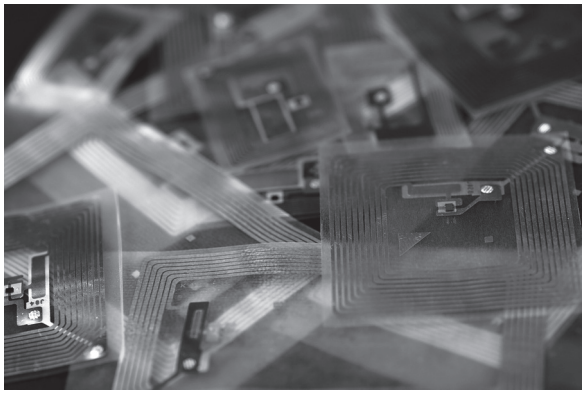
# Zappen, Sniffen en Klonen: interventies met RFID-chips

***Lonneke van der Velden & Mark Ponte***

De ontwikkeling van nieuwe technologieën levert nieuwe vragen op over de *surveillance society.* Met het oog op de nabije toekomst bestaat de zorg of mensen nog uit controlenetwerken kunnen blijven. Dit artikel bespreekt enkele praktijkvoorbeelden van (artistiek) activisme en met name de omgang met *Radio Frequency Identification* (RFID). Middels technische bewerking kunnen kunstenaars en activisten interveniëren met informatie op RFID-chips. Daarnaast is RFID op te vatten als een interactief netwerkmiddel. Het RFID-debat moet niet alleen gaan over de technologie toelaten versus weren, maar ingaan op in welke vorm aan de informatienetwerken deel te nemen. Het is bovendien van belang toegankelijke en praktische middelen te ontwikkelen, waarmee mensen de technologie kunnen verkennen en er op in kunnen spelen.

## Inleiding

We raken steeds meer gewend aan het idee dat technologie deel uitmaakt van ons dagelijkse leven. Bepaalde technologieën registeren onze persoonlijke gegevens of gedragingen. Soms ervaren we dat als een wellicht vervelende maar noodzakelijke veiligheidsmaatregel, en soms maakt het dingen efficiënter, denk aan de OV-chipkaart. Het toenemend gebruik van technologieën ten behoeve van toezicht leidt tot de vraag of wij nog enige mate van controle hebben over de informatie die er over ons gegenereerd wordt. Hebben wij nog enige inbreng in de manier waarop overheden en instanties onze gedragingen in de gaten houden?
Om hier iets over te kunnen zeggen, wordt in dit artikel uitgeweken naar enkele praktijkvoorbeelden van surveillance en reacties hierop. De centrale vraag is op welke manier activisten en kunstenaars interveniëren met surveillancetechnologie. Daarbij wordt gekeken naar huidige toepassingen en plannen met RFID. Er is nog veel onduidelijk over wat voor toepassingen deze technologie zal kennen, en wat dit betekent voor de rol van het individu en de bescherming van haar persoonsgegevens. In het werk van activisten (vaak hackers) en kunstenaars kunnen we niet alleen kritische en crea-




tieve toepassingen van deze technologieën zien: door het toe-eigenen van de technologie wordt wellicht ook een nieuwe verhouding van het individu tot deze technologieën zichtbaar. Na een korte uiteenzetting over de maatschappelijke achtergronden en effecten van de invoer van surveillancetechnologie, wordt ingegaan op de thema's surveillance en verzet. Vervolgens dienen verschillende voorbeelden van artistiek en activistisch gebruik van RFID als casus om te bekijken op welke manier interventies met en in de technologie in praktijk gebracht worden.

### *Radio Frequency Identification* (RFID)

RFID wordt gezien als de digitale opvolger van de streepjescode. Door middel van radiogolven kan informatie van 'getagde' producten of objecten worden gelezen door *readers*. Deze tags zijn voorzien van een uniek identificatienummer dat het mogelijk maakt een object te herkennen en ermee te communiceren. RFID bestaat op zich al sinds de Tweede Wereldoorlog, maar staat de laatste tijd erg in de belangstelling. RFID werd vroeger vooral gebruikt voor de transportindustrie, tegenwoordig is RFID alom tegenwoordig. Zo worden er RFID-tags in winkels gebruikt voor voorraadbeheer en als techniek om diefstal te voorkomen. Veel ingrijpender is het gebruik van RFID voor de identificatie van personen, zoals in de gevangenis in Lelystad, waar alle gevangenen zijn voorzien van een armband met een RFID-tag. Hiermee kunnen zij hun persoonlijke entertainmentsysteem bedienen, maar worden zij ook permanent gevolgd en gaat er een alarm af als iemand zich niet aan het afgesproken programma houdt. Een beroemd en extreem voorbeeld van het taggen van personen is de Baja Beachclub in Rotterdam, waar vaste klanten vrijwillig een aan hun creditcard gekoppelde chip in hun lichaam kunnen laten implanteren om betalingen te kunnen doen.

Maar niet alleen gevangenen of klanten van exclusieve discotheken hebben hiermee te maken. Sinds eind 2006 zijn namelijk alle nieuwe Nederlandse paspoorten voorzien van een RFID-chip, met digitale persoonsinformatie, waaronder een kleurenpasfoto, naam en andere persoonsgegevens. Vanaf 21 september dit jaar komen daar ook vingerafdrukken bij. Deze chips zijn met de juiste apparatuur op afstand af te lezen. Ook de OV-chipkaart en diverse creditcards zijn voorzien van dit soort chips. In de praktijk komt het er op neer dat steeds meer mensen, zonder dat ze het weten, 'getagd' zijn en mogelijk 'gelezen' worden.

