Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie

Marc Langheinrich
Institut für Pervasive Computing, ETH Zürich

The risk RFID technology poses to humanity is on a par with nuclear weapons
Katherine Albrecht (2003)[1]

Kurzfassung. Mit der durch Ubiquitous Computing möglichen feinmaschigen Überwachung vielfältiger Phänomene können nicht nur betriebliche Abläufe, sondern potentiell auch die daran beteiligten Lieferanten, Mitarbeiter und natürlich auch Kunden in einer noch nie da gewesenen Qualität beobachtet werden. Zwar existieren bereits seit längerem technische Mittel und Verfahren, elektronische Informationen datenschutzkonform zu speichern und zu verarbeiten, doch ist ein direkter Einsatz dieser klassischen Technologien im Rahmen des Ubiquitous Computing aufgrund der deutlich veränderten Rahmenbedingungen oft nur begrenzt möglich. Selbst dedizierte Lösungen können im Spannungsfeld zwischen Effizienz und Bequemlichkeit auf der einen und Sicherheit und Datenschutz auf der anderen Seite in vielen Fällen den komplexen Herausforderungen smarter Umgebungen nicht gerecht werden. Der vorliegende Beitrag versucht, die komplexen Zusammenhänge im Bereich des Datenschutzes aufzuzeigen, die sich beim flächendeckenden Einsatz von Identifikationstechnologie ergeben. Insbesondere werden dabei neuere Datenschutzverfahren im Bereich der RFID-Technologie diskutiert und auf ihre Vor- und Nachteile hin untersucht.

1 Unter Beobachtung

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 –*

[1] Zitiert in [Dow03]

frei übersetzt etwa: Konsumenten gegen Datenschutzvergehen und Nummerierung in Supermärkten) im Internet zum weltweiten Boykott der global agierenden Konzerne aufgerufen.[2]

Dass die mit einfachsten Mitteln agierende Protestbewegung eine solch nachhaltige Wirkung hervorruft, lässt auf den Stellenwert schließen, den das Thema Datenschutz und Privatheit in der Öffentlichkeit erlangt hat. Inzwischen gibt es kaum noch Presseartikel oder Fernsehsendungen, welche über Ubiquitous Computing berichten, ohne nachdrücklich auf die möglicherweise weitreichenden 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[3] hatten bereits im März 2002 mehr als die Hälfte aller Deutschen mindestens eine Kundenkarte, in Großbritannien waren es 2003 sogar mehr als 86 % [Sha03]. Für einen Rabatt von oft weniger als ein 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 potentielle Fehlentwicklungen zu erkennen.

Der vorliegende Beitrag möchte dazu das oft nur diffus wahrgenommene Gebiet des Daten- und Persönlichkeitsschutzes zunächst in seiner Begrifflichkeit untersuchen, dessen gesellschaftliche Realitäten in Form historischer Entwicklung und aktueller Gesetzgebung beschreiben und schließlich die besonderen Herausforderungen des Ubiquitous Computing an unser Verständnis von Privatheit herausstellen. Anschließend sollen am Beispiel aktuell diskutierter technischer Datenschutzlösungen für RFID-Tags die Möglichkeiten, aber auch die Grenzen solcher Ansätze aufgezeigt und in einer abschließenden Diskussion bewertet werden.

[2] Siehe www.boycottbenetton.org

[3] Siehe www.tns-emnid.com

2 Zur Begründung des Datenschutzes

Trotz des engen Bezuges zum Internet ist der Aspekt des Schutzes der Privatsphäre und der persönlichen Daten kein neues Phänomen der Informationsgesellschaft. Debatten über die Privatsphäre haben eine lange Geschichte, über deren Zeitraum hinweg sich das Grundbedürfnis nach Privatheit in seiner Ausprägung wiederholt änderte. Bereits 1361 fand sich im englischen Recht der *Justices of the Peace Act*, der das Belauschen und heimliche Beobachten anderer unter Strafe stellte [Lau03]. 1763 folgte der berühmte Ausspruch William Pitts, seinerzeit Mitglied im englischen Parlament: *„The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail — its roof may shake — the wind may blow through it — the storm may enter — the rain may enter — but the King of England cannot enter! — all his forces dare not cross the threshold of the ruined tenement!"* [Bro39].

