorbeeld aangegeven dat betrokkenen geïnformeerd moeten worden over de momenten waarop RFID-gegevens worden gelezen. Bij het nader normeren van beveiligingsmaatregelen is het nodig om kennis te dragen van de technische mogelijkheden en onmogelijkheden van vooral tags en lezers.
In internationaal verband wordt gewerkt aan het verduidelijken en aanscherpen van kernbegrippen.
De invloed die nieuwe wijzen van verkrijging van gegevensbestanden en de verwachte toename van het aantal gegevensbestanden als gevolg van RFID zullen hebben op de handhavende taak van het CBP is nu nog niet aan te geven. Ook indien gebruikers van de techno-

logie naar verantwoorde toepassing streven, is onrechtmatig gebruik van RFID niet uit te sluiten. Het te vroeg inzetten van beperkende middelen kan echter verstikkend werken voor innovaties. Het te laat inzetten van middelen kan leiden tot onomkeerbare maatschappelijke nadelen.

Het is ook uit het oogpunt van bescherming van de persoonlijke levenssfeer niet zinvol om RFID uitsluitend in termen van risico's te benaderen. Parallel aan RFID-ontwikkelingen zal het CBP een objectief beeld moeten krijgen van kansen en bedreigingen en van de kracht en betekenis van specifieke instrumenten om bedreigingen te voorkomen. Met het uitbrengen van deze bijdrage aan de discussie en door deel te nemen aan voortgaand overleg in verschillende fora hoopt het CBP een inbreng te hebben in de ontwikkeling van evenwichtige standpunten over de maatschappelijke implicaties van RFID.

Bijlagen

Bijlage 1

Summary

The development of Radio Frequency Identification – RFID – has been rapidly gaining momentum in recent times. The technology makes it possible to generate, store or otherwise process unprecedentedly large quantities of data, including personal data.
RFID has considerable implications for privacy and the perception of privacy, making it a subject of social debate. Cooperation and knowledge-sharing are very important in the formation of opinion on the social preconditions for the responsible use of RFID. In its specific role as a regulator, the Dutch Data Protection Authority [College bescherming persoonsgegevens (CBP)] is issuing this discussion document in order to further stimulate debate about the benefits and drawbacks of the technology.

Privacy by Design
The main driving force behind the current use of RFID is improving ligistics. The main drawbacks lie in the fact that the data obtained can be used to assess people, often without their knowledge. The most important guarantee to avoid or alleviate these risks must be sought in Privacy by Design. When designing applications and infrastructures, privacy risks must be taken into account from the outset.

Other guarantees
Insofar as RFID applications involve personal data, the existing legal framework applies. However, there are also some grey areas in which it might become necessary to clarify or elaborate standards.
The development of new restrictive measures at too early a stage may stifle innovations, yet if such measures are taken too late, the social detriment may become irreversible. Given the speed at which RFID is developing, if balanced viewpoints on the use of the technology are to be formed it seems wise at this stage to place the emphasis mainly on the possibilities that Privacy by Design can offer for building in guarantees of responsible application.

Awareness
All spheres of society need to be aware of the obligations, rights and possibilities applicable to them in environments in which RFID is used.
- *The people affected*

The people affected – citizens, consumers – can contribute, in organised fashion or otherwise, to social discourse about RFID. They have the right to information on the application of the technology, for example as a result of the clear and complete labelling of goods. Where possible, the people affected must have the option of renouncing the use of RFID to process data about them. Moreover they must also be able to view the data stored about them using RFID and have recourse to a good complaints resolution system for potential abuses or improper use.
- *The parties applying the technology*

If it is not sufficiently evident that the use of RFID carries privacy risks, it is advisable not to use it. It is not always appropriate to switch to a new technology. The use of RFID must be visible and transparent, proportional and safe. This aim may be served by collaborative projects to develop codes of conduct and best practices and to conduct audits. The provision of information to the public is essential.
We must guard against the accumulation of data acquired using RFID.
Finally, we must avoid the situation wherein the costs associated with counterbalancing RFID-related risks would have to be passed on to the people affected. These people must not, for instance, be penalized with higher prices or longer waiting times if they choose RFID-free alternatives.
- *The government*