In de toekomst zullen er steeds meer toepassingen komen van RFID, niet alleen als betalingsmiddel, identificatie of volgsysteem, maar ook om contact te maken tussen verschillende gebruiksvoorwerpen. Men spreekt dan ook wel van het 'Internet der dingen': 'The Internet is undergoing a major evolution that will see more and more physical objects connected to it. As such, previously unconnected objects, such as books, clothes, food, will progressively be linked to the network.' (European Commission, 2 juni 2009). Uiteindelijk zal iedereen hier mee te

maken krijgen en RFID is de voorloper daarvan: '*RFID marks the dawn of the Internet of Things.*' (Santucci 2009, 5).

## Technologie en toezicht in Nederland

RFID moet een hoop processen effectiever en veiliger doen verlopen (RFID Platform Nederland). Ook wordt verwacht dat RFID een belangrijke rol zal gaan vervullen als het gaat om de datavergaring over personen (Rathenau 2007, 43). In de afgelopen jaren hebben de mogelijkheden van overheden en instanties om inzicht te krijgen in personen een enorme vlucht genomen. Iedere burger in Nederland is verplicht om te allen tijde een identificatiebewijs op zak te hebben om die desgewenst aan de politie te kunnen tonen. Sinds 2001 is het gebruik van cameratoezicht in de openbare ruimte explosief gestegen. Binnenkort zijn aanbieders van telecommunicatie verplicht om het belgedrag van klanten voor een periode van minimaal een jaar te bewaren, en het e-mail-, internetverkeer voor een periode van een half jaar. Onze paspoorten, creditcards en – als het aan het CDA ligt – zelfs onze fietsen worden binnenkort van RFID-chips voorzien (vgl. www.rfidnederland.nl).

Met name in de opsporing zijn de mogelijkheden om burgers te onderzoeken verruimd in de laatste decennia.[(1)] Ook andere organisaties dan de overheid doen aan dataverzameling, wat overigens niet betekent dat deze informatie alleen bedrijfsdoeleinden dient. Geprivatiseerde organisaties zijn van groeiende betekenis voor de opsporing omdat zij informatie kunnen verschaffen over uiteenlopende kenmerken van burgers (Rathenau 2007, 69). Informatie die aanvankelijk wordt geregistreerd voor specifieke doeleinden (de kwaliteit van het reisverkeer, marketing, efficiëntie) maakt dus deel uit van bredere kennisnetwerken die ook de onderzoeksmogelijkheden van overheden ten goede komt.

Een van de effecten is dat 'normale' (onverdachte) personen steeds meer onderwerp worden van toezicht. De manier van onderzoek doen ontwikkelt zich steeds meer in de vorm van 'pro-actieve' verkenningen, aan de hand van gedragingen, familie, of vriendenkring. Ook worden burgers steeds transparanter voor overheden. Er bestaat een scala aan technieken voor het vastleggen van iemands gedragingen (zoals communicatie, financiële transacties, reisgegevens) welke vervolgens naast risicoprofielen worden gelegd (idem, 68). Het geheel aan maatregelen maakt dat meer burgers op een meer ingrijpende manier in de gaten worden gehouden.

### *Surveillance society*

Door toenemende controlemogelijkheden bij zowel overheden als private instanties wordt wel eens gezegd dat wij in een '*surveillance society*' leven, een samenleving gekenmerkt door een doorlopend toezicht. De manier waarop toezicht plaatsvindt in de huidige technologische samenleving komt niet overeen met de standaarddefinitie van een directe observatie van een verdacht persoon (Marx 2000, 10). Hedendaags toezicht richt zich minder op verdachte personen, en meer op relevante contexten. Toezicht kan, in plaats van direct, op grote afstand plaatsvinden en bestaat niet zozeer uit visuele observatie, maar uit de combinatie van verschillende waarneembare indrukken.

Volgens Gary Marx maken technische middelen het mogelijk om boven het direct waarneembare en vrijwillig kenbaar gemaakte uit te stijgen: het moderne surveillance kijkt niet naar wat een bepaald iemand op een specifiek moment laat zien, maar relateert contexten en patronen. Het baseert zich op data die op zichzelf niet interessant zijn maar samen genomen des te meer (idem, 12).

Surveillance vindt plaats binnen netwerken: naast de surveillant en de gesurveilleerde zijn er tal van actoren en elementen die meespelen, zoals commerciële ondernemingen, verschillende soorten overheden, NGO's, en de technologieën zelf (Martin et al. 2009, 213). Sommige auteurs gebruiken daarom het begrip 'surveillant assemblage' om surveillancetechnieken van deze tijd te typeren (Haggerty & Ericson 2000; Martin et al. 2009). Die term (ontleend

aan Deleuze) zou meer recht doen aan huidige vormen van surveillance, waarbij de objecten van controle vanuit hun locatie worden opgedeeld en geabstraheerd naar informatiestromen, verplaatst en herschikt voor analyse aan de hand van bestaande categorieën (Haggerty & Ericson 2007, 4).[2]

Behalve informatievergaring heeft surveillance ook effecten. Lyon omschrijft surveillance als 'any collection and processing of personal data, whether identifyible or not, for the purpose of influencing or managing those whose data have been garnered' (Lyon 2001, aangehaald in Fernandez & Huey 2009, 199). De invloed waar hier naar gerefereerd wordt gaat niet om een instrumentele macht (zoals het gebruiken van informatie om iemand te arresteren), maar om een subtieler effect: degenen onder surveillance worden 'bewerkt' door de aanwezigheid van toezicht.