Eine der frühesten Definitionen von Privatheit stammt vom späteren Richter am Obersten Gerichtshof der USA, Louis Brandeis, und seinem Anwaltskollegen Samuel Warren. Bereits 1890 veröffentlichten die beiden den wegweisenden Aufsatz *The Right to Privacy* [WaB90], welcher im amerikanischen Recht die zivilrechtlichen Grundlagen für Klagen gegen die Verletzungen der Privatsphäre schaffte. Dass der Aufsatz auch heute noch eine hohe Relevanz besitzt, liegt dabei vor allem auch an den Umständen, unter denen sich Warren und Brandeis zu ihrer Publikation genötigt sahen: „*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right ‚to be let alone.' [...] Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"* Waren es damals die aufkommende Sensationspresse und die durch die Fortschritte in der Photographie möglichen „Paparazzi-Fotos",[4] die nach Meinung von Warren und Brandeis eine Anpassung des Rechts erforderten, sind es heute *Smart Labels*, *Memory Amplifier* und *Smart Dust*, welche es erforderlich machen, den Schutz der Privatsphäre sowohl technisch als auch rechtlich und sozial neu zu evaluieren.

Bei aller technikgeschichtlicher Relevanz scheint allerdings Warrens und Brandeis' Definition der Privatheit als *„the right to be left alone"* aufgrund der Vielzahl von Interaktionen im heutigen Informationszeitalter kaum praktikabel. Eine zeitgemäße Definition der *informationellen Privatheit* kommt von Alan Westin, der 1967 angesichts der zunehmenden Verbreitung von maschineller Informationsverarbeitung diese wie folgt definiert: *„Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others"* [Wes67].

Neben diesem auf Datenverarbeitungsanlagen abzielenden Aspekt unterscheidet man heute weiterhin die *Privatheit der Kommunikation* (z.B. Brief- und Fernmeldegeheimnis), die *territoriale Privatheit* (der Schutz der eigenen vier Wände,

[4] Am 18. Oktober 1884 erhielt Georg Eastmann, der Gründer der Eastman Kodak Company, Patent 306 594 für die Erfindung des photographischen Films. Statt mittels schwerer Glasplatten im Studio konnte dank Kodaks günstiger „Snap Camera" nun praktisch jedermann auch ohne Einwilligung des Subjektes einen „Schnappschuss" machen.

der sich in einem gewissen Rahmen auch auf das Auto oder den Arbeitsplatz erstreckt), sowie die *körperliche Privatheit*, also der Schutz vor ungerechtfertigten Leibesvisitationen bzw. körperlichen Untersuchungen (letztere beiden werden auch oft als *physische* oder *lokale Privatheit* zusammengefasst). Darüber hinaus geht es bei der sogenannten *dezisionalen Privatheit* um die *„Sicherung der Interpretationshoheit über das eigene Leben"*, wie Beate Rössler, Professorin für Philosophie an der Universität Amsterdam, beschreibt [Rös01], d.h. um die Freiheit, unbefangen selbst entscheiden zu können: *„mit wem will ich zusammenleben; welchen Beruf will ich ergreifen; aber auch: welche Kleidung trage ich"* [Rös02]. Privatheit also als Autonomie des Individuums; als die Fähigkeit, die Frage nach der Person, die man sein will zu stellen und zu beantworten und dann – im Privaten – auch tatsächlich nach den eigenen Wünschen zu leben.

2.1 Moderne Datenschutzgesetze

Mehr als hundert Jahre nachdem Brandeis und Warren den Grundstein für das moderne Datenschutzrecht legten, haben sich zwei grundlegende Herangehensweisen zum Schutz der Privatsphäre etabliert: der vor allem in Europa populäre Ansatz umfassender, sektorenübergreifender Datenschutzgesetze und der in den USA favorisierte Mix aus spezifischen Gesetzen und freiwilliger Selbstbeschränkung von Industrie und Handel. Die Anfang der 1990er Jahre mit der steigenden Popularität des grenzüberschreitenden Internets oft vorausgesagte Entwertung nationaler Gesetzgebung fand allerdings nicht statt – vielmehr erfuhr dieser Bereich im ausklingenden zwanzigsten Jahrhundert eine stark zunehmende Dynamik, indem viele Staaten ihre existierenden Gesetze sowohl an aktuelle technische Entwicklungen anpassten als auch im internationalen Vergleich aktualisierten und harmonisierten.

Während bis heute in den USA keine umfassende Gesetzgebung zum Datenschutz existiert, die Staat und Privatpersonen gleichermassen betrifft und man es statt dessen der Industrie überlässt, durch freiwillige Selbstbeschränkung die Privatsphäre zu wahren, begann man auf der anderen Seite des Atlantiks schon früh damit, nationale Gesetzgebungen nicht nur auf alle Formen der Datensammlungen – sowohl staatlicher als auch privater Natur – anzuwenden, sondern darüber hinaus auch europaweit zu harmonisieren. Bereits 1973 und 1974 erließ der Europarat[5] mit den Resolutionen (73)22 und (74)29 zwei Richtlinien für die nationale Gesetzgebung betreffend private bzw. öffentliche Datenbanken. Im Jahr 1985 folgte mit der Konvention 108/81, dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten", ein normatives Vertragswerk zur Harmonisierung nationaler Datenschutzgesetze [COE04]. Mit der 1995 verabschiedeten Europäischen Datenschutz-Direktive 95/46/EC (im Folgenden „Direktive" genannt) schaffte man schließlich ein auch über die Gren-