Government authorities must not be focused on using RFID solely to be able to have ever more data at their disposal. Citizens must have confidence that the government is using RFID in a responsible way. As a special user of the technology, the government must assure itself of

optimum security facilities in a number of areas. It also has a role in stimulating the sharing of knowledge and research, both nationally and internationally, and in public information.

- *System developers*

System developers and designers of ICT tools must test RFID applications not just for their technical aspects, but also for their ability to ensure compliance with privacy regulations. Technology-based measures are usually the preferred option for containing risk.

Bijlage 2

Sydney Statement

INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS

RESOLUTION ON RADIO-FREQUENCY IDENTIFICATION
Final Version 20 November 2003

Following a proposal by the Data Protection and Access to Information Commissioner Brandenburg, the Independent Center for Privacy Protection Schleswig-Holstein, Germany, the Spanish Data Protection Agency and the Data Protection Commissioner of the Canton Zug, Switzerland, the International Conference resolves that:

Radio-frequency identification (RFID) technology is increasingly being deployed for a variety of purposes. While there are situations in which this technology can have positive and benign effects, there are also potential privacy implications. RFID tags are so far primarily used to identify and manage objects (products) to control the supply chain or to protect the authenticity of the product brand; however, they could be linked with personal information such as credit card details and even used to collect such information, or to locate or profile persons possessing tagged objects. This technology could allow for the tracing of individuals and for linking collected information with existing databases.

The Conference highlights the need to consider data protection principles if RFID tags linked to personal information are to be introduced. All the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology. In particular
a) any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;
b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way ;
c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and
d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.

These principles should be taken into account when designing and using products with RFID.

The remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process, would raise additional privacy concerns.

The Conference and the International Working Group on Data Protection in Telecommunications will monitor closely the technological developments in this field in greater detail in order to ensure the respect for data protection and privacy in the context of "ubiquitous computing".

Explanatory Note:

Radio-frequency identification tags (RFID tags) are currently being tested and increasingly being used as a more advanced form and possible replacement of bar codes ("smart labels"). The size of these microchips is about 1/3 of a millimetre (and smaller – "smart dust"). Most of

them operate as passive transponders (without batteries) by listening to radio signals sent by transceivers (RFID readers) and using the energy of the received radio signal to reflect and answer it. Active RFIDs have a greater range (depending on the readers used). Since prices for RFID microchips and readers are dropping their widespread deployment becomes increasingly economically viable. RFID tags are likely to become essential drivers of ubiquitous (or pervasive) computing. Due to their storage and capacity for interactive communication they are far more powerful than bar codes. In addition they provide for unique identification of each tagged unit whereas bar codes are identical for every unit of the same product.

RFID tags can be used to install "smart shelves" in stores in order to better manage the supply chain and facilitate the replenishments of goods or supplies (e.g. the case of Gillette razors). They may also be used for easy (contact-less) payment at the point of sale especially if linked with credit cards. Furthermore an employer may use the technology to tag his property in order to reduce theft by employees. They could be linked with video surveillance cameras to check employee as well as customer behaviour. Specific documents may be tagged to be traced more easily in an office. Identity cards as well as travel documents (passports, visas) may be equipped with RFID tags. More recently the European Central Bank has announced that Euro notes will be issued with RFID tags in order to fight counterfeiting and money laundering as well as to control circulating notes. Washable RFID tags can be embedded in clothes ("wearable computing") in order to prevent or detect counterfeiting of specific brands and to prove the authentic manufacture of the product. Other possible applications range from car keys (immobilizers) to container management.