## Verzet

Wat doen burgers die steeds 'ingrijpender' in de gaten worden gehouden? Is er ruimte voor zoiets als 'verzet' in een *surveillance society* waarin technologie zo'n belangrijke rol speelt? Het verzetsthemanummer van *Surveillance and Society* stelt dat verzet in de huidige surveillance society moeilijk te conceptualiseren valt en dat er weinig voorbeelden concreet uitgewerkt zijn. De trend is om surveillance als een bedreiging en totaliserend systeem te zien (Fernandez & Huey, 198). Bovendien blijft verzet vaak beperkt tot een individuele praktijk. Zo spreken populaire beschrijvingen van surveillance over persoonlijke beschermingsmechanismen, maar ze negeren het idee dat er ook collectieve of georganiseerde vormen van verzet tegen surveillance zouden kunnen bestaan.

Een scala aan voorbeelden van technieken van individueel 'alledaags verzet' is te vinden in Marx (2003). Hij noemt dit 'neutralisatietechnieken'. Onder de elf categorieën die hij onderscheidt, valt het uitstoten van valse informatie, controleurs die een oogje dichtknijpen en het filmen van controlerende instanties ('de bal terugkaatsen').

Ook bij activistisch ingestelde projecten bestaat de tendens om in het individuele te blijven hangen, stelt Monahan (2006). Dit laat hij zien aan de hand van een aantal vormen van (artistiek) activisme rondom het gebruik van *Closed Circuit Television* (CCTV). Hij stelt ter discussie of deze vormen van activisme te beschouwen zijn als politieke interventies. Hij maakt in zijn bespreking een onderscheid tussen 'technische' en 'sociale' interventies, wat verwijst naar het niveau waarop de interventies plaatsvinden. Voorbeelden van technische interventies zijn de 'i-map' van het *Institute for Applied Autonomy,* een kaart met 'cameraroutes' zodat je weet hoe je moet lopen en ®™arks '*Guide to Closed Circuit Television destruction*', een handboek dat ingaat op het hoe en waarom van het stukmaken van camera's. Voorbeelden van sociale interventies zijn Steven Manns '*Shooting Back project',* waarbij mensen die meewerken met CCTV de camera op zichzelf gericht krijgen en de *Surveillance Camera Players,* een groep artiesten die performances doet voor bewakingscamera's in publieke ruimtes en zo, door te interveniëren, bewakers en passanten confronteert met de routinematigheid van bewaking.

Volgens Monahan zijn deze vormen van 'contrasurveillance' met name gelokaliseerd op het niveau van de relatie tussen gesurveilleerde en surveillant. Activisten vragen daarmee aandacht voor hoe bewakingscamera's deel zijn van ons dagelijkse leven, maar in mindere mate wordt het publiek zelf actief bij de projecten betrokken. Bovendien construeren de activisten de problematiek voornamelijk in geïndividualiseerde en geabstraheerde termen, en daarmee ook hun methodes van interveniëren. Daardoor slagen ze er ook niet in om de institutionele en beleidskanten van surveillance te raken, of de culturele assumpties waarop het systeem gedijt (Monahan 2006, 517). Ze 'missen' als het ware de kracht van sociale bewegingen (idem, 531). Sterker nog: volgens Monahan kunnen de projecten leiden tot een versterking van het surveillancesysteem: het systeem leert van de activisten over haar eigen zwakke plekken (vgl. Haggerty 2007, 20).

De activisten slagen er dus niet in een wijziging te bewerkstelligen van de termen op grond

waarvan surveillance plaatsvindt. Monahan lijkt niet alleen te staan in zijn teleurstelling: 'The victories of resistance are usually immediate and case-specific' (Haggerty 2007, 20). Als er al zoiets als 'verzet' plaatsvindt dan is dat lokaal of ontwijkend: 'Resistance is typically not motivated by a desire to eliminate or modify systems, but to evade their grasp' (ibidem).

Maar wat verwachten we precies van 'verzet' in de huidige surveillance society? De huidige mechanismen van surveillance worden door de in dit artikel eerder genoemde auteurs omschreven als complexe systemen (Marx 2003), netwerken (Martin et al. 2009) en assemblage (Haggarty 2000). Volgens Martin et al. verbreedt het idee van surveillance als 'assemblage' ook het perspectief op verzet. De auteurs pleiten voor een *multi-actor perspective*, met oog voor (onderdelen van) autoriteiten die deel uitmaken van verzetstechnieken, mensen die in eerste instantie ongezien zijn, en soms de technologieën zelf.

Een perspectief met aandacht voor de gevarieerdheid aan actoren sluit aan bij de poging die men in het wetenschapsonderzoek (sociaal-wetenschappelijk onderzoek naar wetenschap en technologie) onderneemt om tot een complexer technologiebegrip te komen. Daarbij wordt technologie binnen een breder netwerkperspectief beschouwd en sociale en technische factoren niet rigide onderscheiden (Rip 1995). Technologie is niet iets externs dat we instrumenteel kunnen inzetten ('we kunnen het gebruiken voor...') of iets dat ons domineert (we zitten dan in de slachtofferrol of zijn weigeraar). Technologie hangt samen met de sociale omgeving waarin het zich ontwikkelt en een zekere flexibiliteit kent. Technologie zou daarom beter opgevat kunnen worden als een 'sociaal-technisch systeem'.[3] De flexibiliteit binnen dat systeem is afhankelijk van hoe actoren zich onderling positioneren, iets wat een vorm van 'politiek' genoemd zou kunnen worden:

'The main point about the assumption that politics are embedded in the design of socio-technical systems is that a challenge to authority can also be directed at technology design in addition to or instead of being directed at technology policies or the lifestyles that govern patterns of use' (Hess 2009, 518).[4]

Bij de bespreking van CCTV-activisme onderscheidt Monahan technische van sociale interventies. Ondanks dat hij wijst op verschillende studies over technologie waarin is aangetoond dat technische en sociale aspecten met elkaar verbonden zijn (Monahan 2006, 517), blijven de implicaties van die inzichten in zijn studie onuitgewerkt. Dit artikel neemt een andere insteek waarbij gepoogd wordt de technologie op een breder niveau te bekijken. Wat voor potentieel heeft RFID-technologie? Wat voor verbanden kunnen er met die technologie aangegaan worden? Een technische interventie brengt misschien geen sociale beweging tot stand, maar kan mogelijk wel invloed uitoefenen op hoe het netwerk waarbinnen kennis gegenereerd wordt zich ontvouwt.

## Interventies met RFID

RFID gaat een belangrijke rol spelen in het 'Internet der dingen': het netwerk waardoor wij binnen enkele decennia in verbinding zullen staan met objecten, computers, internetcommunicatie, etc. De eerste reacties op het groeiend gebruik van RFID-chips en hun mogelijke impact op privacy of controle lijkt er een te zijn van persoonlijke beschermingsmechanismen: hoe voorkomen we dat we getagd worden? De discussie over RFID wordt bovendien gevoerd in legalistische termen: er moet wettelijk vast gelegd worden of we een *opt-out* of een *opt-in* beleid willen (*NRC Next*, 19 augustus 2009). *Opt-out* is als de chips standaard geactiveerd zijn, tenzij je aangeeft dat ze uitmoeten. *Opt-in* is als de chips zijn gedeactiveerd tenzij je aangeeft dat ze aanmoeten (vergelijk het met het Nederlandse donorbeleid dat werkt als een *opt-in* beleid: je geeft je lichaamsmateriaal na je dood niet weg, tenzij je aangeeft dat wel te willen). Om aan het Internet der dingen te kunnen ontkomen denken ethici na over *the right to silence*, het recht om afgesloten te zijn van het Internet der dingen. Kunstenaars werken aan afsluitbare ruimtes. Zo werkt de Britse kunstenaar Stanza aan een *freezone,* een

informatievrije zone zonder netwerk of computers, en maakt de Duitse kunstenares Härtig een non-space, een tent die elektromagnetische straling weert (*NRC Next*, 19 augustus 2009).
Maar de termen waarin dit debat gevoerd wordt (we moeten wettelijk vastleggen dat er de keuze is om de technologie toe te laten of te weren) gaan uit van een instrumenteel technologiebegrip. Uit de praktijk blijkt dat er ook andere manieren en technieken bestaan om met RFID om te gaan. Kunstenaars hebben een belangrijke taak om die manieren bloot te leggen: zij exploreren nieuwe relaties die we met de technologie aan kunnen gaan. Hieronder volgen een aantal voorbeelden van kunstenaars en activisten die werken met RFID-technologie, niet alleen om zich te vrijwaren van de registrerende RFID-readers, maar ook om zich te mengen in de informatiestromen die er gegenereerd worden. Ook zal blijken dat RFID een creatief potentieel heeft voor (sociale) interactie.

## Creatief met RFID

Doordat sinds 2006 ons paspoort is voorzien van een RFID-chip en we bovendien steeds meer pasjes met zo'n chip krijgen is binnenkort bijna iedere Nederlander getagd. En in principe is de persoonsinformatie op die kaarten op afstand leesbaar. Kunstenaars, activisten en andere critici reageren op verschillende manieren met RFID. Hieronder worden vier 'technieken' besproken: het onschadelijk maken van de chip of tags, het detecteren en mogelijk verbergen van tags, het kraken, manipuleren en bewerken van tags, en het creëren met RFID.

*Zapping*
'We have to expect to be surrounded by RFID-Tags almost everywhere within the near future, and they will serve many different purposes. The benefits and risks of this technology and it's use are already being discussed. However, there will be attempts to use RFID-Tags to establish constant surveillance and to further threaten and compromise the privacy of customers (and citizens and even non-citizens, when governments start to use RFID-Tags like the German government already did)' (22C3 2009).
Een mogelijke reactie op RFID als surveillancetechnologie is het onschadelijk maken ervan. Dat gebeurt op twee niveaus. Net zoals bijvoorbeeld een camera, is een RFID-chip te vernielen. Op de videowebsite *YouTube* zijn tientallen filmpjes te vinden over het kapotmaken van RFID chips. Activisten, knutselaars en hackers laten zien hoe je chips uit bankpasjes kan demonteren (Federaljackdotcom 2008). Zo blijkt een stevige mep met een hamer redelijk effectief en ook met een paar seconden in de magnetron is een RFID-tag kapot (Imfriggincrazy 2008).
Maar een meer geavanceerde manier van het onklaar maken van RFID-tags is de door hackers ontwikkelde *RFID Zapper*. Dit is een tot klein elektronisch apparaatje omgebouwde weggooicamera die een zeer sterk elektromagnetisch veld genereert dat, net een magnetron, een RFID-chip onschadelijk maakt. Het voordeel van dit apparaat is dat het getagde product zelf niet beschadigd wordt:
'To defend yourself against such [surveillance] measures, you might want a small, simple and relatively appealing gadget to permanently deactivate RFID-Tags around you, e.g., to deactivate RFID-Tags in recently bought clothing or books without damaging them' (22C3 2009).