[5] Der Europarat ist eine seit 1949 bestehende zwischenstaatliche Organisation zur europaweiten Harmonisierung der rechtlichen und sozialen Praktiken. Ihm gehören neben den 25 Ländern der Europäischen Union 20 weitere Länder an (siehe www.coe.int).

zen Europas hinaus wirkendes internationales Werkzeug zum Schutz der Privatsphäre.

Die Direktive hat dabei zwei Kernpunkte. Zum einen verpflichtet sie die Mitgliedsstaaten der Union, innerhalb einer dreijährigen Frist eine zur Direktive kompatible, nationale Gesetzgebung zu erlassen.[6] Diese europaweite Angleichung erlaubt einen ungehinderten Informationsfluss zwischen den Mitgliedsstaaten, da die personenbezogenen Daten europäischer Bürger überall den gleichen, von der Direktive vorgeschriebenen Mindestschutz genießen. Auf der anderen Seite verbietet die Direktive explizit den Transfer personenbezogener Informationen in „nicht sichere Drittländer", d.h. Länder, deren Datenschutzgesetze nicht den gleichen Schutz bieten, wie von der Direktive vorgeschrieben. Nachdem Politiker zu verstehen gaben, dass sie durchaus Willens waren, die europäischen Vertretungen nicht-europäischer Konzerne auf die Einhaltung dieser Richtlinie zu verklagen, sollten diese die persönliche Daten von EU-Bürgern (z.B. Kundendaten, aber auch die Lohn- und Gehaltslisten der Angestellten) an die jeweiligen Konzernzentralen in Drittländer ohne ausreichende Datenschutzgesetze exportieren, begannen zahlreiche Staaten umgehend mit der Anpassung ihrer Gesetzgebung, um von der EU-Kommission als „sicheres Drittland" bewertet zu werden und dadurch Teil des europäischen Informationsbinnenmarkts zu bleiben.[7]

2.2 Fair Information Practices und informationelle Selbstbestimmung

Die von der Direktive geforderten Mindeststandards bei Datenerhebung und Datenverarbeitung sind eine konsequente Weiterentwicklung der bereits 1973 in einem Bericht des *United States Department for Health Education and Welfare (HEW)* aufgestellten *Fair Information Practices*, die Anfang der 1980er Jahre von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) in ihrer „Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten" [OEC80] aufgegriffen und als acht Grundprinzipien formuliert wurden:[8]

1. Beschränkung der Datenbeschaffung (*collection limitation*): Daten sollten in rechtmäßiger Weise und wenn immer möglich mit der Einwilligung des Datensubjekts erhoben werden.
2. Qualität der Daten (*data quality*): Die erhobenen Daten sollten dem Zwecke ihrer Erhebung angemessen, korrekt, vollständig und aktuell sein.

---

[6] Inzwischen haben alle ursprünglichen 15 Mitgliedsländer die Direktive umgesetzt.

[7] Im März 2004 waren Argentinien, die Britischen Kanalinseln, Kanada, die Schweiz und Ungarn als sichere Drittländer im Sinne der Direktive von der EU-Kommission zertifiziert (siehe europa.eu.int/comm/internal_market/privacy/adequacy_en.htm). Ein separates Abkommen, das *Safe Harbor Agreement*, regelt den Datenaustausch mit den USA [SoR03] (siehe www.export.gov/safeharbor/sh_overview.html).

[8] Ein guter Überblick zur Geschichte der *Fair Information Practices* und deren Einfluss auf heutige Gesetze findet sich in [PRC04].

3. Zweckbestimmung (*purpose specification*): Der Zweck der Datenerhebung sollte vorher festgelegt werden.
4. Limitierte Nutzung (*use limitation*): Zu einem bestimmten Zweck gesammelte Daten sollten nicht für andere Zwecke genutzt werden.
5. Sicherheit der Daten (*security*): Die gesammelten Daten sollten adäquat vor Verlust, Diebstahl oder unerlaubten Änderungen geschützt werden.
6. Transparenz (*openness*): Die Methoden der Datenverarbeitung sollten offen gelegt werden.
7. Beteiligung (*individual participation*): Dem Einzelnen sollte ein gebührenfreies Auskunftsrecht, sowie die Richtigstellung und Löschung seiner Daten zustehen.
8. Verantwortbarkeit (*accountability*): Die für die Datenverarbeitung Verantwortlichen sollten für Verstöße zur Rechenschaft gezogen werden können.

