RFID und die Zukunft der Privatsphäre

Marc Langheinrich

Inst. für Pervasive Computing, ETH Zürich, 8092 Zürich, Schweiz
langhein@inf.ethz.ch

Kurzfassung. Drahtlose Funketiketten – in der englischen Abkürzung oft auch als *RFID-Tags* bezeichnet – sind zu einer der bekanntesten Technologien der Vision vom Pervasive bzw. Ubiquitous Computing geworden. Ihr Einsatz als Schnittstelle zwischen realer und virtueller Welt und deren Potential zur umfassenden und automatisierten Überwachung vielfältiger Prozesse nährt die Angst vor einer allgegenwärtigen Überwachung des Einzelnen durch Staat und Wirtschaft, sowie vor dem Missbrauch durch Kriminelle. Sind solche Ängste eher unbegründet, da zwischen Vision und Realität immer noch technische, soziale und rechtliche Machbarkeiten Grenzen ziehen? Oder sind RFID-Tags Vorreiter einer Entwicklung, bei der wir uns mehr oder weniger zwingend hin in Richtung einer Gesellschaft bewegen, in der es ganz normal sein wird, dass praktisch all unsere Handlungen und Bewegungen aufgezeichnet und in digitalisierter Form für andere abrufbar sein werden? Dieser Beitrag[1] versucht, die Gefahren und Herausforderungen einer solchen Entwicklung anzusprechen, die sich sowohl in technischer, vor allem aber auch in gesellschaftlicher Hinsicht beim Einsatz von drahtlosen Funketiketten auftreten, sowie deren Potenzial anhand heutiger gesellschaftlicher Trends und Begehrlichkeiten zu beurteilen.

[1] Dieser Beitrag beruht in Teilen auf früheren Veröffentlichungen des Autors, u.a.: *Die Privatsphäre im Ubiquitous Computing –Datenschutzaspekte der RFID-Technologie*, in: E. Fleisch, F. Mattern (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, Springer-Verlag, 2005; *RFID and Privacy*, in: M. Petkovic, W. Jonker (Hrsg.): Security, Privacy, and Trust in Modern Data Management, Springer-Verlag, 2006; sowie: *Gibt es in einer total informatisierten Welt noch eine Privatsphäre?* in: F. Mattern (Hrsg.): Die Informatisierung des Alltags – Leben in smarten Umgebungen, Springer-Verlag, 2006.

1 Einleitung

RFID-Tags oder Smart Labels haben wohl wie keine andere Technologie des Ubiquitous Computing Ängste in der Bevölkerung mobilisiert, in naher Zukunft in einem Überwachungsstaat zu leben. Als Anfang 2003 der Modehersteller Benetton ankündigte, zwecks Lieferkettenoptimierung den Einsatz von RFID-Chips in Textilien seiner „Sisley"-Marke zu erwägen, brach ein unerwartet heftiger Sturm der medialen Entrüstung aus [Com03]. Nur wenige Wochen später sah sich Benetton genötigt, in einer Pressemitteilung seine Pläne zurückzuziehen [Ben03, EET03]. Ähnliche Beschwichtigungen waren Ende Oktober desselben Jahres sowohl vom Einzelhandelsgiganten Wal-Mart [CST03] als auch vom größten Rasierklingenhersteller der Welt, Gillette, zu hören [CNN03]. In allen drei Fällen hatte eine bis dato eher unbekannte Konsumentenschutzgruppe namens CASPIAN (Consumers Against Supermarket Privacy Invasions And Numbering – frei übersetzt etwa: Konsumenten gegen Datenschutzvergehen und Nummerierung in Supermärkten) im Internet zu einem weltweiten Boykott der global agierenden Konzerne aufgerufen. Gemeinsam mit deutschen Datenschützern vom Bielefelder FoeBuD (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.) schafften CASPIAN-Aktivisten es auch, dass die Eröffnung eines mit RFID-Technik ausgestatteten Vorzeigemarkt der Metro-Gruppe – der „Extra Future-Store" in Rheinberg bei Duisburg – zum PR-Debakel geriet.[2]

Dass die mit einfachsten Mitteln agierende Protestbewegung eine solch nachhaltige Wirkung hervorruft, lässt auf den Stellenwert schließen, den das Thema Datenschutz und Privatsphäre in der Öffentlichkeit erlangt hat. Inzwischen gibt es kaum noch Presseartikel oder Fernsehsendungen, welche über Ubiquitous Computing berichten, ohne nachdrücklich auf die möglicherweise weit reichenden Konsequenzen bis hin zum Überwachungsstaat hinzuweisen, in dem „Schnüffelchips [...] in Joghurtbechern, Kreditkarten oder Schuhen [...] Ihr Leben durchsichtig wie Glas" machen [Zei04]. Gleichzeitig setzt sich aber auch der Siegeszug der Kundenkarte ungebrochen fort, durch deren Nutzung Supermarktketten einen noch nie da gewesenen Einblick in das individuelle Kaufverhalten ihrer Kunden erhalten. Nach einer Emnid-Studie hatten bereits im März 2002 mehr als die Hälfte aller Deutschen mindestens eine Kundenkarte, in Großbritannien

[2] Der Handelsriesen wurde prompt mit dem „Big Brother Award 2003" ausgezeichnet. Die Big Brother Awards werden seit 1998 in verschiedenen Ländern – seit 2000 auch in Deutschland – alljährlich an Personen und Firmen verliehen, die „in besonderer Weise und nachhaltig die Privatsphäre von Menschen beeinträchtigen…" Siehe auch www.bigbrotherawards.de

waren es 2003 sogar mehr als 86 % [Sha03]. Auf eine große Anfrage der FDP im deutschen Bundestag im Februar 2005 hin schätzte die Bundesregierung über 70 Millionen ausgegebene Rabatt- und Kundenkarten [Bun05]. Für einen Preisnachlass von oft weniger als einem Prozent des Warenwertes ist ein Großteil der Verbraucher also offenbar bereit, das Kaufverhalten offen zu legen und zum Zwecke der Marktforschung und zur individuellen Angebotsunterbreitung analysieren zu lassen.
Dieser Widerspruch zwischen Besorgnis um den Verlust der Privatsphäre durch RFID-Tags einerseits und der freiwilligen Preisgabe detaillierter Informationen im Austausch für kleinste Rabatte andererseits ist allerdings weder neu noch überraschend. Sicherheit und Datenschutz waren schon immer Ausdruck des Abwägens, bei denen Bequemlichkeit und finanzielle Vorteile mit den möglichen ideellen und physischen Schäden nicht immer rational aufgerechnet wurden. Doch ist es müßig, den Konsumenten belehren zu wollen und ihn auf diesen offensichtlichen Widerspruch hinzuweisen. Vielmehr gilt es, irrationale Ängste von begründeten Vorbehalten zu unterscheiden und tatsächlich mögliche Bedrohungen für unser soziales Gefüge zu identifizieren, um bereits im Vorfeld der technischen Entwicklung potenzielle Fehlentwicklungen zu erkennen.

Der vorliegende Beitrag möchte zum einen am Beispiel der RFID-Technik und dessen aktuell diskutierten technischen Datenschutzlösungen die Möglichkeiten, aber auch die Grenzen solcher Ansätze aufzeigen. Zum anderen soll abgeschätzt werden, ausgehend von heutigen Entwicklungen und Trends, inwieweit sich RFID und andere Technologien des Ubiquitous Computings in unserem Alltag etablieren und dadurch unsere (gefühlte und tatsächliche) Privatsphäre beeinflussen werden. Auch wenn abschließende Aussagen über die Zukunft oft schwierig, wenn nicht gar unmöglich erscheinen, kann eine solche Betrachtung womöglich das Bewusstsein für die Problematik schärfen und Handlungszwänge aufzeigen, die in Folge einer informatisierten Gesellschaft [Mat03] auf uns zu kommen.

2 Die Vorteile drahtloser Funketiketten

Drahtlose Funketiketten – RFID-Tags – sind prinzipiell eine Identifikationstechnik ähnlich dem altbekannten Barcode. Gegenüber dem optischen Auslesen eines Barcodes bietet die Verwendung von RFID-Tags jedoch eine Reihe signifikanter Vorteile:

1. *Automatisierung*: Während Barcodes eine Sichtverbindung zum Lesegerät benötigen, die entweder manuell hergestellt bzw. auf Fliessbändern aufwändig durch mehrere Aufdrucke und/oder verschieden

orientierte Lesegeräte sichergestellt werden muss, können Funketiketten prinzipiell ohne besondere Ausrichtung, d.h. auch „um die Ecke“ bzw. „von hinten“ gelesen werden.[3]

2. *Identifizierung:* Funketiketten ermöglichen es, mehr Informationen auf kleinerem Raum unterzubringen und können dadurch nicht nur eine Produkt*klasse* identifizieren („Dies ist eine Packung Margarine“), sondern auch individuelle Seriennummern („Dies ist Margarinen-Packung #94810394“), die beispielsweise durch Verknüpfung mit einer Herstellerdatenbank weitere Detailinformationen verfügbar machen kann (z.B. „produziert am 11.6.2006 in Werk 4“).
3. *Integration:* Infolge der drahtlosen Kommunikation zwischen Lesegerät und Funketikett können Hersteller RFID-Tags beinahe beliebig in ein Produkt integrieren, wodurch nicht nur die Robustheit des Etiketts verbessert werden kann (z.B. Schutz vor Schmutz oder Abnutzung), sondern auch das Produktdesign unabhängiger gestaltet werden kann.

Mit der Hilfe von RFID-Tags können also, zumindest prinzipiell, Produkte und Gegenstände weitaus verlässlicher, einfacher und genauer identifiziert werden als mit traditionellen Barcodes.

Darüber hinaus bietet RFID jedoch noch einen weiteren, entscheidenden Vorteil gegenüber Barcodes: ausgestattet mit entsprechender kryptografischen Fähigkeiten kann ein *Kopieren* eines Funketiketts praktisch ausgeschlossen werden. Während ein Barcode konstruktionsbedingt alle in ihm „enthaltene“ Information für jegliche Lesegeräte gleichermaßen zur Verfügung stellt, können im drahtlosen Kommunikationsprotokoll zwischen RFID-Tag und Leser aufwändige Authentisierungsmechanismen integriert werden, die nicht nur unautorisierten Lesegeräten das Auslesen verbietet, sondern ebenfalls sicherstellen, dass ein auf dem Funketikett gespeichertes Geheimnis nicht direkt auslesbar ist, dessen Vorhandensein jedoch vom auslesenden Lesegerät zweifelsfrei überprüfbar ist. Ein populäres Beispiel für einen solchen Einsatz ist die in fast allen modernen Fahrzeugen integrierte Wegfahrsperre: ein im Autoschlüssel integrierter Funkchip wird beim Betätigen der Zündung von einem integrierten Lesegerät ausgelesen und identifiziert im Rahmen eines Authentisierungsprotokolls den Schlüssel als ein Original. Ein weiterer Grund für die Verwendung von drahtlosen Funketiketten ist also ihr Einsatz zur *verlässlichen* Identifizierung:

4. *Authentisierung*: RFID-Tags können eine weitaus verlässlichere Identifikation als Barcodes ermöglichen, da sie – mit kryptografischen

[3] In der Praxis gestaltet sich dies natürlich weitaus schwieriger, siehe Abschnitt 5 in diesem Kapitel.

Protokollen ausgestattet – ein unerlaubtes Duplizieren eines Etiketts praktisch ausschließen.