*Sniffing*
Een andere methode is het opsporen van de informatie die je bij je draagt. Op het multimedia congres Picnic liep in 2007 een man rond met een omgebouwd tennisracket. Op het tennisracket zat een klein elektronisch apparaatje dat was aangesloten op een laptop die heel hard begon te piepen als er een RFID-chip in de buurt was. Deze installatie van de vorig jaar overleden hacker Mark Hoekstra was bedoeld als actie. 'Het was een soort 'public intervention' om duidelijk te maken dat mensen getagd zijn en dat wordt dan publiekelijk gedemonstreerd. Veel mensen hebben namelijk geen idee wat RFID inhoudt en dat zij getagd zijn.' (Interview met Boon 2009).
Normaliter worden mensen pas bewust gemaakt van (de mankementen van) de techno-

logie als er iets mis is, zoals de spectaculaire kraak van de OV-chipkaart (De Winter 2008a), maar over het algemeen weten we weinig van de aanwezigheid van de vele tags in onze omgeving. Bewustwording is dus stap één in het omgaan met RFID. Dat is niet alleen iets waar hackers en techneuten over nadenken, ook het ministerie van Economische zaken heeft een verkennende studie laten verrichten naar de mogelijkheden van een RFID informerend systeem in de vorm van een logo op alle producten voorzien van een tag, maar vooralsnog ziet het er niet naar uit dat zoiets daadwerkelijk ingevoerd gaat worden (Aanbestedingsbrief staatsecretaris van Economische Zaken, 5 februari 2009).

Uiteraard is het zo dat we in veel gevallen eigenlijk niet om de technologie heen kunnen. Wie in Amsterdamse metro wil reizen moet een OV-chipkaart met RFID-chip hebben en ook om het paspoort kom je nauwelijks heen. Wel kun je de chips, met behulp van speciale hoesjes of aluminiumfolie afschermen zodat ze niet meer op afstand te lezen zijn.

Ook zijn er allerlei techneuten aan de slag gegaan om gadgets, installaties en toepassingen te maken waardoor mensen op aanwezige chips geattendeerd worden. Zo werd de hierboven beschreven *RFID racket reader* ontwikkeld door Mark Hoekstra voor het Mediamatic's RFID-hackers Camp (Hoekstra 2007). Kunstenaar en techneut Marc Boon ('*mediator between art and technology*') is dit concept verder gaan ontwikkelen en bedacht de *RFID Sniffer*. Een relatief eenvoudige gadget ter grote van een creditcard met daarop een ledlampje dat gaat branden als het tegen een RFID-chip wordt gehouden. Boon maakte niet alleen het apparaatje, hij ontwikkelde een bouwpakket dat mensen in staat stelt zelf een *Sniffer* in elkaar te zetten en organiseerde verschillende populaire workshops.

Uit een interview met Boon blijkt dat hij zijn workshops en *Sniffers* ziet als een '*awareness project*', waarmee hij mensen niet alleen wil laten zien wat RFID is, maar ook duidelijk wil maken dat het in ieders leven aanwezig is (Interview Marc Boon 2009). Vandaar het actief bezig zijn met een detectieapparaatje. Daarmee kun je mensen echt bewust maken van de steeds toenemende aanwezigheid van RFID. Want hoewel Boon vooral geïnteresseerd is in de sociale en artistieke kanten van RFID ('wat kan ik er mee creëren?') en hij op zich neutraal staat ten opzichte van de technologie, ziet hij ook de risico's in het hebben van te veel vertrouwen in de technologie. Als je RFID gebruikt als een technisch middel om zekerheid of veiligheid te verschaffen dan genereer je daar volgens Boon een kwetsbaarheid mee: als de technologie faalt dan is de veiligheid verbroken. Met zijn *Sniffer* wil hij mensen in staat stellen om te leren wat RFID is, waar het zich allemaal in bevindt en wat het doet. Wat mensen vervolgens met die informatie doen (spelen, slopen, blokken, kraken of hergebruiken) moeten ze vervolgens zelf weten:

'Die *Sniffer* kan mensen bewust maken van het feit dat zij gegevens of identificatie bij zich dragen die, zonder dat zij het weten, gelezen kan worden. Omdat het een draadloze technologie is kunnen de pasjes gelezen worden zonder dat je het zelf door hebt. Dat is een essentieel verschil met de barcode of een pasje met een foto dat je laat zien, dan weet je dat je iets laat zien en hebt de keuze omdat wel of niet te doen. Als je gegevens onbewust gescand kunnen worden bij een deur of poortje, dan heb je daar geen controle over. De *Sniffer* is een middel om inzicht te geven of je tags bij je hebt en er over na te denken wat je daarmee moet.' (Interview Boon 2009)