Insgesamt lassen sich die *Fair Information Practices* in fünf Grundsätzen zusammenfassen: Offenheit, Datenzugriff und -kontrolle, Datensicherheit, Datensparsamkeit und individuelle Einwilligung [Cus03]. Gerade letzterer Punkt gewann dabei im Laufe der Zeit immer mehr an Bedeutung: Zwar forderten bereits die eher technisch orientierten Datenschutzgesetze der 1970er Jahre die Möglichkeit des Einzelnen zur Korrektur personenbezogener Daten, doch geschah dies eher aus der Motivation heraus, die Richtigkeit der gespeicherten Daten zu gewährleisten, als die Datenerhebung selbst in Frage zu stellen. Erst in der als Volkszählungsurteil in die Geschichte eingegangenen Entscheidung des Bundesverfassungsgerichts wurde 1983 das bis dahin geltende Persönlichkeitsrecht um die „informationelle Selbstbestimmung" ergänzt [May98].[9] In der Urteilsbegründung hieß es dazu: *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, [...] kann in seiner Freiheit, aus eigener Selbstbestimmung zu planen und zu entscheiden, wesentlich gehemmt werden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der der Bürger nicht mehr wissen könnte, wer was, wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."*

Das Konzept der informationellen Selbstbestimmung[10] stellt einen bedeutenden Schritt moderner Datenschutzgesetzgebung hin zum autonomen Individuum dar. Zum einen erweitert es die *Fair Information Practices* um einen partizipativen

[9] Auslöser war die Kontroverse um die am 27. April 1983 geplante Volkszählung, von der Bundesregierung als „Totalzählung" angekündigt, die in über hundert Verfassungsbeschwerden resultierte [Rei01].

[10] Im Englischen als *self-determination over personal data*, oder kurz aber etwas unglücklich als *data self-determination*, übersetzt.

Ansatz, der über ein „Take it or leave it“ hinaus dem Einzelnen erlauben soll, ohne Angst vor gesellschaftlichen Nachteilen über die Verwendung seiner persönlichen Daten entscheiden zu können. Zum anderen stellt es den Schutz der Privatheit nicht mehr nur als Individualrecht dar, sondern betont die positive gesellschaftliche Komponente des Datenschutzes. Privatheit also nicht als Laune des Einzelnen, sondern als Pflicht einer demokratischen Gesellschaft, wie Julie Cohen bemerkt: *„Prevailing market-based approaches to data privacy policy […] treat preferences for informational privacy as a matter of individual taste, entitled to no more (and often much less) weight than preferences for black shoes over brown or red wine over white. But the values of informational privacy are far more fundamental. A degree of freedom from scrutiny and categorization by others promotes important noninstrumental values, and serves vital individual and collective ends“* [Coh00].

3 Datenschutzprobleme allgegenwärtiger Computer

Datenschutz war schon immer bezogen und ausgerichtet auf das technisch Machbare. War es das Aufkommen der individuellen Fotographie gegen Ende des 19. Jahrhunderts, die Warren und Brandeis beunruhigten, die Verbreitung von Telegraph und Telefon zu Beginn des 20. Jahrhunderts, die die Ausdehnung territorialer Privatrechte auf den Schutz unserer Kommunikation mit sich brachte, oder die staatliche Nutzung elektronischer Datenverarbeitungssysteme in den 1960er Jahren, die die modernen Datenschutzgesetze mit ihrem Fokus auf die informationelle Privatheit prägten: Technik veränderte manches, was im Alltag möglich war, und stieß so schließlich auch eine Neuausrichtung unserer Vorstellung von Privatheit an. Nachdem die Kommerzialisierung des Internets Mitte der 1990er Jahre die vorläufig letzte Welle von Gesetzesänderungen ausgelöst hatte, steht nun bereits die nächste technische Revolution bevor: die der smarten Alltagsgegenstände und allgegenwärtigen Computer.

Zwar klingt beim unbedarften Beobachter auch immer ein Aspekt von Science-Fiction mit an, wenn von „intelligenten Autos“ und „smarten Eigenheimen“ die Rede ist, vom alten Traum dienstbarer Maschinen, die mit Intelligenz versehen uns klaglos unsere Arbeit abnehmen. Doch geht es beim Ubiquitous Computing vordergründig eigentlich um etwas Banaleres, wenn auch nicht notwendigerweise weniger Nützliches: der Überwindung von Medienbrüchen [FMB03]. Mit Miniatursensoren, billigen Mikrochips und drahtloser Kommunikation lässt sich die Welt des Computers in bisher ungeahnter Weise in unseren Alltag hinein verlängern. Dies funktioniert in gewisser Weise auch in die andere Richtung, unser Alltag lässt sich ebenso in weitaus verlässlicherer (und effizienterer) Weise im Computer abbilden. Die Grenze zwischen dem Realen und dem Virtuellen scheint zu verschwinden – ein Abbild der realen Welt lässt sich immer genauer und einfacher im Computer nachspielen und damit auch vom Computer aus manipulieren.