The RFID technology has numerous privacy implications. This is obvious in the case of implanted microchips But also in the more widespread case of tagged objects and goods undoubtedly the information transmitted also refers to the person carrying or wearing (or otherwise associated with) a tagged item or a "constellation" of brands thereby revealing the individual's taste. Therefore personal data can be processed and transmitted or read with the help of RFIDs or at least such object-related information can easily be linked with personal information (e.g. when a credit card is used for buying the tagged item). RFID tags have the potential of tracking the movements of a person who possesses or handles tagged objects. Plans to afford technical devices legal protection against circumvention may prevent data subjects from disabling or deactivating RFID tags which function in a privacy-unfriendly way (e.g. after having paid and left the shop).

Since this issue has led to a growing public debate in a number of countries it is recommended that the International Conference addresses the related privacy problems at this stage in order to encourage privacy-friendly solutions which have been proposed. The International Working Group on Data Protection in Telecommunications at its 34th meeting in Berlin on September 2 and 3, 2003, has expressed its support for this proposal.

Bijlage 3

Enige literatuur

Er is inmiddels zeer veel geschreven over RFID en privacy. Naast de in deze publicatie al eerder aangehaalde literatuur worden hieronder enkele publicaties uitgelicht. Ook tijdens RFID-bijeenkomsten zijn er zienswijzen naar voren gebracht die hebben bijgedragen aan de vorming van CBP-denkbeelden of die CBP-zienswijzen hebben aangescherpt.

Cavoukian 2004
Ann Cavoukian Ph. D., T**ag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology,** Ontario: Information and Privacy Commissioner/Ontario februari 2004

ECP.NL 2005
ECP.NL, **Privacyrechtelijke aspecten van RFID**, mei 2005, ISBN 9076957142

WP29, 2005
WG29, **Working document on data protection issues related to RFID technology 105**, 19 januari 2005

WP29, 2005
WG29 , **Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology**, WP 111 28 juli 2005

Garfinkel 2002
Simson Garfinkel, **An RFID Bill of Rights, Technology review MIT,** oktober 2002

In de serie Achtergrondstudies en verkenningen zijn verschenen:

A.H.C.M. Smeets, **Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde.** A&V 28; College bescherming persoonsgegevens, Den Haag, 2004

Drs. S. Lieon en mr. M. Th. van Munster-Frederiks, **De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers.** A&V 27; College bescherming persoonsgegevens, Den Haag 2004.

Mr. drs. T.F.M. Hooghiemstra, **Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg.** A&V 26; College bescherming persoonsgegevens, Den Haag 2002.

Dr. J.A.G. Versmissen en mr. drs. A.C.M. de Heij, **Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid.** A&V 25; College bescherming persoonsgegevens, Den Haag 2002.

Mr. M.M.M. van Eijk en drs. W.J. van Helden, **Klant te koop. Privacyregels voor adressenhandel.** A&V 24; Registratiekamer, Den Haag 2001.

G.W. van Blarkom en drs. J.J. Borking, **Beveiliging van persoonsgegevens**. A&V 23; Registratiekamer, Den Haag 2001.

Dr. J.A.G. Versmissen, **Sleutels van vertrouwen, TTP's, digitale certificaten en privacy**. A&V 22; Registratiekamer, Den Haag 2001.

Mr. drs. J.H.J. Terstegge, **Goed werken in netwerken. Regels voor controle op e-mail en internetgebruik van werknemers**. A&V 21; (1e druk; Registratiekamer, Den Haag 2000) 2e druk herzien door drs. S. Lieon, College bescherming persoonsgegevens, Den Haag 2002.

Dr. R. Buitenhuis, drs. N.G.M. van Campen, drs. W.J. van Helden, dr. H.H. de Vries, **Bankverzekeraars en privacy. Gegevensverwerking in financiële conglomeraten**. A&V 20; Registratiekamer, Den Haag 2000.

drs. W.J. van Helden, **Herkomst van de klant. Privacyregels voor etnomarketing**. A&V 19; Registratiekamer, Den Haag 2000.