Diesem Umstand verdanken RFID-Tags ihre abseits aller Proteste bereits weit fortgeschrittene Verbreitung in Eintrittskarten (z.B. als drahtloser Skipass in vielen Skigebieten, bzw. im Rahmen der WM2006 in Millionen von Eintrittskarten), als drahtloses Zahlungsmittel (z.B. in vielen Betriebskantinen, aber auch im in den USA beliebten *Exxon Speedpass* zum bargeldlosen Tanken) und nicht zuletzt im neuen biometrischen Reisepass.

Gerade die letzten Beispiele zeigen bereits, dass RFID-Tags eine recht große Bandbreite an Anwendungsgebieten abdecken – vom fälschungssicheren Reisepass bis hin zu Coladosen und Rasierklingen – und dass die technischen Anforderungen an die jeweils eingesetzten Tags sehr unterschiedlich ausfallen können. Der folgende Abschnitt soll deshalb zunächst einen kurzen technischen Überblick liefern, um die unterschiedlichen Systeme und ihre verschiedenen Eigenschaften bezüglich ihres Risikos für unsere Privatsphäre besser beurteilen zu können.

3 Ein kurzer Techniküberblick

RFID-Systeme bestehen aus RFID-Tags und mindestens einem RFID-Lesegerät. Die RFID-Tags werden an die zu identifizierenden Gegenstände angebracht und können, sobald sie in die Nähe des Lesegerätes gelangen, von diesem drahtlos ausgelesen und – in Abhängigkeit von den eingesetzten RFID-Tags – möglicherweise auch beschrieben werden. RFID-Tags bestehen aus einem so genannten Kopplungselement, welches für die Kommunikation mit dem Lesegerät benötigt wird (und in vielen Fällen auch zur Energieversorgung des Tags) und einem Mikrochip, welcher beispielsweise die ID des Funketiketts speichert. Das Lesegerät stellt die (drahtlose) Schnittstelle zu den RFID-Tags dar und verfügt typischerweise über einen separaten Mikroprozessor mit internem Speicher, um einem PC oder einem ähnlichem Gerät die Verwendung einfacher Befehle (z.B. „Schreibe den Wert 1234 in Tag Nummer 15“) zu ermöglichen.

Während praktische alle RFID-Systeme aus diesen beiden Komponenten bestehen – einem Lesegerät und einer Anzahl drahtlos auslesbaren Mikrochips – so unterscheiden sich existierende Systeme je nach anwendungsabhängigen Anforderungen im Detail teilweise erheblich. Wichtigste Unterscheidungsmerkmale sind dabei die Art der Energieversorgung (aktiv, semi-aktiv oder passiv), die Funkfrequenz (im LF-, HF-, UHF- oder MW-Band liegend), die Kopplungsart (induktiv oder elektromagnetisch) und das eingesetzte Kommunikationsprotokoll.

Passive RFID-Tags verfügen über keine eigene Energiequelle, sondern werden vom Lesegerät während des Auslesens gleichzeitig auch mit Energie versorgt. Aktive Tags besitzen hingegen eine eingebaute Batterie, die sowohl die Reichweite als auch die Verlässlichkeit der Kommunikation erheblich erhöht.[4] Aktive Funketiketten sind typischerweise weitaus teurer (mehrere Euros statt wenige Cents) und klobiger als die teilweise staubkorngroßen passiven RFID-Tags und finden deshalb selten den Weg zum Endkunden – eher findet man sie beispielsweise an wieder verwendbaren Behältern in der Logistik. Mit RFID-Tags versehene Massenware – Kaugummipäckchen, Getränkedosen oder Banknoten – wird praktisch ausschließlich mit der passiven Variante ausgestattet werden.

Die verwendete Frequenz eines RFID-Systems beeinflusst nachhaltig dessen Reichweite und ist eng verwandt mit der eingesetzten Kopplungsart. LF- (*low frequency*, zwischen 100-135 kHz) und HF-Systeme (*high frequency*, um 13.56 MHz) verwenden den Effekt der magnetischen Induktion zur Kommunikation zwischen Leser und RFID-Tag.[5] Hierbei befinden sich sowohl am Lesegerät wie auch auf den Funketiketten Spulen, welche bei Stromdurchfluss ein Magnetfeld erzeugen, ähnlich einem Elektromagneten (aber weitaus schwächer). Befindet sich ein Funketikett nun im magnetischen Feld eines Lesegerätes (dem so genannten *near field*), so erzeugen Veränderungen im Magnetfeld des Lesers Spannungsänderungen an der Spule des RFID-Tags (um umgekehrt), welche dort gemessen und in Informationen bzw. Befehle übersetzt werden. Dieser Effekt tritt jedoch nur im relativ klar abgegrenzten *near field* auf und setzt dadurch der möglichen Reichweite solcher Systeme klare Grenzen (bei HF-Systemen liegt diese theoretisch mögliche Reichweite beispielsweise bei 3.5m, praktikabel sind bei diesem Verfahren sogar lediglich Reichweiten bis 1.5m).

UHF- (*ultra high frequency*, um 850-900 MHz) und MW-Systeme (*microwave*, bei 2.45 bzw. 5.8 GHz) verwenden statt Spulen und magnetischer Induktion Dipolantennen, welche ein elektromagnetisches Feld (das so genannte *far field*) zur Kommunikation bzw. Energieübertragung erzeugen. Antennen auf den RFID-Tags empfangen die Radiowellen des Lesegeräts, ähnlich den batterielosen Radios Anfang des 20. Jahrhunderts (so genannten Detektorempfängern), und können auf diesen Wellen eigene Signale zum Leser „zurückstreuen“ (*backscatter*). Elektromagnetische Systeme ermöglichen höhere Reichweiten als induktive Systeme – typi-

[4] Semi-aktive Tags besitzen ebenfalls eine Batterie, verwenden diese allerdings nur zum Betrieb des Mikrochips, nicht aber zum Senden der Daten. Dadurch können weitaus kleinere Batterien verwendet werden.

[5] Dieses Verfahren wird praktisch ausschliesslich bei passiven RFID-Systemen eingesetzt [Fin02]

scherweise fünf bis sieben Meter – und können womöglich in Zukunft durch verbesserte Empfänger bis zu einigen Dutzend Metern erreichen.

Die verwendete Kopplungstechnologie bestimmt nicht nur die Funkfrequenz, sondern oft auch das verwendete Kommunikationsprotokoll zwischen Lesegerät und Tags. Insbesondere sind hier die Protokolle zur *Singularisierung* einzelner RFID-Tags von Interesse, die so genannten *Anti-Kollisions*-Protokolle. Diese sind nötig, da einzelne Funketiketten nicht in der Lage sind, etwaige in der Nähe befindliche RFID-Tags zu bemerken und sich deshalb die mehr oder weniger zeitgleichen Antworten mehrer RFID-Tags überlappen und dadurch gegenseitig stören würden. Ein Anti-Kollisions-Protokoll gibt deshalb Lesegeräten die Möglichkeit, solche Störungen nicht nur zu erkennen, sondern auch im Falle einer Signalüberlappung die fraglichen RFID-Tags durch wiederholtes „Befragen“ nach und nach zu identifizieren.

UHF- und MW-Systeme verwenden typischerweise baum-basierte, *deterministische* Protokolle, in denen das Lesegerät den Raum aller möglichen (binären) ID-Präfixe schrittweise abfragt, z.B. „Alle Tags deren ID mit *0* beginnt, bitte antworten!“ Sobald zwei oder mehr RFID-Tags dasselbe Präfix besitzen, kommt es in solch einem Fall zu einer Kollision. Das Lesegerät verlängert daraufhin das abgefragte Präfix um eine *0* bzw. eine *1*, um so die im Konflikt stehenden Tags zu trennen. Dies wird wiederholt, bis jeweils nur noch ein einzelnes Funketikett antwortet. Während dieser Ansatz relativ aufwändig ist und für die effiziente Durchführung relativ hohe Durchsatzraten benötigt, liegt der große Vorteil in dessen deterministischem Verhalten: er garantiert das Auslesen aller Tags in endlicher Zeit.

Die typischerweise langsameren LF- und HF-Systeme verwenden stattdessen *nicht-deterministische* Verfahren, die auf dem auch für Ethernet genutzten „Slotted ALOHA“-Protokoll beruhen. Hierbei warten die Funketiketten nach einer Leseanfrage jeweils eine gewisse, zufällig gewählte Zeit, bevor sie antworten. Erkannte RFID-Tags, d.h. Tags deren Daten störungsfrei übertragen wurde, können dann vom Lesegerät explizit „stumm“ geschaltet werden, bevor dieses eine weitere Runde beginnt, um die verbleibenden Tags störungsfrei auslesen zu können. Während dieses Verfahren besonders für kleine Tag-Populationen effizienter ist als die oben beschriebenen, baum-basierten Ansätze, so kann es bei vielen Tags zu größeren Verzögerungen kommen.

4 Datenschutzimplikationen

So vorteilhaft der Einsatz von RFID-Tags gegenüber dem konventionellen Barcode sein kann – erhöhter Automatisierungsgrad, genauere Identifikation, unauffällige Integration und sicher Authentisierung – so unvorteilhaft sind diese Aspekte, wenn es um den Schutz der Privatsphäre geht:

1. *Automatisierung*: Mitgeführte Funketiketten lassen sich ohne die Zuhilfenahme der jeweiligen Trägerperson auslesen, in vielen Fällen sogar ohne manuelle Justierung des Lesegerätes. Dies senkt die Kosten und erleichtert so das Durchführen von Datensammlungen erheblich.
2. *Identifizierung*: Eine verbesserte Identifizierung einzelner Gegenstände erhöht gleichfalls die Möglichkeiten zur eindeutigen Identifikation der diesen Gegenstand mitführenden Person. Dies ermöglicht weitaus genauere Kunde- bzw. Bürgerprofile.
3. *Integration*: Die drahtlose Kommunikation erlaubt nicht nur das unbemerkte Auslesen sondern auch das unbemerkte *Anbringen* eines Funketiketts an (bzw. in) einen Gegenstand. So könnte die Tatsache, dass ein Auslesen eines Gegenstandes überhaupt möglich ist, leicht vor dessen Besitzer verborgen bleiben.
4. *Authentisierung*: Die obigen Punkte sind besonders kritisch beim Einsatz solcher Funketiketten in Gesundheits-, Sicherheits- und Zahlungssystemen, bei denen personenbezogene Daten eng mit einem RFID-Tag verknüpft bzw. direkt darauf gespeichert sind.

Diese vier Aspekte drahtloser Funketiketten bedrohen zwei Arten der individuelle Privatsphäre: die *informationelle* Privatsphäre (*data privacy*) und die *ortsbasierte* Privatsphäre (*location privacy*).

Sobald ein von einer Person mitgeführter, mit Funketiketten ausgestatteter Gegenstand von einem Lesegerät identifiziert wird, kann auf den momentanen Aufenthaltsort dieser Person geschlossen werden. Dies funktioniert nicht nur mit eindeutigen IDs: auch wenn lediglich Produkt*gruppen*, z.B. ein bestimmtes Jeansmodell bzw. ein bestimmte Schuhmarke, identifiziert werden, so können durch die spezifische Kombination dieser Gegenstände, so genannten *constellations*, weiterhin individuelle Personen identifiziert werden [Wei03]. Durch das Wissen um die Aufenthaltsorte persönlicher Gegenstände, z.B. dass der Wagen einer Person um eine bestimmte Zeit eine automatische Mautstation passiert hat, können andere leicht auf die Bewegungen ihrer Besitzer – und damit in den meisten Fällen auch auf deren Tätigkeiten – mit hoher Wahrscheinlichkeit schließen.