Das Problem des Datenschutzes liegt also genau in dieser Abbildung – in der Übersetzung von Fakten der realen Welt in Informationsstückchen, in der Digitalisierung unseres Lebens zum Zwecke der automatisierten Verarbeitung. Es überrascht daher nicht, wenn Ubiquitous Computing zumindest prinzipiell die heutige

Realität des Datenschutzes in hohem Maße zu verändern vermag. Im Folgenden sollen diese Veränderungen der Datenschutzproblematik kurz erläutert und deren Implikationen anhand von Beispielen illustriert werden. Weiterhin sollen die existierenden Prinzipien für Datenschutz – die *Fair Information Practices* – im Lichte dieser technischen Entwicklung untersucht und kommentiert werden.

3.1 Eine neue Qualität der Datenerhebung

Das bewusste Beobachten der Handlungen und Gewohnheiten von Mitmenschen ist wohl so alt wie die Menschheit selbst. Während diese Art der Beobachtung in der „guten alten Zeit" noch von unseren engsten Nachbarn durchgeführt wurde, begannen mit dem Einsetzen der automatisierten Datenverarbeitung nun Maschinen diese Rolle zu übernehmen, allerdings mit einem wichtigen Unterschied: Nicht mehr nur die Abweichungen vom Alltäglichen wurden erfasst, sondern vielmehr das Alltägliche selbst wurde Gegenstand der Beobachtung.

Ubiquitous Computing erlaubt es, diese Art der Alltagsüberwachung weit über die heute mögliche automatisierte Informationsgewinnung aus Kreditkartentransaktionen, Telefonverbindungen und Internet-Nutzung hinaus auszudehnen. Dieser Qualitätssprung lässt sich anhand von fünf Aspekten beschreiben:

- *Ausdehnung.* Nicht nur die räumliche Abdeckung von Beobachtungsaktivitäten wird durch Ubiquitous Computing erweitert, sondern auch ihre zeitliche Abdeckung nimmt viel größere Ausmaße an. Angefangen von vorgeburtlichen Diagnosen, die auf der Krankenkassen-Chipkarte des Babys gespeichert werden, über Aktivitätsmuster aus Kindergärten und Schulen, bis hin zur Arbeitsplatzüberwachung und Gesundheitskontrollen in Altersheimen. Und während heute der PC Zuhause durch Betätigung des Ausschalters wirkungsvoll an der Datenerhebung gehindert wird, so wird es in der Vision der nahtlosen und unbemerkten Interaktion mit unsichtbaren Computern diesen Ausschalter kaum mehr geben – eine bewusste Begrenzung der Erhebung ist also kaum mehr möglich.
- *Art der Datenerhebung.* Auch wenn wir heute oftmals die Momente, in denen wir Daten über uns preisgeben, gar nicht mehr bewusst wahrnehmen, so lassen sie sich zumindest im Nachhinein meist noch rekonstruieren: Der Kreditkartenantrag enthielt Informationen über mein Einkommen, im Teilnahmefomular für das Gewinnspiel habe ich meine vier Lieblingsfilme angegeben und beim Kurzurlaub letztes Wochenende konnte meine Bank sehen, wo ich am liebsten einkaufe. Doch diese ausgezeichneten Momente der Datenerhebung verschwinden in gleichem Maße, wie die Computer selbst verschwinden und allgegenwärtig werden: Scannt eine „smarte Tasse" unbemerkt meinen Fingerabdruck, während ich aus ihr trinke? Hat diese Fußmatte einen RFID-Leser, der meine Schuhe registrieren kann? Selbst wenn man sich solcherlei Datensammlungen entziehen möchte, wird dies in Zukunft aufgrund des mangelnden Bewusstseins über die Momente dieser Erhebungen kaum noch möglich sein.
- *Datentypen.* Seit es automatisierte Datenverarbeitung gibt, haben sich die erhobenen Datensätze kaum verändert: Name, Adresse, Alter, Kaufverhalten, etc. Mit Ubiquitous Computing eröffnet sich hingegen eine völlig neue Art der

„Echtzeit"-Daten – unser momentaner Aufenthaltsort, unser Gesundheitszustand, oder unsere tatsächlichen (im Gegensatz zu den von uns vorgegebenen) Vorlieben – die niemals zuvor in solch detaillierter Form ermittelbar waren. Diese umfassende Katalogisierung unserer Person könnte letztendlich unseren Beobachtern vielleicht sogar einen tieferen Einblick in unseren Charakter geben, als es uns selbst möglich ist.