*Cloning*

Je kunt tags niet alleen detecteren, uiteindelijk kun je ze lezen, kopiëren en zelfs manipuleren. Dat is problematisch als er persoonsgegevens in het geding zijn terwijl RFID juist de veiligheid moet verbeteren. In de afgelopen jaren is duidelijk geworden dat de toepassing van RFID op OV-chipkaart, creditcard en paspoorten door gedreven hackers vrij snel te kraken en te kopiëren is, vul maar eens 'RFID' in bij het zoekscherm van websites als *Youtube* of *Googlevideo*. Zo laat hacker Pablos Holman zien hoe je met een apparaatje van acht dollar en een laptop de persoonsgegevens van een American Express Credit Card kan lezen: niet alleen het

creditcardnummer, maar ook de naam en de geldigheidsduur (Boingboingtv 2008).
Eind 2007 werd duidelijk dat de Milfare-chip op de Nederlandse OV-chipkaart gehackt was. Karsten Nohl en Henryk Plötz toonden op *het Chaos Cumputer Camp* in Berlijn hoe je deze chip kan kraken (Nohl & Plötz 2007). Niet lang daarna werden de goedkope wegwerpkaart en de meer ingewikkelde kaarten met daarop ook reisinformatie gekraakt (De Winter 2008b).
In augustus 2008 lukte het beveiligingstester Jeroen van Beek van KPMG en de Universiteit van Amsterdam om de chip op zijn paspoort te kopiëren (klonen) en deze kopie vervolgens aan te passen. Het lukte Van Beek om die nieuwe chip te voorzien van foto's van Elvis en Osama Bin Laden: door de originele chip met een hamer kapot te slaan, wordt alleen de kloon uitgelezen door controleapparatuur (De Winter 2008c). Het lezen en kopiëren van kaarten kan ook op afstand. Hacker Chris Paget liet in een filmpje op *Youtube* zien hoe hij met relatief goedkope computerapparatuur in zijn auto al rijdend in staat was RFID-paspoorten te detecteren en, zonder dat de eigenaars ook maar iets merkten, zelfs te kopiëren (Goodin 2009).
Volgens Marc Boon is het verbazingwekkend hoe snel nieuwe toepassingen en beveiligingen gekraakt worden. De oorzaak ligt hierbij gedeeltelijk bij een zeer gedreven, internationaal georiënteerde wereld van hackers, die elkaar de loef af willen steken met wie het eerst de nieuwste beveiliging kraakt. 'Een groep van misschien wel duizenden mensen kan natuurlijk makkelijk winnen van een bedrijf, dat misschien vijf man heeft werken op de researchafdeling en die hebben er misschien tien jaar over gedaan om een heel systeem te bedenken. Zoals met de Philips Mifare. En dan is dat binnen twee jaar tijd door een wereldwijde groep hackers gekraakt.'
Boon, die de *Sniffer* oorspronkelijk ontwierp om vanuit zijn technische interesses meer van de technologie van RFID te leren, is momenteel bezig met een *DIY [Do It Yourself] RFID Clone pakket* (Interview Boon 2009). De *Cloner* moet net als de *Sniffer* een handzaam apparaatje worden dat met een druk op de knop te bedienen is. Het verschil met de *Sniffer* is dat de tag niet alleen gedetecteerd wordt, maar ook gekopieerd (gekloond), waardoor het apparaatje zich kan voordoen als de gekloonde tag, dus als een bepaald boek, een cd of een toegangspas voor een kantoor.
Het spelen met RFID ligt vaak op de grens tussen kunst en activisme. Zoals de meerdelige installatie *Zapped!* van onder anderen de kunstenaars Beatriz da Costa en Heidi Kumao. Dit is een installatie met een instructievideo over RFID en de zeer tot de verbeeldingsprekende *Roach Release station*: een aantal kakkerlakken met een RFID-tag op hun rug. Het idee is dat je deze kakkerlakken kunt loslaten op plekken waar intensief gebruik wordt gemaakt van RFID, zoals een distributiecentrum. De tags zijn geprogrammeerd met een korte boodschap die er voor moet zorgen dat de scanners in zo'n gestandaardiseerde omgeving in de war raken door de onbekende tags (Debatty 2008). In combinatie met de hierboven genoemde mogelijkheid tot klonen, zou je natuurlijk niet alleen het systeem in de war kunnen brengen: je kan het zelfs voor de gek houden door bijvoorbeeld een kakkerlak voor een blik doperwten aan te laten zien.

*Real life social networking*
Een laatste interessante mogelijkheid met RFID is *creatie*: het aangaan van nieuwe verbindingen. Het kan ook gebruikt worden voor installaties en voor *real life social networking.* Miljoenen mensen maken tegenwoordig gebruik van websites als *Hyves*, *Facebook* of *LinkedIn*. Met RFID kunnen sociale netwerken ook zonder computer opgebouwd en bijgewerkt worden.
Wederom kunnen hier Mediamatic en PicNic als voorbeeld dienen. De afgelopen jaren kregen de bezoekers van PicNic een zogenaamde IkTag, een RFID-tag die gekoppeld was aan een profiel op een website. Met de tag konden mensen zich begeven in een multimediale omgeving. Zo kon er bij een foto-installatie een foto voor het online profiel worden gemaakt en was er een *Friend Drink Station* voor oude en nieuwe sociale contacten. Congresbezoekers werden hier gestimuleerd om met nieuwe mensen een drankje te drinken. Bij het station kon je je aan elkaar voorstellen en werd er met behulp

van de tag automatisch een visitekaartje uitgeprint, om uit te wisselen. Uiteraard werd je ook in het online sociale netwerk aan elkaar gekoppeld (Mediamatic 2009; Interview Boon 2009). Een vergelijkbaar systeem gebruikt het Instituut voor Beeld en Geluid om tentoonstellingen persoonlijk te maken. Met behulp van een RFID-tag kunnen niet alleen bepaalde multimediarepresentaties worden bekeken, ook kunnen dingen opgeslagen worden in een persoonlijke account, waarop je later thuis de opgeslagen zaken terug kan bekijken (Phi Data 2009). RFID kan dus een middel zijn voor interactie tussen de online en de offline wereld.