Sobald die IDs drahtloser Funketiketten nicht nur zufällige Zahlenreihen darstellen, sondern Daten (z.B. eine Kundennummer oder eine Herstellerangabe wie beim *Elektronischen Produkt Code (EPC)* [EPC04]), bzw. so-

bald sie über eine Datenbank mit Daten verknüpft werden können, wird über die Ortung hinaus auch die *informationelle* Privatsphäre der Person bedroht. Gleichermaßen kritisch ist die Speicherung von personenbezogenen Daten direkt auf dem RFID-Tag, z.B. Ort und Datum des Kaufs eines Produkts. Diese Informationen können auch durch das Abhören legitimer Auslesevorgänge bzw. durch das Vortäuschen legitimer Lesevorgänge von unberechtigten Dritten in Erfahrung gebracht werden. Einen besonderen Fall stellt das Auslesen von Produkt-IDs dar, deren Mitführen nicht öffentlich bekannt ist. Hierunter fallen die oft zitierten Beispiele vom Auslesen der Unterwäschenmarke einer Person, der Inhalt von Einkaufstaschen und das Ausspionieren von Einrichtungsgegenständen in einer Wohnung. In vielen Fällen kommt es dabei gar nicht darauf an, die Identität einer Person in Erfahrung zu bringen – es reicht zu wissen, dass *diese* Person einen Schwangerschaftstest in der Apotheke gekauft hat oder dass in *diesem* Haus modernste Unterhaltungselektronik steht.

Wie könnten solcherlei Angriffe auf die Privatsphäre aussehen? Der Kolumnist Andrew Kantor vom US-Massenblatt USA Today schreibt: „*A department store's RFID system recognizes that you're carrying an item you bought there last week. Now it knows who you are. And if there are readers scattered about, it knows where you're going. Come home to a phone call, 'Mr. Kantor – we noticed you were shopping for a television…'*" [Kan03]. Gerade solche Einzelhandels-Szenarien sind wohl die meist zitierten Bedrohungen einer Zukunft mit RFID. Erfahrene Marketingexperten bezweifeln, ob mit solch plumpen Methoden wie von Herrn Kantor befürchtet je eine verkaufsförderliche Atmosphäre geschaffen werden könnte. Ebenso fraglich bleibt, ob skrupellose Supermarktbesitzer in Zukunft nicht nur ihre eigenen Funketiketten auslesen, sondern auch die der Video- bzw. Bibliothek, Bundesdruckerei (Ausweis, Bargeld) oder Krankenkasse (Gesundheitskarte), nur um bessere Kundenprofile erstellen zu können. Zum einen werden die einzelnen Systeme schon rein technisch kaum kompatibel sein[6], zum anderen gelten auch für Einzelhändler in den meisten Jurisdiktionen klare Datenschutzgesetze, die beispielsweise im europäischen Raum ein solches Vorgehen klar verbieten[7].

Doch auch ohne flächendeckende Integration solcher Systeme könnte eine solche Entwicklung in Einzelfällen erhebliche Nachteile mit sich

[6] So verwenden praktisch alle heutigen Bibliothekssysteme HF-Funketiketten (13.56 MHz), während Einzelhändlern aufgrund der höheren Leseraten RFID-Chips im UHF-Bereich einsetzen (um 900MHz).

[7] Dazu kommt, dass sich das systematische unerlaubte Auslesen von Funketiketten aufgrund der nötigen Sendeleistung von RFID-Lesegeräten nur schwer vor Konsumentenschützern oder Regulierungsbehörden verstecken liesse [Lan06].

bringen. Ein gutes Beispiel für die negativen Folgen detaillierter Datensammlungen, auch bei relativ begrenzten Bereichen, geben die populären Kundenkarten. Als der 59-jährige Robert Rivera 1998 in einem Vons-Supermarkt in Los Angeles auf einer Jogurtlache ausrutschte und sich an der Kniescheibe verletzte, wollte er den Supermarktbetreiber verklagen. Doch der zog angeblich die Einkaufsgeschichte von Rivera zu Rate, die er durch die Nutzung seiner Vons-Kundenkarte angesammelt hatte, und machte Rivera's Anwalt klar, dass die überdurchschnittlichen Alkoholeinkäufe ihres geschätzten Kundens in einem etwaigen Prozess durchaus dazu verwendet werden könnten, Rivera als debilen Alkoholiker erscheinen zu lassen, der schlicht und einfach aus Trunkenheit stürzte [Vog98]. Ein ähnlicher Fall ereignete sich 2004 in Kanton Bern in der Schweiz: Am Tatort einer Brandstiftung in Niederwangen findet die Polizei ein Werkzeug[8] aus dem Sortiment der Einzelhandelskette Migros. Nach anfänglicher Weigerung verurteilt schließlich das Obergericht des Kantons Bern die Migros-Geschäftsleitung zur Herausgabe einer Liste aller Kunden, die dieses Werkzeug unter Vorzeigen ihrer Kundenkarte gekauft hatten.

Doch nicht nur zur Verbrechensbekämpfung, auch zur Durchführung von Verbrechen können drahtlose Funketiketten dienen: „*Sophisticated thieves walk by homes with RFID readers to get an idea of what's inside. Slightly less sophisticated thieves do the same thing in a parking lot, scanning car trunks*" [Kan03]. Es bleibt offen, ob mehr oder weniger professionelle Diebe nicht bereits aufgrund der Lage eines Hauses, bzw. dem äußeren Erscheinungsbild einer Person oder ihres Autos entscheiden könnten, wo sich ein Verbrechen lohnt. Düstere Visionen sehen dabei schon mehr als nur einfachen Diebstahl auf uns zu kommen: „*In the future, there will be this very tiny microchip embedded in the envelope or stamp. You won't be able to shred it because it's so small… Someone will come along and read my garbage and know every piece of mail I received*" [Rob03]. Interessanterweise wirbt bereits heute die U.S.-amerikanische Firma Stamps.com, die Software für den Ausdruck von Postwertzeichen am eigenen PC vertreibt, mit solch einem Szenario: „*PC Postage also helps contribute to mail security by reducing the volume of anonymous mail in the mail stream*" [Ray02].

Überwachungsszenarien dieser Art werden schnell auf nationale und internationale Ebene ausgeweitet: „*A seamless network of millions of RFID receivers strategically placed around the globe in airports, seaports, highways, distribution centers, warehouses, retail stores, and consumer's homes, all of which are constantly reading, processing, and evaluating*

[8] Aus fahndungstechnischen Gründen bleibt unklar, welches Werkzeug (z.B. Hammer oder Schraubenzieher) gefunden wurde.

consumer behaviors and purchases“ [EPI01]. Gerade im Zusammenhang mit biometrischen Reisedokumenten scheint das Potenzial von RFID grenzenlos: „W*ürde es Sie stören, wenn in Ihrem Pass ein Funkchip versteckt wäre – darin alle möglichen privaten Daten gespeichert? Behörden oder Unternehmen könnten herausschnüffeln, wo Sie gerade sind, welche Automarke Sie gerade fahren, welche Krankheit Sie plagt und ob Sie Arbeitslosengeld beziehen*“ [Zei03].

Datenschützer sehen in dieser zunehmenden Digitalisierung unseres Lebens eine schleichende Umkehr der Unschuldsvermutung auf uns zukommen. So mahnt Helmut Bäumler, der ehemalige Landesdatenschutzbeauftragter Schleswig-Holsteins, im Zusammenhang mit der Verwendung von RFID-Tags in Geldscheinen: „*Stellen Sie sich mal vor, man findet plötzlich in Ihrer Brieftasche oder in der Brieftasche von jemand anders einen Geldschein, der zuvor von Ihnen dort hingegeben worden ist, und die Polizei hat den Verdacht, der könnte aus einer Straftat stammen. Da hätten sie eine Menge zu tun, um zu belegen, dass sie nicht der Hehler sind, und dass sie nichts mit dieser Straftat zu tun haben*“ [Zei03]. Ebenso warnen Kritiker vor einer zunehmenden Technikgläubigkeit bei sicherheitsrelevanten Anwendungen, wie beispielsweise RFID-basierten Reisepässen: „*Note also that the mere presence of the reader, the chip and the general ePassport security pixie dust will… have a psychological effect on border control staff. They will tend, because the machine says the passport's clean, to drop their guard, not really inspect either picture or bearer properly. This kind of effect is well documented, and it's the same kind of thing as people walking in and out of companies unchallenged despite wearing a security tag in the name of 'Michael Mouse'*“ [Let06].

Berthold et al. [BGS05] identifizierten in Interviews mit über dreissig Teilnehmern neben den drei oben genannten Ängsten – Profilbildung, krimineller Missbrauch und Verfolgung („Tracking“) – zwei weitere Bedrohungsszenarien drahtloser Funketiketten: *Objektverantwortlichkeit* und *Technologiepaternalismus*. So könnte mit Funketiketten versehener Abfall leichter zum Käufer zurückverfolgt werden, um so Müllsünder, z.B. in öffentlichen Parks, zur Rechenschaft zu ziehen. Ebenso war unklar, in welchem Ausmass mit RFID gekennzeichnete Gegenstände von smarten Umgebungen dazu verwendet werden könnten, gesellschaftlich erstrebenswertes Handeln zu erzwingen, wie beispielsweise Mülleimer, die keine Glasflaschen mehr akzeptieren oder Versicherungsprämien, die in Abhängigkeit vom Kühlschrankinhalt (z.B. Eiscreme oder Gemüse) steigen oder fallen.

5 Technische Schutzmassnahmen

Konkret führen die im vorigen Kapitel genannten Bedrohungen zu den folgenden Schutzzielen: Schutz vor verdecktem Auslesen, Schutz vor unerlaubtem Abhören und dem Schutz vor Datenlecks:

1. *Verdecktes Auslesen*: Die Daten des RFID-Tags werden ohne das Wissen des Trägers ausgelesen. Dabei kann die informationelle Privatsphäre direkt (wenn z.B. eine Kundennummer auf dem Tag gespeichert ist) oder indirekt (durch das Offenlegen nichtöffentlich bekannter Besitztümer, z.B. der Inhalt einer Einkaufstüte) gefährdet werden. Durch das Verfolgen individueller, einer Person zugeordneter IDs wird die ortsbasierte Privatsphäre bedroht.
2. *Abhören*: Statt aktiv Funketiketten auszulesen, können Angreifer auch die Kommunikation mit legitimen Lesegeräten abhören, meist aus größerer Entfernung als beim aktiven Auslesen. Selbst wenn die Daten auf dem Tag bzw. bei der Übertragung verschlüsselt werden, so können untere Protokollschichten wie beispielsweise das Anti-Kollisionsprotokoll das Vorhandensein bestimmter RFID-Tags einem Angreifer offen legen.
3. *Datenlecks*: Unabhängig von der verwendeten RFID-Technologie besteht bei vielen RFID-basierten Anwendungen die Gefahr, dass mehr Daten als nötig ausgelesen, auf dem Tag gespeichert bzw. mit ihm verlinkt werden. Dieses generelle Problem automatischer Datenverarbeitung wird durch den potentiell flächendeckenden Einsatz von Funketiketten signifikant verschärft. Gerade auch die kommerziellen RFID-Systemen zugrunde liegende Informationsinfrastruktur ist in seiner aktuellen Ausprägung anfällig für Einbruchsversuche und Datenlecks [FGS05].