- *Erhebungsgrund.* Auch der von vielen Datenschutzgesetzen vorgeschriebene klare Erhebungsgrund, also z.B. das Übermitteln meiner Adresse zwecks Zusendung eines Paketes, wird beim Ubiquitous Computing oft nur noch schwer einzugrenzen sein. Statt künstlicher Intelligenz setzt man auf eine möglichst exakte Erfassung des aktuellen Kontexts, um auch ohne echtes Verständnis der Situation eine „smarte" Reaktion zu erhalten. Oder man versucht durch hohe Redundanz, auch in der Datenerhebung, technische Unzuverlässigkeiten, z.B. beim Lesen von RFID-Tags, auszugleichen. Dieser Selbstzweck bei der Datenerhebung – das Sammeln von möglichst vielen Informationen, da später potentiell alles relevant sein kann – erschwert nicht nur die gesetzlich geforderte Zweckbindung, sondern erhöht gleichzeitig auch den Sammeleifer: selbst scheinbar banale Informationen können durch Computeranalyse mit relevanten Fakten korreliert werden.
- *Datenzugriff.* Schließlich dürfte die Interkonnektivität zwischen vielen smarten Gegenständen ein kaum mehr zu überblickendes Datennetz schaffen, dessen Datenströme mit traditionellen Zugriffkontrollen nicht mehr zu verwalten sind: *„Everything will be connected to everything else"* [Luc99].

3.2 Herausforderungen an den Datenschutz

Wie kann nun diesem durch den Einsatz von Ubiquitous Computing begründeten Trend hin zu einer umfassenden Alltagsüberwachung entgegen gewirkt werden? Einen Bauplan für die datenschutzkonforme Behandlung persönlicher Informationen liefern die oben erwähnten *Fair Information Practices*, deren praktische Umsetzung jedoch im Rahmen dieser neuen Technologie entsprechend angepasst werden muss. Zu beachten sind in jedem Fall die Grenzen eines solchen Ansatzes: selbst eine hundertprozentige Einhaltung der Prinzipien kann keineswegs *garantieren*, dass einmal gesammelte Daten auch wirklich gemäß diesen Praktiken zum Einsatz kommen. Vielmehr etablieren sie eine Messlatte, einen Mindeststandard, dessen Einhaltung natürlich überprüft werden sollte – sei es durch staatliche oder unabhängige Organe, oder auch durch den Nutzer selbst. Wichtig ist allerdings, dass adäquate technische Mittel für solch eine Überprüfung zur Verfügung stehen. Ohne diese bleibt ein effektiver Datenschutz illusorisch, mit diesen wäre aber langfristig vielleicht sogar eine nachhaltige Verbesserung heutiger Bedingungen denkbar.

So wird beispielsweise das Prinzip der Offenheit in heutigen Datensammlungen entweder implizit durch die aktive Teilnahme des Datensubjektes (z.B. durch das Ausfüllen von Formularen) oder explizit durch eine Beschilderung (z.B. bei der Kameraüberwachung im Supermarkt) erreicht. In einer Welt voller ubiquitärer Dienste, in der die Interaktion mit dem Computer so weit in den Hintergrund tre-

ten soll, dass man sie gar nicht mehr bemerkt, tritt aber auch eine etwaige Datensammlung in den Hintergrund – die aktive Teilnahme des Einzelnen wird durch die unbemerkte Nutzung computerisierter Services also nicht nur vereinfacht, sondern vielleicht sogar unmöglich gemacht. Diesem Verschwinden von Bewusstmachung lässt sich grundsätzlich auf zwei verschiedene Arten begegnen. Eine Möglichkeit ist, den Selbstschutz des Einzelnen zu verbessern, d.h. sowohl die Erkennung als auch die Verhinderung solcher andernfalls unmerklichen Datensammlungen zu erleichtern. Auf der anderen Seite sind aber auch Mechanismen zur expliziten Ankündigung solcher Datensammlungen nützlich, die es dem Dienstanbieter erleichtern, die Tatsache der Erhebung sowie deren Parameter (d.h. welche Daten zu welchem Zweck erhoben werden) dem Einzelnen im voraus zu melden. Letzterer Ansatz hat nicht nur den Vorteil, dass Vertrauen zwischen Kunden und Anbietern geschaffen werden kann, sondern erleichtert darüber hinaus auch die Überprüfung der so öffentlich gemachten Versprechungen hinsichtlich der Nutzung der gesammelten Daten. Ein ubiquitäres Ankündigungssystem muss dabei notwendigerweise über die bisher üblichen visuellen Methoden hinaus angeboten werden, da potentiell jeder beliebige Gegenstand infolge seiner Benutzung Daten sammeln kann. Im Gegenzug kann eine technisch aufwendigere Ankündigung aber auch weitaus mehr Möglichkeiten bieten als etwa traditionelle Mechanismen in Bild und Schrift. So könnte eine drahtlos empfangbare, maschinenlesbare Ankündigung nicht nur detailliertere Informationen enthalten, sondern auch automatisch bzw. halbautomatisch aufgrund vorher spezifizierter Präferenzen des Nutzers verarbeitet werden, um so die Datensammlung im Rahmen des Möglichen anzupassen oder zumindest zu protokollieren.