## Conclusies: interveniëren met het Internet der dingen

Wat kunnen we verwachten van RFID? Ten eerste blijkt dat het implementeren van RFID, ten behoeve van het veiliger maken van processen een schijnveiligheid creëert. Hoewel het de bedoeling is dat bijvoorbeeld paspoorten beter beveiligd zijn tegen identiteitsfraude en diefstal is het juist mogelijk geworden om gegevens op afstand in te zien, en om persoonsgegevens te kopiëren, manipuleren en hergebruiken. Iets dergelijks geldt ook voor de creditcardindustrie. Hacker Pablos Holman zegt daarover: 'The credit card industry understands very clearly that creating a secure system isn't really a priority, creating a system that feels secure to the user is. In reality it is easier for me to get numbers now than it was with the old system. Now all I got to do is get near your ass with my reader' (Boingboingtv 2008).

Welke ruimte hebben criticasters hier? Eerder is aangegeven dat in de huidige surveillance society verzet moeilijk te conceptualiseren valt. Ook worden activistische projecten met surveillancetechnologie door analisten bekritiseerd omdat ze het individuele niveau niet weten te overstijgen. Maar als je het idee volgt van een 'surveillance assemblage', dan is het spelen met (in dit geval) RFID meer dan slechts een 'technische interventie'. Het is het bewerken van die assemblage. Via het detecteren en klonen van RFID-chips kan men interveniëren met de informatie die gegenereerd wordt, en zodoende netwerken van surveillance beïnvloeden of verstoren. In alledaags gebruik zou een kloner de *readers* in verwarring kunnen brengen. Bovendien is de apparatuur goedkoop en kan het speels en interactief ingezet worden. Het biedt dus ook mogelijkheden voor collectief gebruik. De technologie zal wellicht geen grote sociale bewegingen veroorzaken, maar wie weet schept het ruimte voor nieuwe kritische verbanden waar de technologie deel van uitmaakt.

Een belangrijke les die te trekken is uit de manier waarop kunstenaars omgaan met RFID is dat we ons niet alleen hoeven neer te leggen bij de technologie of haar moeten proberen te ontwijken. In plaats van een keuze tussen voor of tegen de technologie, moeten er verkenningen gedaan worden naar de mogelijkheden van hoe we ons er creatief mee kunnen verhouden. In plaats van een discussie te voeren over een *opt-in* versus *opt-out* beleid, pleiten we ervoor om de nadruk te verleggen, waarbij er meer aandacht komt voor de optie om te interveniëren met de informatie. Een *opt-in/opt-out* beleid neemt immers de winkel of (overheids)instantie als referentiepunt: zij bepalen de inhoud van de tags die aan of uitgezet worden aan de hand van een keuze van de cliënt, zelfs als die ervoor kiest om de tags uit te zetten. Maar die zeggenschap moet niet alleen gaan over 'aan of uit', maar ook over *wat* aan of uit staat en ook *wat er op staat*. Dus: we willen *zeggenschap over onze tags*.

De tendens dat persoonlijke informatie in steeds complexere netwerken opgeslagen en gebruikt wordt, vraagt om nieuwe technieken van 'identiteitsmanagement'. Zo stelt Santucci, Directeur-Generaal Informatie Maatschappij en Media van de Europese Commissie, dat complexe systemen van identiteitsmanagement ontworpen moeten worden om de rechten van 'datasubjecten' te kunnen (blijven) uitoefenen (Santucci, 13). Het Rathenau Instituut adviseert gebruikers te betrekken bij het ontwerpen van RFID-systemen om zodoende meer ruimte te maken voor aanpassingen die de anonimiteit en keuzevrijheid van de gebruiker waarborgen (Rathenau 2007, 15). Wij voegen daaraan toe dat er praktische toegankelijke middelen op de

markt zouden moeten komen die ons de mogelijkheid geven om met onze tags te werken. Momenteel zijn deze er, maar voor een select gezelschap. Tijd voor de *MyTag*?

Met dank aan Marc Boon.

*Mark Ponte (1979) is journalist en historicus en is te bereiken via voetnoot@xs4all.nl*
*Lonneke van der Velden (1981) is afgestudeerd in de wetenschapsdynamica en filosofie en is werkzaam aan de Universiteit van Amsterdam.*

## Noten

(1) Vaak wordt dit direct gekoppeld aan het '11 september paradigma'. Volgens het Rathenau Instituut liggen de wortels van verschillende uitbreidingen echter al in de decennia daarvoor: in de opkomende aandacht voor georganiseerde misdaad in de jaren 80, de IRT-affaire, het wegvallen van de communistische vijand als traditioneel aandachtspunt voor veiligheidsdiensten en Europese beleidsvorming (Rathenau 2007, 35).

(2) Vgl. Foucaults panopticon (1975). Volgens Foucault zijn 'panoptische technieken' vanaf de negentiende eeuw op allerlei plekken in opkomst. Instituties als ziekenhuizen en scholen zijn door hun transparante ordening 'observatoria van gedrag', waarin zieken en pupillen zich als het ware 'richten' naar het spel van toezicht. Voor een interessante discussie over de prominentie van Foucaults idee van het panopticon en de vraag of het theorievorming over de huidige vormen van surveillance en verzet daartegen niet in de weg staat, vgl. Haggerty & Ericson 2000 en Martin et al. 2009.