Zunächst bleibt festzustellen, dass bei allem Potenzial der RFID-Funktechnik diese auf physikalischen Grundsätzen magnetischer Felder bzw. elektromagnetischer Wellen beruht und daher nicht beliebige Funktionalität aufweisen kann. So stellt beispielsweise die Größe des magnetischen Feldes um ein RFID-Lesegerät, das so genannte *near field*, eine recht konkrete Grenze dar, jenseits derer ein Auslesen induktiv gekoppelter Funketiketten praktisch unmöglich ist [Fin02] – bei den populären HF-Tags sind dies z.B. maximal dreieinhalb Meter. Ebenso bedingt die Bauweise der eingesetzten Tags, z.B. deren Antennengröße, ihre maximale Reichweite. Hitachis Submillimeter große µ-chips[9] können ohne externe Antenne praktisch nur aus wenigen Millimeter Entfernung gelesen werden, mit einer externen, fünf Zentimeter großen Stabantenne sind es knapp 30

[9] www.hitachi.co.jp/Prod/mu-chip/

Zentimeter. Viel versprechender ist in solchen Situationen statt des verdeckten Auslesens das Abhören, da Lesegeräte infolge der für die RFID-Tags nötigen Energiezufuhr mit einem Vielfachen der benötigten Sendeleistung funken.

Weiterhin ist die Verlässlichkeit des Auslesens lediglich in sorgfältig vorbereiteten Situationen, d.h. im industriellen Logistikkreislauf bzw. in einer abgeschotteten Laborumgebung, ausreichend hoch, da die überaus schwachen Signale eines Funketiketts leicht durch metallische Leiter und Flüssigkeiten[10] verzerrt bzw. überdeckt werden können. Ein verdecktes Auslesen ohne die Hilfe spezieller Schleusen oder einer großen Anzahl redundanter Antennen wird sicherlich viele Zufallstreffer landen, jedoch kaum in der Lage sein, zum Zwecke einer lückenlosen Kontrolle verlässlich alle passierenden Funketiketten auszulesen. So scheint beispielsweise IBMs Vision eines Supermarktes ohne Kassenschlangen[11] in naher Zukunft kaum machbar: zu unzuverlässig lassen sich RFID-Etiketten aus einer Einkaufstasche heraus lesen, zu einfach ist ein „zufälliges" Abschirmen von Tags durch Alufolie möglich, als dass ein verlustfreies automatisches Abrechnen möglich wäre.

Natürlich steht diesen physikalischen Grenzen die stetige Weiterentwicklung der Technik gegenüber, die leicht zu einer großzügigen Extrapolation heutiger Lesedistanzen von Zentimeter in Meter (und darüber hinaus) führen kann. Niemand kann heutzutage mit Sicherheit voraussagen, ob es nicht doch einmal möglich sein wird, mit Hilfe hoch sensitiver Schaltkreise selbst die schwächsten Signale kurzreichweitiger RFID-Tags aus großer Entfernung unbemerkt auszulesen. Dennoch darf ob allem Technikfortschritt weder die soziale noch die wirtschaftliche Machbarkeit außer Acht gelassen werden, sonst wären die populären Visionen der 1950er und 1960er – atomgetriebene Autos und Unterwasserstädte – heute schon längst Realität. Hierzu mehr im Abschnitt 6 weiter unten.

5.1 Zugriffskontrolle

Unabhängig aller physikalischer Grenzen ist es natürlich trotzdem sinnvoll, RFID-Systeme zu entwickeln, die Datenlecks vermeiden, das Abhören unterbinden und das unbemerkte Auslesen erschweren. Eine Vielzahl an technischen Vorschlägen existiert bereits, auch wenn deren praktische

[10] Menschen bestehen aus über 50% Wasser, ebenso wie viele Früchte (z.B. Tomaten) und natürlich Getränkeflaschen und –dosen (welche auch noch in einem metallischen Leiter – der Dose – stecken).

[11] Siehe beispielsweise www.youtube.com/watch?v=WPtn0fM4tuo bzw. die Suche nach „IBM" und „RFID" auf www.youtube.com

Umsetzung bisher kaum über Laborexperimente hinaus kam. Der wohl bekannteste Schutz vor unbemerkten Auslesen ist die „Kill"-Funktion in den Standards von EPCglobal [Aut02, Auto03], der treibenden Kraft hinter der Funketiketten-Standardisierung im Einzelhandel. Die zugrunde liegende Idee ist simpel: Die von Herstellern und Händlern zur Lagerkettenoptimierung eingesetzten RFID-Tags werden beim Verkauf an den Endkunden entweder physisch entfernt oder aber, wenn ein Entfernen nicht möglich ist, dauerhaft deaktiviert. Dadurch wird ein Auslesen des Tags außerhalb des Ladens unmöglich gemacht und damit die Gefahren der unbemerkten Identifikation, der Lokalisation und Verfolgung sowie der unerlaubten Profilbildung verhindert.

Der aktuelle EPCglobal-Standard [EPC04] schreibt dazu zwecks Deaktivierung für alle konformen Tags einen Kill-Befehl vor, der jedoch zur Ausführung ein während oder kurz nach der Produktion auf dem Tag gespeichertes 24-Bit-Passwort erfordert, um unautorisiertes „Einschläfern" eines Tags (z.B. im Regal) zu erschweren.[12] Erhält ein Tag das korrekte Passwort zusammen mit dem Kill-Befehl, darf es danach laut Spezifikation in keiner Weise mehr auf Signale eines Lesers reagieren [Aut03]. Auch wenn potenzielle Kunden in ersten Umfragen dieses Verfahren positiv beurteilten [GüS05], wirft die praktische Umsetzung eines solchen Ansatzes vielerlei Fragen auf. Das Verwalten individueller Passwörter für Millionen von Produkten – vom Videorekorder bis hin zu Kaugummipackung und den Einkäufen an der Käsetheke – entlang einer ganzen Lieferkette (Zulieferer, Hersteller, Großhändler, Einzelhändler) und über beliebige Verkaufsorte hinweg (Großmarkt, Supermarkt, Detailhändler, Kiosks und Würstchengrills) erscheint utopisch. Nicht zuletzt geht durch ein permanentes Deaktivieren der RFID-Tags natürlich auch eine Vielzahl von sekundären Nutzungsmöglichkeiten verloren, wie z.B. der oft beschworene intelligente Kühlschrank und ähnliche smarte Haushaltsgeräte; jeglicher Folgeservice (z.B. bei Kleidung die automatische Auswahl passender Accessoires) und schlussendlich die Automatisierung bei Umtausch, Reparatur und Recycling.

Als Alternative zur „Alles oder Nichts"-Mentalität des Kill-Befehls kamen schon früh Ansätze ins Spiel, die zum Ziel hatten, die Nutzdaten des RFID-Tags (in den meisten Fällen also dessen ID bzw. den darauf befindlichen Produktcode) nicht zu löschen, sondern lediglich vor unerlaubtem Auslesen zu schützen. Sobald ein Produkt in den Besitz des Kunden übergeht, erhält dieser die Kontrolle über die Ausgabe des integrierten RFID-

[12] Während in der ursprünglichen Spezifikation lediglich 8 Bit vorgesehen waren, wird für die nächste Generation bereits die Verwendung von 32 Bit in Betracht gezogen.

Tags und kann so selektiv entscheiden, wer welche Informationen vom Tag auslesen kann. Die grundlegende Idee dazu wurde bereits 2002 von Sarma et al. vorgestellt [SWE02]. Dabei antwortet ein Tag statt mit seiner „wahren“ ID mit einer „MetaID“ – einem verschlüsselten Wert, der nur mit dem Wissen um den verwendeten Schlüssel dechiffriert werden kann. Da jedoch das Verfolgen eines bestimmten Tags trotz Chiffrierung auch weiterhin möglich ist, wurde vorgeschlagen, diesen verschlüsselten Wert nach jedem Auslesevorgang entlang eines vom Schlüssel abhängigen Verfahrens zu ändern. Dadurch könnten legitime Besitzer des gekennzeichneten Gegenstandes diesen weiterhin identifizieren, das unerlaubte Ablesen wäre dadurch jedoch nutzlos geworden.

Auch bei diesem Verfahren gestaltet sich die praktische Umsetzung schwierig. Ähnlich wie zuvor schon beim Kill-Befehl ist unklar, ob sich die für dieses Verfahren nötige soft- und hardwaretechnische Infrastruktur entlang komplexer Lieferketten und außerhalb riesiger Einzelhandelsketten überhaupt ökonomisch und politisch durchsetzen lässt. Juels [Jue04] schlägt deshalb einen stark vereinfachten Ansatz ohne jegliche Verschlüsselung vor, bei dem jedes Funketikett einfach eine fixe Anzahl gespeicherter IDs in fester Reihenfolge verwendet. Doch auch jenseits komplexer Schlüsselsynchronisationsverfahren bleibt die Herausforderung, die zur Kontrolle des RFID-Tags nötigen Informationen beim Verkauf eines Produktes dem Kunden zu übermitteln. Gerade vor dem Hintergrund zahlreicher medienwirksam gescheiterter IT-Systeme (Beispiel: deutsche LKW-Maut) scheint eine reibungslose und spontane Einbinden beliebiger Kunden-IT-Systeme (wenn nicht schon deren Existenz) zwecks automatisierter Übergabe der für die RFID-Tag Verwaltung nötigen Schlüssel in nächster Zukunft schnell utopisch.

Als Alternative zu managementintensiven passwortbasierten Lösungen schlugen Fishkin und Roy [FiR03] bereits frühzeitig distanzbasierte Zugriffskontrollen vor. Dabei würden RFID-Tags die Signalstärke des auslesenden Lesegeräts messen und in Abhängigkeit von dessen daraus ermittelter Distanz mehr oder weniger Details preisgeben – bei großer Distanz beispielsweise lediglich die Präsenz eines Tags, bei größerer Nähe generische Klassenattribute (z.B. die Farbe) und beim geringsten Abstand schließlich die eindeutige ID. Auch wenn das Grundprinzip dieses Ansatzes einfach ist, ist dessen praktische Umsetzung heikel, da die tatsächliche Stärke eines Lesesignals nicht nur vom Abstand zwischen Etikett und Lesegerät ab, sondern auch von der Orientierung des Tags relativ zur Antenne des Lesers (stehen diese genau senkrecht zueinander, geht die Signalstärke meist gegen Null) bzw. der Umgebung (Wasser und metallische Leiter vermindern ebenfalls die Signalstärke). So könnte ein solches System legitime Leseversuche aus nächster Nähe plötzlich erschweren, da das

RFID-Tag fälschlicherweise eine zu große Distanz misst. Umgekehrt könnte ein Angreifer sein Lesegerät mit überhöhter Sendeleistung betreiben und so eine größere Nähe vortäuschen lassen. Schnell würden so die mangelnde Verlässlichkeit einer solchen Lösung, als auch deren erhöhte Kosten für die dazu nötige Elektronik auf den Funketiketten, weder Kunden noch Hersteller zufrieden stellen.