Die Maschinenlesbarkeit ist vor allem deshalb wichtig, um die Überbeanspruchung der Nutzer so weit als möglich zu vermeiden: Statt im Sekundentakt vom Benutzer eine Entscheidung bezüglich einer möglichen Datensammlung zu verlangen, trifft ein automatisches System einen Großteil der Entscheidungen selber und fragt nur vereinzelt nach. Noch ist allerdings offen, ob sich persönliche Datenschutz-Präferenzen überhaupt so leicht im Voraus spezifizieren lassen. Zum einen scheint die Bandbreite an möglichen Interaktionen so groß, dass weder eine kompakte noch eine erschöpfende Beschreibung aller möglichen Dienste machbar scheint. Eine effektive Vorauswahl akzeptabler Erhebungssituationen durch den Nutzer scheint deshalb kaum praktikabel: zu oft würde eine unberücksichtigte Ausnahme ein direktes Nachfragen nötig machen. Darüber hinaus ist fraglich, ob Theorie und Praxis persönlicher Datenschutzpräferenzen überhaupt deckungsgleich sind. Man mag beispielsweise generell etwas gegen die Verwendung seiner persönlichen Daten zu Marketingzwecken haben, doch angesichts eines finanziellen Anreizes in der Praxis dann sehr wohl bereit sein, einmal eine Ausnahme zu machen. Sollten theoretische Prinzipien und tatsächliches Handeln weit auseinander liegen, so würde ein automatisches System in vielen Fällen die falsche Wahl treffen und damit kaum vom Nutzer verwendet werden.

Solcherlei Wahlmöglichkeiten bilden die Grundlage für das zweite Prinzip der *Fair Information Practices*: das der individuellen Einwilligung. Auch hier schafft die implizite Interaktion in ubiquitären Umgebungen neue Probleme. Zwar gibt es genügend rechtlich bzw. ethisch vertretbare Situationen, in denen eine Datensammlung auch ohne die Einwilligung des Datensubjektes erfolgen kann (z.B. bei der Videoüberwachung in Supermärkten), doch sollte im Allgemeinen die Preis-

gabe persönlicher Daten eine bewusste Entscheidung des Einzelnen sein. Traditionell gilt deshalb erst die persönliche Unterschrift als Einwilligung, z.B. beim Beantragen einer Supermarkt-Kundenkarte durch das Ausfüllen und Unterschreiben des Antragsformulars. Zwar gibt es das Pendant in Form digitaler Signaturen, die für elektronische Interaktionen eine rechtsverbindliche Einwilligung bezeugen können, doch geht es bei einer ubiquitären Umgebung vielmehr um die Frage, wie solch eine Signatur als Willenserklärung vom Nutzer initiiert werden kann: Angesichts der potentiell riesigen Zahl von impliziten (Mini-)Interaktionen und der ebenso großen Bandbreite an Nutzerschnittstellen scheint es impraktikabel, bekannte Verfahren wie beispielsweise einen Bestätigungs-Knopf allgemein einsetzen zu wollen.