(3) De genoemde claim over bovengenoemde 'nieuwe' surveillancetechnologieën, namelijk dat zij altijd binnen een netwerk werken, wordt binnen het wetenschapsonderzoek dus ook over 'oude' technologie gemaakt.

(4) Het gebruik van het begrip 'politiek' is binnen het wetenschapsonderzoek niet onomstreden. Vgl. Gerard de Vries, 'What is Political in Sub-politics? : How Aristotle Might Help STS.' *Social studies of science* 2007, vol. 37, no. 5, 781-810

## Literatuur

22C3, 'RFID-Zapper', *Events.ccc.de*, geraadpleegd 20 augustus 2009. https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)

Aanbiedingsbrief van de Staatssecretaris van Economische Zaken van 5 februari 2009 Rapport ECP.NL Auteur: Bart W. Schermer, 'Verkenning mogelijkheden uniform logo-systeem voor RFID toepassingen', 2009.

Boingboingtv. How to hack RFID-enabled Credit Cards for $8, *Youtube*, 9 april 2008, http://www.youtube.com/watch?v=vmajlKJlT3U

Debatty Regine. 'interview with Heidi Kumao', 2008.

http://www.we-make-money-not-art.com/archives/2008/05/-you.php

European Commission. 'Internet of Things - An Action plan for Europe - Information from the Commission.' 10524/09, Brussels, 2 June 2009.

Federaljackdotcom. 'How to disable Pay Pass RFID chip in credit card', *YouTube, 19 augustus 2008, http://www.youtube.com/watch?v=cufZ9l7cibU*

Fernandez, Luis A. & Laura Huey. 'Is Resistance Futile? Thoughts on Resisting Surveillance' in: *Surveillance & Society* 2009 6(3), 198-202.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison* (1991 [1977])London: Penguin Books. [Oorspronkelijk verschenen als *Surveiller et punir: Naissance de la prison*. Editions Galimard 1975]

Goodin, Dan. 'Cloning passport card RFIDs in bulk for under $250', *YouTube*, 30 januari 2009, http://www.youtube.com/watch?v=9isKnDiJNPk

Haggerty, Kevin D. & Richard V. Ericson, 'The surveillant assemblage' in: *British Journal of Sociology* 2000 51, 605-22.

Haggerty, Kevin D. & Richard V. Ericson (2007). *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Hess, David J. 'Technology- and Product-Oriented Movements: Approximating Social Movement Studies and Science and Technology Studies' in: *Science, Technology Human Values* 2005; 30, 515.

Hoekstra, Mark. 'RFID Racket Reader', Geektechnique.org, 25 september 2007. http://geektechnique.org/projectlab/814/rfid-racket-reader

Imfriggincrazy, 'Dont put RFID in microwave', *YouTube*, 11 februari 2008.

Martin, Aaron K., Rosamunde Van Brakel and Daniel Bernhard. 'Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework' in: *Surveillance & Society* 2009 6(3), 213-232.

Marx, Gary T. (2000). 'What's New About the "New Surveillance"? Classifying for Change and Continuity' in: *Surveillance & Society* 2000 1(1), 9-29. www.surveillance-and-society.org

Marx, Gary T. (2003). 'A Tack in the Shoe: Neutralizing and Resisting the New Surveillance' in: *Journal of Social Issues*, Vol. 59, No. 2, 2003, 369—390.

Mediamatic, 'Social RFID Hackers Camp', *Mediametic.net*, geraadpleegd 20 augustus 2009, http://www.mediamatic.net/page/77281/en, vgl. http://www.mediamatic.net/search?q_mm=iktag

Monahan, Torin. 'Counter-surveillance as Political Intervention?' *Social Semiotics* 2006 16:4, 515-534.

Nohl, Karsten en Henryk Plötz. '*Mifare. Little security, despite obscurity*', lezing 30 december 2007, http://video.google.com/videoplay?docid=4252367680974396650&q=mifare+ccc&total=1&start=0&num=10&so=0&type=search&plindex=0

*NRC Next*, 'Titel', 19 augustus 2009.

Phi Data, 'Nederlands Instituut voor beeld en geluid', phidata.nl, geraadpleegd 20 augustus 2009 http://www.phidata.nl/content/Default/BeeldenGeluid.aspx

Rathenau Instituut. *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* Den Haag: Rathenau Instituut, 2007; Studie 49.

*Rathenau Instituut, Special*, april 2007.

RFID Platform Nederland, geraadpleegd 9 september 2009 www.watisrfid.nl

Rip, Arie. "What is this thing called technology?" In: *Technologie en Samenleving*, H.J. Achterhuis, M.W. Smits, J. Geurts en A. Rip, red. Heerlen/Leuven/Apeldoorn: Open Universiteit/Garant 1995, 15-27.

Santucci, Gérald. 'From Internet of Data to Internet of Things. Paper for the International Conference on Future Trends of the Internet.' 28 January 2009.

Winter, Brenno de. 'OV-chipkaart in seconden te kraken', *Webwereld*, 12 april 2008, http://webwereld.nl/nieuws/50690/ov-chipkaart-in-seconden-te-kraken.html

Winter, Brenno de. 'Elektronisch paspoort onveilig door slechte lezers', *Webwereld*, 7 augustus 2008. http://webwereld.nl/nieuws/52186/elektronisch-paspoort-onveilig-door-slechte-lezers.html

Winter, Brenno de. 'Ov-chipkaart definitief gehackt', *Webwereld*, 10 maart 2008. http://webwereld.nl/nieuws/50228/ov-chipkaart-definitief-gehackt.html