Realistischer scheinen Token basierte Ansätze, bei denen der Kunde ein so genanntes „Blocker-Tag“ mit sich führt, welches das Auslesen aller in seiner Nähe befindlichen Funketiketten verunmöglicht. Juels et al. [JRS03] verwenden dazu ein modifiziertes RFID-Tag, welches auf jede mögliche ID antwortet und so die tatsächlich mitgeführten Gegenstände versteckt bzw. Lesegeräte praktisch blockiert, da diese beginnen, mehrere Billionen (virtuelle) Funketiketten auslesen zu wollen. Dieser zunächst wieder äußerst einfache wie effizient erscheinende Ansatz muss allerdings in der Praxis ebenfalls relativiert werden. Damit ein mitgeführtes Blocker-Tag nicht jegliche, d.h. auch legitime Lesevorgänge, in einem mehreren Meter großen Radius unterbindet, schlagen die Autoren ein standardisiertes *privacy*-Präfix vor, mit dem zu schützende Funketiketten versehen werden. RFID-Tags ohne dieses Präfix werden vom Blocker-Tag nicht geschützt. Diese Lösung erfordert jedoch, dass persönliche Gegenstände jeweils manuell in den geschützten Bereich ein- und ausgebucht werden.[13] Auch unterliegt ein einfaches Blocker-Tag denselben Unwägbarkeiten wie reguläre RFID-Tags, d.h. eine zu große Nähe zu einem metallischen Leiter könnte seinerseits das Blocker-Tag deaktivieren, wodurch sämtliche geschützten Tags plötzlich sichtbar würden. Erst bei der Verwendung eines batteriebetriebenen Geräts, z.B. eines Mobiltelefons, könnte eine ausreichende Verlässlichkeit eines solchen Ansatzes sichergestellt werden. Lässt man das Handy jedoch zuhause liegen, ist man für den Rest des Tages sämtlichen Lesevorgängen wieder schutzlos ausgeliefert.

5.2 Abhörsicheres Auslesen

Auch wenn mit einem der oben beschriebenen Verfahren lediglich autorisierte Lesestationen Zugriff auf die auf dem RFID-Tag gespeicherten Informationen haben sollten, so besteht aufgrund der Sendeleistungs-Asymmetrie zwischen Lesegerät und Tag die Möglichkeit, dass Daten, die vom Leser zum Tag gesendet werden, von nicht autorisierten Lesestationen mitgehört werden. Denn aufgrund der Energiekopplung zwischen Lesestation und RFID-Tag hat das vom Lesegerät erzeugte Feld immer die

[13] Beim Ausbuchen darf natürlich kein Blocker-Tag in der Nähe sein.

vielfache Reichweite des vom Tag reflektierten Rückkanals. Dies ermöglicht es unbeteiligten Dritten, die vom Leser an das Tag gesendeten Informationen noch in relativ weiter Entfernung mitzuhören.[14]

Die offensichtliche Lösung ist das Verschlüsseln der Datenübertragung. So verwendet der neue deutsche biometrische Reisepass das symmetrische Verschlüsselungsverfahren „Triple-DES“ [Wik06b] mit einem 112-bit langen Schlüssel,[15] um die per Funk an das Lesegerät übertragenen persönlichen Daten zu schützen [Küg05]. Bevor jedoch das Lesegerät den im Pass befindlichen Funkchip auslesen kann, muss dieser durch ein wie oben beschriebenes Anti-Kollisionsverfahren eindeutig ausgewählt (*singularisiert*) werden – ein Vorgang, der für jedes RFID-Tag eine eindeutige ID benötigt.[16] Zwar kann diese laut dem zugrunde liegenden Standard [ISO00] vom Tag jedes Mal zufällig gewählt werden, doch treibt dies die Herstellungskosten signifikant in die Höhe und wird deshalb in den meisten Fällen mit einer statischen ID gelöst.[17] So lassen sich selbst Tags, deren Inhalte verschlüsselt sind, entlang mehrerer Lesegeräte verfolgen. Darüber hinaus ist die Verschlüsselung der Nutzdaten eines Funketiketts und dem damit verbundenen Kennwort-Management – wie schon bei Kill-Befehl oder MetaID – nur für hochpreisige Gegenstände praktikabel, da sowohl die erhöhte Komplexität des RFID-Chips, als auch die zur Ver- und Entschlüsselung nötige Infrastruktur, signifikante Kostenfaktoren darstellen, die sich kaum für Coladosen oder T-Shirts rechnen werden.

Am Beispiel des biometrischen Reisepasses werden auch die praktischen Schwierigkeiten der Verschlüsselung sichtbar: Um ein Auslesen durch autorisierte Stellen nicht zu verunmöglichen, kann ein persönlicher PIN-Code nicht verwendet werden. Ein einziges Standardkennwort scheidet ebenso aus. Stattdessen wird beim ePass der Schlüssel jeweils aus Passnummer, dem Geburtsdatum und dem Ablaufdatum des Ausweises gebildet, der so durch optisches Auslesen des Passes jederzeit z.B. durch

[14] Natürlich können auch die vom Funketikett zurück gesendeten Informationen mit genügend feinfühligen Antennen abgehört werden, sofern unberechtigte Dritte nah genug an einen legitimen Auslesevorgang heran kommen können.

[15] Aufgrund des normierten Schlüsselaufbaus (dieser besteht immer aus der Passnummer, dem Geburtsdatum und dem Ablaufdatum des Ausweises) ist die Stärke des 112-bit Schlüssels allerdings maximal 56-bit [Küg05].

[16] Diese ID kann, muss aber nicht identisch sein mit der „eigentlichen“ ID des RFID-Tags, z.B. dem Produktcode (EPC-Code) bei einer Coladose. Da beim Reisepass die Passnummer durch Verschlüsselung geschützt ist, kann diese dazu nicht verwendet werden.

[17] Ob dies in biometrischen Reisepässen einiger Länder der Fall ist, ist umstritten. So soll beispielsweise der holländische ePass statische IDs im Anti-Kollisions-Protokoll verwenden [Slas04]

Grenzbeamte in Erfahrung gebracht werden kann. Kennt man allerdings einmal diese Daten, so lässt sich ein gesuchter Pass auch ohne optischen Auslesen abfragen. So kamen bereits früh beunruhigende Gedankenspiele zu „smarten“ Bomben auf, die alle vorbeilaufenden Pässe auszulesen versuchen, um beim erfolgreichen Abfragen des Passes der Zielperson schliesslich zu detonieren [Jäg05].

Geht es allein darum, die ID-Übermittlung eines Funketiketts vor unerlaubtem Abhören zu sichern, ist die Verwendung von Zufallszahlen zur Singularisierung die verlässlichste Methode. Ihr Einsatz ist in praktisch allen Standards von EPCglobal (z.B. [EPC04]) bereits vorgesehen, jedoch optional. Hierbei wählen RFID-Tags, sobald sie durch ein Lesegerät mit Energie versorgt werden, zunächst eine zufällige Zahl aus einem ausreichend grossen Zahlenbereich. Im Folgenden kann das Lesegerät im Rahmen eines Anti-Kollisionsprotokolls das Tag mit Hilfe dieser Nummer auswählen (d.h. diese Nummer wird im Klartext mit der hohen Sendeleistung des Lesers übertragen), bevor dieses dann, nach erfolgter Auswahl, mit seiner „wahren“ ID antwortet. Da diese Antwort jedoch mit der weitaus geringeren Sendeleistung des passiven RFID-Tags gesendet wird, ist die Abhörwahrscheinlichkeit, auch ohne Verschlüsselung, relativ gering. Nach einer Unterbrechung der Energiezufuhr und einem späteren erneuten Auslesen wählt das Tag einen neuen Zufallswert und kann so ein Verfolgen durch Abhören der Singularisierung verhindern.[18]

5.3 Proxy-basierter Schutz

Im Zusammenhang mit dem von Juel et al. vorgeschlagenen *Blocker-Tag* (Abschnitt 5.1) war bereits die Rede von der Verwendung eines mächtigeren, batteriebetriebenen Gerätes (z.B. dem Mobiltelefon), welches die nötigen Schutz- und Managementfunktionen – d.h. Schutz vor unautorisiertem Auslesen, sowie ein Kennwortmanagement zwecks Autorisierung und Abhörsicherung – für alle mit sich geführten Funketiketten anbieten kann. Durch die Auslagerung solcher Funktionen können diese darüber hinaus nicht nur verlässlicher, sondern auch anspruchsvoller gestaltet werden. So könnte beispielsweise ein Blocker-Handy ebenso in Abhängigkeit

[18] Dieses Verfahren funktioniert sowohl für UHF- als auch HF-Tags (vgl. Abschnitt 3). Für baum-basierte Anti-Kollisionsprotokolle, die bei UHF-Systemen oft zum Einsatz kommen, schlugen Weis et al. [WSR+03] darüber hinaus mit dem so genannten *Silent-Tree-Walking* ein besonders einfaches, auf XOR-Berechnung basierendes Verfahren vor, welches sich weitaus kostengünstiger als Zufallszahlen implementieren lässt. Bisher wurde dies allerdings noch in keinem Standard umgesetzt.

des Aufenthaltsortes das Auslesen der eigenen Funketiketten frei schalten: z.B. im eigenen Zuhause, oder für das jeweilige Paar Schuhe, welches man trägt, wenn man sich im Schuhgeschäft an der Ecke befindet [JSB05].

Flörkemeier et al. [FLS04] schlagen darüber hinaus vor, explizite Datenschutzinformation in RFID-Protokolle zu integrieren, um so beispielsweise von Lesegeräten zu verlangen, dass sie explizit Urheber und Zweck der Datensammlung in einem maschinenlesbaren Format benennen. Auch wenn nicht jeder Konsument an solcherlei Informationen interessiert sein mag, so würde eine generelle, maschinenlesbare Deklarationspflicht von RFID-Lesevorgängen sowohl behördlichen Datenschützern, als auch Konsumentenschützern eine einfache Überprüfung der Datenschutzgesetze erheblich erleichtern. Dabei würde ein persönliches Assistenzgerät also weniger die Rolle eines „Beschützers“ spielen, sondern die eines „Aufklärers“, der bei Bedarf das Ausleseverhalten einer Umgebung sichtbar macht.

6 Gesellschaftliche Trends zum Einsatz von RFID

Die Frage, ob es in Zukunft wirklich zu einem flächendeckenden – und damit nachhaltig unser Leben beeinflussenden – Einsatz von RFID kommen wird, scheint müßig Angesichts der Tatsache, dass bereits heute eine Vielzahl von Anwendungen wie selbstverständlich mit Funketiketten funktionieren. Mit RFID-Tags versehene Autoschlüssel sind die Grundlage der praktisch in allen Neuwagen zu findenden Wegfahrsperre: erst wenn ein im Zündschloss befindlicher Leser das RFID-Tag im Schlüssel eindeutig identifiziert hat, kann das Auto gestartet werden.[19] Ebenso verbreitet sind kontaktlose Skipässe, die in vielen Skigebieten bereits die lästige Fummelei am Skilift ersparen, da sie bequem in der Jackentasche aufbewahrt werden können und durch die Kleidung hindurch überprüft werden können. Ähnliche kontaktlose Zugangssysteme gewähren in hunderten von Bürogebäuden Firmenmitarbeitern unkomplizierten Einlass. Als batteriegetriebene, aktive Tags („TELEPASS“) erlauben sie täglich tausenden von Pendlern in Italien, ohne Anzuhalten durch Autobahnmautstationen zu fahren.

Ist die offensichtliche Akzeptanz solcher Anwendungen nun ein Zeichen dafür, dass ein flächendeckender Einsatz dieser Technologie unbedenklich

[19] Nicht zu verwechseln mit der ferngesteuerten Türöffnung bzw. –schliessung, wofür typischerweise ein batteriegetriebener Infrarot- bzw. Funksender eingesetzt wird, der ein verschlüsseltes Codewort an den Wagen sendet. Typischerweise sind beide Systeme in einem einzigen Wagenschlüssel untergebracht.

ist? Oder zeigt es lediglich, dass begrenzte, nicht interoperable Insellösungen ein geringeres Überwachungspotential besitzen, als die offen kritisierten Zukunftsvisionen der RFID-Technik? Sind diese Beispiele überhaupt repräsentativ für die zukünftige Verbreitung von RFID? Im Folgenden soll versucht werden, mögliche Treiber für die fortschreitende Verbreitung drahtloser Funketiketten in unserem Alltag zu identifizieren, sowie deren Potential für eine Einflussnahme auf unsere gefühlte wie tatsächliche Privatsphäre abzuschätzen. Dies soll anhand dreier Hauptmotivationen erfolgen: Bequemlichkeit und persönliche Produktivität; wirtschaftliche Effizienz und Kostenersparnis; sowie Gesundheit und nationale Sicherheit.