R.W.A. Wishaw, **De gewaardeerde klant. Privacyregels voor credit scoring**. A&V 18; Registratiekamer, Den Haag 2000.

Mr. M.J.T. Artz en mr. M.M.M. van Eijk, **Klant in het web. Privacywaarborgen voor internettoegang**. A&V 17; Registratiekamer, Den Haag 2000.

Mr. J. de Zeeuw, **Informatieverstrekking. Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving**. A&V 16; Registratiekamer, Den Haag 2000.

Dr. R. Hes, mr. J.J. Borking en mr. drs. T.F.M. Hooghiemstra, **At face value. On biometrical identification and privacy**. A&V 15; Registratiekamer, Den Haag 1999.

Mr. M.J.T. Artz **Koning Klant. Het gebruik van klantgegevens voor marketingdoeleinden**. A&V 14; Registratiekamer, Den Haag 1999.

Mr. J.J. Borking, **Intelligent software agents and privacy**. A&V 13; Registratiekamer, Den Haag 1999.

Mr. drs. T.F.M. Hooghiemstra, **Privacy & Managed care**. A&V 12; Registratiekamer, Den Haag 1998.

R. Hes en mr. J.J. Borking, **Privacy-enhancing technologies: the path to anonimity**. A&V 11 revised edition; Registratiekamer, Den Haag 1998.

Mr. J.J. Borking, mr. M.J.T. Artz en L. van Almelo, **Gouden bergen van gegevens. Over data-warehousing, datamining en privacy**. A&V 10; Registratiekamer, Den Haag 1998.

Mr. C.G. Zandee, **Doelbewust volgen. Privacyaspecten van cliëntvolgsystemen en andere vormen van gegevensuitwisseling**. A&V 9; Registratiekamer, Den Haag 1998.

Mr. J. de Zeeuw, **Informatiegaring door de fiscus. Privacybescherming bij derdenonderzoeken**. A&V 8; Registratiekamer, Den Haag 1998.

Mr. dr. P.C. Ippel, **Gegeven: de Genen. Morele en juridische aspecten van het gebruik van genetische gegevens.** A&V 7; Registratiekamer, Den Haag 1996.

Mr. H.J.M. Gardeniers, **Chipcards en privacy. Regels voor een nieuw kaartspel**. A&V 6, Registratiekamer, Den Haag 1995.

H. van Rossum, **Privacy-enhancing technologies: the path to anonymity, volume I and II**. A&V 5; Registratiekamer, Den Haag 1995.

Mr. drs. A.F. Rommelse, **Zwarte lijsten. Belangen en effecten van waarschuwingssystemen**. A&V 4; Registratiekamer, Rijswijk 1995.

Mr. drs. A.F. Rommelse, **Ziekteverzuim en privacy. Controle door de werkgever en verplichtingen van de werknemer**. A&V 3; Registratiekamer, Rijswijk 1995.

J.P.M. van Casteren, **Bevolkingsgegevens: Wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden**. A&V 2; Registratiekamer, Rijswijk 1995 (niet meer beschikbaar).

Mr. B.J.P. Hulsman en mr. dr. P.C. Ippel, **Personeelsinformatiesystemen – de Wet persoonsregistraties toegepast**. A&V 1; Registratiekamer, Rijswijk 1994 (niet meer beschikbaar).

Vrijwel alle publicaties van het CBP kunt u inzien en/of downloaden van de website www.cbpweb.nl. Voor het toezenden van meerdere gedrukte publicaties worden kosten in rekening gebracht.

COLLEGE BESCHERMING PERSOONSGEGEVENS

Juliana van Stolberglaan 4-10
Postbus 93374
2509 AJ Den Haag

T 070 888 85 00
F 070 888 85 01
E info@cbpweb.nl

WWW.CBPWEB.NL