6.1 Bequemlichkeit und persönliche Produktivität

Skipass, Mautgerät und Autoschlüssel „funktionieren“, weil sie dem Nutzer einen greifbaren Vorteil bieten. Sie gestalten Abläufe *bequemer*, als sie es ohne den Einsatz von RFID waren. Streifenkarten, die erst mühsam vom Liftpersonal abgeknipst werden mussten, oder Magnetkarten, die in kleine Schlitze am Lifteingang eingeführt wurden, erforderten ein umständliches Ausziehen der Handschuhe, ein Suchen nach der richtigen Anoraktasche und das anschließende Wiederverstauen. Dies barg nicht nur die Gefahr, dass ein unachtsam geschlossener Reißverschluss während der Lift- oder Talfahrt aufgehen und das Ticket herausfallen konnte, sondern führte auch zu verlängerten Abfertigungszeiten am Skilift. Ein gut eingestelltes, drahtloses Zugangssystem erlaubt nicht nur schnellere Abfertigung, sondern befreit den Nutzer von dem umständlichen Hantieren mit manuellen Tickets. Das in einige Swatch-Uhren eingebaute *Snowpass/Access* System[20] erlaubt sogar das Speichern von Tages-, Wochen- und Saisonkarten, zum Teil sogar bequem vor der Anreise ins Skigebiet vom heimischen PC aus. Das italienische *TELEPASS* System befreit nicht nur von der lästigen Suche nach Kleingeld oder dem ständigen Nachkaufen spezieller Mautkarten, sondern erlaubt die Verwendung einer privilegierten, praktisch staufreien Extraspur. Und dank dem Einbau einer RFID-basierten Wegfahrsperre können Autofahrer ihre Versicherungsprämie senken, ohne eine separate Alarmanlage installieren zu müssen, die aufwändiges Ein- und Ausschalten verlangt.

Dabei geht es nicht nur um die durch den Einsatz von moderner Technik *unmittelbar* eingesparte Zeit – das schnellere Durchfahren der Maut- oder Liftstation, bzw. das schnellere Abschließen des Autos ohne separate Alarmanlage. Auch der indirekte, d.h. durch Vorbereitung und Unterhalt nö-

[20] Siehe www.swatch.com/snowpass

tige Aufwand kann für den Nutzer moderner Technik einen signifikanten Anstieg der Bequemlichkeit – und damit implizit eine hohe Akzeptanz trotz potenzieller negativer Folgen – bedeuten. Bestes Beispiel ist das Mobiltelefon, welches im eingeschalteten Zustand dem jeweiligen Mobilfunkbetreiber (bzw. im Falle eines Verbrechens den Strafverfolgungsbehörden) ein praktisch lückenloses, weltweites Bewegungsprofil des Kunden liefert. Doch der Vorteil, schnell und unkompliziert überall und jederzeit Termine umzudisponieren bzw. Auskünfte einholen zu können, wiegt für viele Nutzer die Nachteile einer potenziellen Überwachung mehr als auf. Gleiches gilt für die moderne Errungenschaft des bargeldlosen Bezahlens durch Geld-, Bank- und Kreditkarten, die den Karten ausgebenden Instituten detaillierte Einblicke in die Kauf- und Bewegungsmuster der Kunden erlauben. Doch angesichts ihrer substantiellen Vorteile (keine umständliche Suche nach Kleingeld, Bankautomat oder Wechselstube) werden die „Gefahren" für die persönliche Privatsphäre nüchtern abgewogen und in den meisten Fällen als akzeptabel beurteilt.

Die obigen Beispiele deuten darauf hin, dass ein Einsatz drahtloser Funketiketten zur effizienteren Durchführung altbekannter Vorgänge, d.h. sowohl im eigentlichen Ablauf, als auch in der dazu nötigen Vorbereitung, mit hohen Akzeptanzraten bei Konsumenten rechnen kann. Statt Coladosen und Kaugummipackungen werden es also zunächst hochpreisige Konsumgüter sein, die – zunächst durchaus noch optional – mit Funketiketten versehen dem Konsumenten einen direkten Mehrwert bieten können. So könnten reparaturanfällige Haushaltsgeräte wie Kaffee-, Wasch- und Geschirrspülmaschinen eine unkomplizierte Garantieabwicklung dank RFID-basierter Identifikation durch den Kundendienst bieten. Mit der zunehmenden Verbreitung von so genannten NFC-fähigen[21] Mobiltelefonen, die RFID-Tags auslesen können, sind sogar Selbstdiagnosesysteme denkbar, bei denen der Kunde sein Handy an das defekte Gerät hält und die Fehlerursache übermittelt bekommt, um entweder ein fehlendes Ersatzteil direkt im Herstellershop bestellen zu können bzw. den Besuch eines Servicemechanikers zu vereinbaren.

Überhaupt scheint die NFC-Technologie das Mobiltelefon in Zukunft mehr denn je zum zentralen Bestandteil des modernen Lebens zu machen. So erproben bereits seit geraumer Zeit mehrere Verkehrsverbünde in Europa in groß angelegten Feldversuchen den Einsatz NFC-basierter Fahrkartensysteme. Realität ist dies bereits in Japan, wo Handybesitzer beim Ein-

[21] Die Abkürzung NFC steht für *Near Field Communication* und bezeichnet einen herstellerübergreifenden Standard, der es z.B. Mobiltelefonen erlaubt, spezielle NCF-kompatible Funketiketten drahtlos auszulesen. Siehe dazu auch den Beitrag von Mattern in diesem Band.

treten bzw. Verlassen der U-Bahn-Station nur kurz ihr Handy an das Drehkreuz halten, um automatisch den korrekten Fahrpreis zwischen Ein- und Ausstiegsort abgebucht zu bekommen [JRE05]. In Hanau bei Frankfurt/Main kann seit April 2006 in sämtliche Stadtbussen per NFC-Handy bezahlt werden – nach einem zehnmonatigen Feldversuch mit über 150 Kunden stieß dieses Angebot auf so viel Begeisterung, dass es praktisch übergangslos im Regelbetrieb eingesetzt wurde. Der Besitzer eines entsprechenden Mobiltelefons hält beim Ein- und Aussteigen das Handy einfach in die Nähe des im Bus angebrachten Lesegerätes und erhält zum Monatsende eine Rechnung, in der sämtliche unternommene Fahrten mitsamt den Kosten aufgeführt sind [Tec06].

Beispiele wie diese illustrieren weitaus besser das Entwicklungspotenzial drahtloser Funketiketten, als die frühen technikverliebten und realitätsfernen Beispiele wie etwa der mehr als überstrapazierte „smarte Kühlschrank“[22]. Der ungebremste Drang nach persönlicher Produktivität und Bequemlichkeit in einem für den Einzelnen immer komplexer werdenden Alltag kann also als eine wichtige Triebfeder für den weiter voran schreitenden Einsatz der RFID-Technologie gewertet werden – insofern solche Lösungen einen tatsächlichen Mehrwert für den Nutzer leisten können. Sobald dies gegeben ist – wie beispielsweise bei Wegfahrsperren, Skipässen oder NFC-basierten Fahrkartensystemen – sind die typischerweise mit RFID assoziierten negativen Folgen für viele Kunden kaum noch wahrnehmbar. So scheint es durchaus realistisch, dass sich solche RFID-basierte Anwendungen, zumindest in isolierten Anwendungsgebieten, bereits in naher Zukunft immer mehr durchsetzen werden.

6.2 Wirtschaftlichkeit

Nicht erst seit Globalisierung und hohe Arbeitslosigkeit Schlagzeilen machen, ist *wirtschaftliche* Effizienz ein Thema. Der Einsatz von RFID-Technologie, vor allem in der Logistik, verspricht nun signifikante Kosteneinsparungen nicht nur in der Lagerhaltung, sondern auch in der Produktion.[23] Einzelhandelsgigant Wal-Mart schreibt bereits seit Anfang 2005 seinen hundert grössten Zulieferern die Verwendung von Funketiketten auf Paletten und Verpackungseinheiten vor[24] – ersten Auswertungen zufolge

[22] Zahlreiche Kritiker des Ubiquitous Computing haben dieses Haushaltsgerät bereits der Lächerlichkeit preisgegeben, sogar ein Comic über „Frigomax – den Kühlschrank auf Draht“ existieren (www.itoons.de/comics/frigomax/)

[23] Zur Theorie des Bull-Whip Effektes, siehe z.B. [FlM05]

[24] Inzwischen (Juni 2006) setzen die 300 grössten Wal-Mart Zulieferer RFID auf Paletten und Verpackungseinheiten ein [Das06].

konnte dadurch für viele Produkte die „out-of-stock“-Quote um bis zu 62% reduziert werden [Col06], was sich beispielsweise bei (ebenfalls auf den Kartons mit Funketiketten ausgestatteten) Rasierklingen von Gilette in einer Umsatzsteigerung von 19% niederschlug [Das06]. Ähnliche Erfolge melden die deutsche Metro und der britische Einzelhändler Tesco, die ebenfalls RFID-Technologie in einigen ihrer Verteilzentren einsetzen [Ren06].[25]

Auch wenn der Einsatz von RFID hier fernab vom Kunden in Logistikzentren und Warenhäusern stattfindet, darf der Einfluss erfolgreicher RFID-Lieferketten auf die Privatsphäre des einzelnen Konsumenten nicht unterschätzt werden: die Investitionen der grossen Vorreiter Wal-Mart, Tesco und Metro (als auch des US-amerikanischen Verteidigungsministeriums, eines der grössten Logistikunternehmen weltweit) helfen auf breiter Front, die Kosten zu senken sowie Know-How aufzubauen, was wiederum die Verbreitung von RFID auch im kleineren Massstab begünstigt. So sind beispielsweise in allen 69 Samsung-Tesco-Supermärkten[26] in Korea sämtliche Einkaufswagen und -körbe mit RFID-Tags ausgestattet, mit denen die Bewegungen der Kunden innerhalb eines Marktes verfolgt werden [Tan06]. Angeblich wurden anhand dieser Daten bereits in einigen Märkten erfolgreich Produktstandorte relokalisiert.[27] Ebenso haben bereits mehrere grosse öffentliche Bibliotheken (Wien, Graz, Winterthur, München, selbst im Vatikan) Funketiketten in ihren Büchern integriert, um sowohl die Lagerhaltung als auch den Ausleihprozess zu optimieren [Kan04].

Die Beispiele zeigen, dass die Verbreitung von RFID-Chips in Alltagsgegenständen auch ohne die Allmachtsfantasien totalitärer Staaten in naher Zukunft stetig voranschreiten wird. Mit wachsenden Absatzmärkten fallen die Kosten und steigt das Know-How, die Grundvoraussetzungen für den erfolgreichen und rentablen Einsatz von RFID in zahllosen Bereichen, wodurch wiederum die Einführung von Kundenbindungsprogrammen auch für Klein- und mittelständische Betriebe rentabel wird. So könnte beispielsweise die Existenz einer weltweit standardisierten Informationsinfrastruktur zum Dekodieren von EPC-Tags den Aufbau eines solchen Kundendatei den Aufbau eines deutschland- oder europaweiten Verbunds ermöglichen, in dem Kosten weiter gesenkt und „Synergieeffekte“ ausge-

[25] Nicht zu verwechseln mit dem Einsatz von RFID in Supermärkten.

[26] Samsung-Tesco Supermärkte sind ein Joint Venture zwischen dem Elektronikriesen Samsung und dem britischen Einzelhändler Tesco.

[27] Dies steht im Gegensatz zum modernen „Beer and Nappies“-Märchen, dass Wal-Mart angeblich dank Data Mining einen hohe Korrelation zwischen Bier- und Windelkäufen erkannt haben soll und durch cleveres Umplatzieren der entsprechenden Produktgruppen Millionengewinne einfahren konnte [Bis06,Fri97]

nutzt werden könnten. Kundenkarten, die sich schnell und einfach auf ein NFC-fähiges Mobiltelefon laden lassen und von dort jederzeit auslesbar sind, könnten im gleichen Maße die Akzeptanz und Nutzung unter den Kunden erhöhen.

6.3 Sicherheit

Die persönliche Sicherheit ist nicht erst seit den Anschlägen vom 11. September ein Thema. Doch seit Selbstmordattentäter nicht mehr nur in Ländern der Dritten Welt oder im Nahen Osten operieren, sondern auch von ruhigen Vororten in Nordamerika und Europa, ist das Bewusstsein für die Verletzlichkeit einer offenen Zivilgesellschaft, die auf einen freien Informationsaustausch, Waren- und Personenverkehr beruht, stetig gewachsen. Eine detaillierte Überwachung der zahllosen Güter- und Personenströme scheint für viele Bürger der einzige Weg, Straftaten nicht mehr nur aufzuklären, sondern bereits im Vorfeld zu verhindern.

So befürworteten beispielsweise im Vorfeld der Fußballweltmeisterschaft 84% der Deutschen eine lückenlose Videoüberwachung aller öffentlichen Plätze [Spi06], eine Studie des Instituts für Kriminologische Sozialforschung der Universität Hamburg fand eine ähnliche hohe Zustimmung in der Bevölkerung [Küp06]. Intelligente Programme sollen dabei helfen, in der zunehmenden Bilderflut „verdächtige“ Personen und Verhaltensweisen zu erkennen und Sicherheitspersonal rechtzeitig darauf aufmerksam machen. Auch wenn aktuelle Systeme noch kaum mit der Komplexität einfacher Alltagssituationen (z.B. wartenden Reisenden auf einem Zuggleis) zurecht kommen, so haben nicht zuletzt durch Videoüberwachung möglich gewordenen rasche Fahndungserfolge – die Kofferbombenleger von Dortmund und Koblenz im Juli 2006 [Ram06],[28] oder etwa die Überführung zweier minderjähriger Mörder im Fall James Bulger 1993 in England [Wik06a] – die Akzeptanz für Überwachungssysteme signifikant erhöht. Inzwischen sollen in Großbritannien, dem "Videoüberwachungsland", mehr als 40.000 Kameras in 530 städtischen Überwachungssystemen installiert sein [Küp06], weitere 300 Systeme kommen darüber hinaus in kommunalen Wohnblocks zum Einsatz [Ali06].

Der Einsatz von RFID zwecks Erhöhung der Sicherheit scheint in Anbetracht solcher Erfolge nahe liegend und akzeptabel, wie beispielsweise die Verwendung der Funketiketten in den mehr als 3 Millionen Eintrittskarten zur Fußball-WM im Sommer 2006 in Deutschland zeigte. Zwar wa-

[28] Videos von den Überwachungskameras können auf den Webseiten des BKA bezogen werden: www.bka.de/fahndung/personen/tatkomplexe/trolley/video.html

ren die Auflagen bei Verkauf und Weitergabe der Karten heftig umstritten und nur schwierig umzusetzen,[29] doch wurde zum Schutz vor Fälschern, Hooligans und Terroristen weitgehend akzeptiert, dass persönliche Angaben wie Name, Alter, Ausweisnummer und Konto- bzw. Kreditkartennummer auf dem RFID-Tag gespeichert und innerhalb der WM-Stadien jederzeit überprüft werden konnten.

Ein anderes Beispiel in diese Richtung stellt die DNS-Analyse dar, die – zumindest in Großbritannien – einen der Videoüberwachung nicht unähnlichen Aufstieg zum Wundermittel gegen Kriminalität hinter sich hat. Inzwischen besitzt das Königreich die größte DNS-Kartei der Welt, mit über 2.5 Millionen Datensätzen – 5% der Bevölkerung [SiW05]. Nachdem Anfangs DNS-Proben nur von verurteilten Sexualstraftätern gesammelt wurden, wurde die Sammlung erst auf alle verurteilten Kapitalverbrecher, schließlich auf alle *angeklagten* Kapitalverbrecher ausgeweitet [Hos06]. Inzwischen können DNS-Proben von jedem Bürger gesammelt werden, der eines Verbrechens angeklagt ist – selbst wenn die DNS-Probe für die Ermittlungen unnötig ist (z.B. Anklagen wegen der Teilnahme an einer unerlaubten Demonstration, oder wegen Bettelns) [SiW05].

Diesen Trend bezeichnet der britische Datenschutzexperte Gus Hosein als „Entkriminalisierung von Datensammlungen“ [Hos06]: Während Datenschutzgesetze traditionell das Prinzip der „Datenvermeidung und Datensparsamkeit“ vorschreiben,[30] bei dem „*keine oder so wenig personenbezogene Daten wie möglich*“ erhoben werden sollen, so beobachtet Hosein in der aktuellen Rechtssprechung, dass dieser Erforderlichkeitsgrundsatz mehr und mehr auf die *Nutzung* der bereits gesammelten Daten verschoben wird, statt die Sammlung selbst zu hinterfragen [Hos06]. In Anbetracht der Möglichkeiten, mit RFID-Tags versehene Gegenstände einfach und ohne Beeinträchtigung für den Nutzer auslesen und identifizieren zu können, scheint diese Entwicklung besonders relevant, da die durch den Einsatz von RFID-Systemen anfallenden Datensammlungen in ihrer Zusammensetzung so kaum noch hinterfragt werden würden.

Selbst jenseits von Terrorismus und Gewaltverbrechen wird die institutionalisierte Kontrolle mehr und mehr ausgedehnt, nicht um den Bürger vor anderen, kriminellen Elementen zu schützen, sondern vor sich selbst. Klassisches Beispiel ist der in Europa übliche Zwang zum Abschluss einer Kranken-, Renten-, Arbeitslosen- und Autohaftpflichtversicherung, oder der praktisch weltweit übliche restriktive Verkauf von Alkohol und Niko-

[29] Ein Grossteil der Tickets war persönlich und durfte nur an Familienangehörige bzw. in Härtefällen übertragen werden.

[30] So auch das aktuelle deutsche Bundesdatenschutzgesetz (BDSG) in §3a, siehe auch bundesrecht.juris.de/bdsg_1990/__3a.html

tin, bzw. das Verbot von Rauschmitteln und Drogen, wie etwa Marihuana oder Kokain. Neben harten Zwängen und Strafen setzen mehr und mehr Staaten auch auf sanftere Methoden der Überzeugung, den so genannten *soft paternalism* [Eco06], wie beispielsweise großflächige Warnhinweise auf Zigarettenverpackungen oder Steuervergünstigungen für Nutzer des öffentlichen Nahverkehrs.

Neue Technologien erlauben es nun, diese Formen von Kontrolle und Überredung auf viele Bereiche auszudehnen. So warnen schon seit einigen Jahren die meisten Neuwagen mit einem Alarmsignal, wenn ohne Anlegen des Anschnallgurtes der Motor gestartet wird. Der schwedische Automobilhersteller Saab stellte bereits 2004 den *Alcokey* vor, eine Variante der klassischen Wegfahrsperre, die nur dann die Zündung frei gibt, wenn der Fahrer vorher durch Blasen in ein Röhrchen seine Nüchternheit beweisen konnte [ODo06]. Spiekermann und Pallas sehen bereits die neue Form des „Technologiepaternalismus“ auf uns zukommen [SpP05], bei dem mit Hilfe der RFID- und anderer Sensortechnik automatische Systeme ihre Besitzer bei der Einhaltung von Regeln oder Empfehlungen überwachen und gegebenenfalls deren Befolgung erzwingen. Mit RFID-Tags ausgestattete Verkehrszeichen könnten es Autos erlauben, lokale Verkehrsregeln zu detektieren und beispielsweise das Parken im absoluten Halteverbot zu unterbinden, indem etwa das Abschalten des Motors unmöglich gemacht wird. Zigarettenautomaten könnten die Ausgabe ihrer Ware vom Auslesen eines gültigen, mit RFID-Technik ausgestatteten Ausweisdokuments abhängig machen, um Minderjährigen den Zugriff zu verweigern.

7 Werden wir auch in Zukunft noch eine Privatsphäre haben?

Wohin führt uns die zunehmende Durchdringung unseres Alltags mit winzigen, drahtlos auslesbaren Funketiketten? Viele der oft zitierten Bedrohungsszenarien – Supermarktketten, die jeden unserer Schritte beobachten und uns mit scheinbar allwissenden Telefonanrufen terrorisieren, oder Diebe, die mit einem einfachen Lesegerät in Sekundenschnelle unseren Gesamtwert[31] oder den unseres Hauses taxieren – scheinen für die potenzielle Angreifer weder praktikabel, noch besonders effektiv.

Die Beispiele im vorherigen Abschnitt versuchten zu illustrieren, dass zu den *technischen Möglichkeiten*, die den flächendeckenden Einsatz von

[31] Also unser mitgeführtes Bargeld, plus etwaige auf dem Schwarzmarkt verkäufliche Designer-Kleidungsstücke oder begehrte amtliche Dokumente, wie Ausweise oder Führerscheine.

RFID in naher Zukunft zumindest praktisch machbar erscheinen lassen, also eine ganze Reihe von *gesellschaftlichen Wünschen* kommen, die diesen Einsatz auch gezielt umzusetzen versuchen könnten. Jedoch ohne den für dieses Thema so typischen Überwachungsreflex bei Bürgern und Kunden auszulösen, da konkreter Mehrwert für den Anwender geschaffen wird: vereinfachte Abläufe, günstigere Preise und ein sichereres Leben.

Die „Gefahr", wenn man sie denn so nennen möchte, besteht also vielleicht vielmehr darin, dass wir selbst aufgrund unserer eigenen Bequemlichkeit, unserem Spaß am Sparen und unserer Angst vor potenziellem Unglück dabei *mithelfen* wollen, unser Leben mit der Hilfe von RFID mehr und mehr zu überwachen. Internet-Läden wie Amazon oder Apples iTunes demonstrieren bereits heute, welchen Mehrwert das detaillierte Aufzeichnen unseres Kauf- bzw. Hörverhaltens für uns haben kann. Statt gefühlter Überwachungsdiktatur durch allgegenwärtige Funkchips also in Zukunft ein Paradies an kostenlosen (!) Dienstleistung, die uns die Orientierung im Konsumdschungel erleichtern und uns auf einmalige Angebote aufmerksam machen? Wenn wir z.B. bei unserem nächsten Ikea Besuch gefragt werden, ob wir unser Payback-Profil in unseren Einkaufswagen laden wollen, um „Lifestyle-gerechte" Tipps beim Möbelkauf zu erhalten – wer würde es nicht einfach einmal ausprobieren? Und wenn es funktioniert und später sogar noch unsere bereits getätigten Einkäufe beim Möbelgiganten mit einbeziehen kann – wie viele Kunden würden dies als Bedrohung ihrer Privatsphäre ansehen?

Die bis dato prominenten technischen Herausforderungen der RFID-Technik – Zugriffskontrolle, Schutz vor Verfolgbarkeit und Abhörsicherheit – treten bei der freiwilligen Nutzung drahtloser Funketiketten mehr und mehr in den Hintergrund. Zwar wird es auch weiterhin wichtige und nötige Entwicklungen auf diesem Gebiet geben und geben müssen, gerade in Bezug auf die Fälschungs- und Auslesesicherheit offizieller Ausweise wie Reisepass oder Gesundheitskarte. Doch für den Grossteil der in Zukunft im Umlauf befindlichen Tags wird ein einfacher Abhörschutz und eine konsequente Reichweiten- und Datenbegrenzung genügen. „*Physics is our best friend*," wie RFID-Pionier Prof. Sanja Sarma vom MIT bemerkte [Sar06].

Gerade jenseits von Verschwörungstheorien und kriminellen Machenschaften werden legale, aber unachtsam und undifferenziert durchgeführte Datensammlungen wohl den grössten Effekt auf unsere zukünftige Privatsphäre haben werden. Auch wenn europäische Datenschützer nicht müde werden, auf die auch für RFID geltende Gesetzeslage hinzuweisen [DPP03], so bleibt eine wirkungsvolle Durchsetzung schwierig, wenn Betreiber von RFID-Systemen im öffentlichen Raum deren Verwendung nicht ausreichend dokumentieren müssen.

Die Frage wird also in Zukunft vielleicht gar nicht mehr lauten müssen „Werden wir noch eine Privatsphäre haben?“ sondern „Werden wir noch eine Privatsphäre haben wollen?“. Womöglich wird es sogar zu keiner der beiden Fragen kommen, da – richtig eingeführt – die RFID-Technik uns nicht als Einschränkung unserer Freiheit, sondern als ein Garant dafür vorkommen könnte. Mit Hilfe von getaggten Produkten, smarten Einkaufswagen, smarten Mobiltelefonen und smarten Umgebungen können wir leichter denn je an die richtige Information zum richtigen Zeitpunkt kommen (z.B. ein automatisches Allergie-Warnsystem beim Einkauf). Wir können leichter denn je von aktuellen Angeboten profitieren und unser Leben besser als vorher organisieren. Mit RFID versehene amtliche Ausweise mögen einen Hauch von George Orwell versprühen, doch scheinen sie vielen schon heute in Anbetracht der Gefahren (und einiger spektakulärer Fahndungserfolge) gerechtfertigt. Und ein staatlicher Paternalismus bedient sich smarter Produkte und intelligenter Autos, um die Zahl der Unfälle zu senken und ein durch RFID bereits effizienter gestaltetes Gesundheitssystem weiter zu entlasten.

Schöne neue Welt?

Literatur

[Ali06] Alioth M (2006) Briten wollen gefilmt werden, NZZ am Sonntag, 27.8.2006: 3

[Aut02] Auto-ID Center (2002) 860 MHz-960 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Recommended Standard, Version 1.0.0, www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

[Aut03] Auto-ID Center (2003) 860 MHz-935 MHz Class 0 Radio Frequency Identification Tag Protocol Specification Candidate Recommendation, Version 1.0.0, www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

[Ben03] Benetton (2003) No microchips present in garments on sale. Benetton Pressemitteilung, 4. April 2003, www.benetton.com/press/sito/_media/press_releases/rfiding.pdf

[BGS05] Berthold O, Günther O, Spiekermann S (2005) Verbraucherängste und Verbraucherschutz. Wirtschaftsinformatik, 47(6):1–9

[Bun05] Deutscher Bundestag (15. Wahlperiode) (2005) Antwort der Bundesregierung auf die Große Anfrage der Abgeordneten Gisela Piltz, Ernst Burgbacher, Rainer Funke, weiterer Abgeordneter und der Fraktion der FDP: Überprüfung der personengebundenen datenschutzrechtlichen Bestimmungen. Drucksache 15/4725. www.bundestag.de/ aktuell/hib/2005/2005_037/01.html

[CNN03] C|Net News.com (2003) Networking: Gillette shrugs off RFID-tracking fears. 14. August. news.com.com/2100-1039_3-5063990.html?tag=cd_mh

[Com03] ComputerWeekly.com (2003) Privacy concerns as Benetton adds "smart tags" to clothing line, 13. März 2004, www.computerweekly.com/Article120113.htm

[CST03] Chicago Sun-Times (2003) Lifestyle: Chipping away at your privacy, 9. November 2003, www.suntimes.com/output/lifestyles/cst-nws-spy09.html

[EET03] EETimes (2003) Semiconductors: Benetton backs off RFID deployment, 5. April 2003, www.eetimes.com/semi/news/OEG20030405S0001

[EPC04] EPCglobal (2004) EPC Tag Data Standards Version 1.1 Rev.1.24, April 2004,www.epcglobalinc.org/standards_technology/EPCTagDataSpecification11rev124.pdf

[EPI01] EPIC – Electronic Privacy Information Center (2001) Radio frequency identification (RFID) systems. The A to Z's of Privacy Website. www.epic.org/privacy/rfid/

[FGS05] Fabian B, Günter O, Spiekermann S (2005) Security analysis of the object name service for RFID. In: Proceedings of the 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing.

[Fin02] Finkenzeller K (2002) RFID-Handbuch. 3. Auflage. Hanser Fachbuchverlag.

[FSL04] Flörkemeier Ch, Schneider R, Langheinrich M (2004). Scanning with a purpose – supporting the fair information principles in RFID protocols. In 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan.

[GüS05] Günther O, Spiekermann S (2005) RFID And The Perception Of Control: The Consumers View. Communication of the ACM, 48(9):73-76

[Hos06] Hosein G (2006) Combating Criminality in a World of Ambient Technology. Conference on safeguards in a world of ambient intelligence (Vortrag), 21. März 2006. swami.jrc.es/pages/documents/SWAMIHosein20060321_000.pdf

[ISO00] ISO/IEC (2000) The ISO/IEC Standards Series 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards. Parts 1-4. See www.wg8.de/sd1.html

[Jäg05] Jäggi W (2005) Biometrie und RFID, brisante Mixtur im neuen Pass. Tagesanzeiger Online, 29. Juni 2005. tages-anzeiger.ch/dyn/leben/technik/537105.html

[JSB05] Juels A, Syverson P, Bailey D (2005) High-power proxies for enhancing RFID privacy and utility. Workshop on Privacy Enhancing Technologies (PET 2005)

[JRE05] JR-East (2005) Mobile Suica Service to Start Saturday, January 28, 2006. Pressemitteilung. www.jreast.co.jp/e/press/20051101/index.html

[Jue04] Juels A (2004) Minimalist cryptography for low-cost RFID tags. The Fourth International Conference on Security in Communication Networks (SCN 2004). Springer-Verlag, LNCS 3352

[Kan03] Kantor A (2003) Tiny transmitters give retailers, privacy advocates goosebumps. USAToday.com – CyberSpeak, 19. Dezember 2003.

[Küg05] Kügler D (2005) Risiko Reisepass. c't, 2005(5): 84–89

[Küp06] Küpper M (2006) Sicherheitsdebatte – Mehrheit wünscht sich Überwachungskameras. Spiegel Online, 18. August 2006, www.spiegel.de/politik/deutschland/0,1518,druck-432375,00.html

[Let06] Lettice J (2006) How to clone the copy-friendly biometric passport. The Register Online, 26. August 2006. http://www.theregister.co.uk/2006/08/04/cloning_epassports/

[Mat03] Mattern F (2003) Total vernetzt – Szenarien einer informatisierten Welt. Springer-Verlag

[ODo06] O'Donnel J (2006) Will all autos some day have breathalyzers? USA Today Online, 28. April 2006. www.usatoday.com/money/autos/2006-04-24-breathalyzer-usat_x.htm

[Ray02] Ray R (2002) Taking another look at digital postage. Smallbiztechnology.com Website, 14.8. 2002. www.smallbiztechnology.com/smallbizarticles/digitalpostagestatus.shtml

[Rob03] Roberti M (2003) Big brother's enemy. RFID Journal, Juli 2003. www.rfidjournal.com/article/articleview/509/1/1/

[Sar06] Sarma S (2006) Some issues related to RFID and Security. Vortrag am zweiten Workshop über RFID Security (RFIDSec'06), Graz, Österreich, Juli 2006. Folien verfügbar unter events.iaik.tugraz.at/RFIDSec06/Program/slides/001%20-%20Invited%20Talk%20-%20Sanjay%20Sarma.ppt

[SiW05] Simoncelli T, Wallace H (2005) Spiralling out of control. Index on Censorship 2005(3). www.eurozine.com/articles/2005-10-25-simoncelliwallace-en.html

[Sla04] Slashdot Diskussionsforum (2004) Fatal Flaw Weakens RFID Passports. Beitrag von *Cili(687222)* vom 4.11.2004. yro.slashdot.org/comments.pl?sid=167316&threshold=1&mode=thread&cid=13952118

[Spi06] Der Spiegel (2006) Panorama – Auf Nummer Sicher. Umfrage von TNS Infratest im Auftrag des Spiegel-Magazins, 2006(9): 20

[SpP05] Spiekermann S, Pallas F (2005) Technology Paternalism – Wider Implications of RFID and Sensor Networks. Poiesis & Praxis - International Journal of Ethics of Science and Technology Assessment 2005(4), Springer Verlag. edoc.hu-berlin.de/oa/articles/reFDoa9WpdlyU/PDF/27aIqGTe3Neo.pdf

[Sta03] Stapleton-Gray R (2003) Scanning the Horizon: A Skeptical View of RFIDs on the Shelves. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org/papers/stapleton-gray3.pdf

[SWE02] Sarma SE, Weis SA, Engels DW (2002) RFID Systems and Security and Privacy Implications. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), Redwood Shores, USA. Springer-Verlag, LNCS 2523

[Tec06] tecChannel.de (2006) Near Field Communication: Handy als Busfahrkarte. Meldung vom 24.4.2006, tecChannel.de Website. www.tecchannel.de/news/themen/telko/437329/

[Vog98] Vogel J (1998) When cards come collecting – How Safeway's new discount cards can be used against you. Seattle Weekly, September 24-30, 1998. www.seattleweekly.com/news/9838/features-vogel.php

[WSR+03] Weis SA, Sarma SE, Rivest RL, Engels DW (2003) Security and privacy aspects of low-cost radio frequency identification systems. In Security in Pervasive Computing: First International Conference. Springer LNCS Band 2802: 201–212. www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=2802

[Wik06a] Wikimedia Foundation (2006) James Bulger. Wikipedia: The Free Encyclopedia, 00:18, 29.8.2006 UTC. en.wikipedia.org/wiki/James_Bulger

[Wik06b] Wikimedia Foundation (2006) Triple DES. Wikipedia: The Free Encyclopedia. 12:15, 30.8.2006 UTC. en.wikipedia.org/wiki/Triple_DES

[Zei03] Zeidler M (2003) Markus Zeidler. RFID: Der Schnüffelchip im Joghurtbecher. Monitor-Magazin, 8. Januar 2003. www.wdr.de/tv/monitor/beitrag.phtml?bid=554&sid=108