Am wünschenswertesten sind sicherlich solche Art Dienste, die keinerlei persönliche Daten von Nutzern benötigen, bzw. diese in einer nicht identifizierbaren Form verwenden. Solange nämlich nur anonyme Daten zum Einsatz kommen, sind praktisch keine der oben beschriebenen Datenschutzpraktiken relevant – weder muss um die individuelle Einwilligung gebeten werden, noch müssen etwa Sicherheitsaspekte oder Zugriffsrechte bedacht werden. Mit Hilfe von Pseudonymen können darüber hinaus personalisierte Dienstleistungen angeboten werden, ohne die wahre Identität des Nutzers kennen zu müssen. Zwar sind Anonymisierungsverfahren und Pseudonyme bereits seit längerer Zeit im Internet weit verbreitet, doch lassen sich die dabei verwendeten Techniken nur schwer ins Ubiquitous Computing übertragen. Dies liegt vor allem daran, dass ubiquitäre Datenerhebungen oftmals unmittelbarer Natur sind: Eine Kamera, ein Mikrofon oder auch ein Indoor-Lokalisationssystem nehmen anders als ein Webformular den Benutzer direkt wahr und können nicht etwa durch Verwendung eines Anonymisierungsdienstes wie anonymizer.com ohne Offenlegung der Identität des Benutzers verwendet werden. Indirekte Sensoren wie beispielsweise druckempfindliche Bodenplatten können auch ohne die direkte Wahrnehmung primärer biometrischer Attribute durch Data-Mining-Techniken Menschen an ihrem Gang identifizieren. Und die beim Ubiquitous Computing typische enge Verknüpfung der Sensorinformationen mit Ereignissen der realen Welt erlaubt selbst bei der konsequenten Verwendung von Pseudonymen eine einfache Personenidentifikation: So konnten z.B. Forscher durch Zurückverfolgung der pseudonymisierten Bewegungsdaten eines Indoor-Lokalisiationssystemes alle Benutzer des Systems anhand ihres bevorzugten Aufenthaltsortes (typischerweise das Büro des Mitarbeiters) einwandfrei identifizieren [BeS03].

Auch die Sicherheitsanforderungen an ubiquitäre Systeme gestalten sich weitaus schwieriger als bei heutigen Client-Server-Systemen, bei denen alle Nutzer im voraus bekannt sind und eine feste Benutzerschnittstelle existiert (typischerweise Tastatur und Bildschirm oder ein fest installierter Kartenleser), über die die Anmeldung explizit erfolgt. Die für das Ubiquitous Computing typische große Bandbreite an technischen Geräten bedingt eine individualisierte Sicherheitslösung in Abhängigkeit von den jeweiligen Geräteresourcen (z.B. Rechenleistung, Speicher, Batterieleistung), der Art der zu übertragenden bzw. zu speichernden Daten sowie der jeweiligen Nutzungssituation. Gerade letzterem Punkt kommt aufgrund der engen Verknüpfung des Ubiquitous Computing mit unserem täglichen Leben eine große Bedeutung zu. Peter Cochran, ehemaliger Leiter der Forschungsabteilung von British Telecom, fasst dies pointiert so zusammen: *„Do I mind anyone acces-*

sing my medical or employment records, CV, and other personal details? Frankly, I don't give a fig! [...] Should I be knocked unconscious in a road traffic accident in New York – please let the ambulance have my medical record. Please let them know that I am going deaf and that I am diabetic. I really don't want it to be a secret – I want to live!" [Coc01].

Der in den *Fair Information Practices* geforderte Datenzugriff durch den Benutzer wird in Datensammlungen ubiquitären Charakters weitaus komplexer werden, da statt einem einfachen Datensatz (z.B. einer Postadresse) dem Benutzer ein komplexes Sensorendestillat präsentiert werden müsste, das darüber hinaus in den meisten Fällen eher eine Vermutung als eine Tatsache darstellt. Wann genau sich solch vage Informationsgefüge in verwertbare bzw. disputierbare Fakten verwandeln, die damit wieder den gesetzlichen Bestimmungen zur Datenkontrolle durch den Benutzer unterliegen, wird sich wohl erst nach einigen Jahren der Erfahrung mit dieser Art von Datensammlungen feststellen lassen. Bereits jetzt abzusehen ist allerdings, dass die umfangreichen Sensorerhebungen den in Europa so wichtigen Grundsatz der Datensparsamkeit erheblich strapazieren werden: Um möglichst kontextbezogen reagieren zu können, werden zukünftige Dienstleistungen auf immer weniger Daten verzichten wollen, auch wenn deren Relevanz auf den ersten Blick nicht gegeben ist. Eine Erhebungsgrundlage „auf Verdacht" ist in unserem heutigen Verständnis von Datenschutz aber nicht vorgesehen – inwiefern man in Zukunft, nach einigen praktischen Erfahrungen mit solchen Diensten, diesen Grundsatz revidieren werden muss, bleibt abzuwarten.

Festzustellen ist in jedem Fall schon heute, dass die Techniken des Ubiquitous Computing und entsprechende Einsatzszenarios uns zwingen werden, die technische Entwicklung derart voran zu treiben, dass die in den *Fair Information Practices* enthaltenen Grundsätze datenschutzgerechter Informationsverarbeitung soweit wie möglich umsetzbar bleiben. Gleichzeitig wird auch ein Umdenken über die Umsetzbarkeit dieser Prinzipien nötig werden, damit diese nicht von der technischen Realität zur Bedeutungslosigkeit degradiert werden. Einen ersten Einblick von diesem Wechselspiel zwischen technisch Machbarem und gesellschaftlich Wünschenswertem bietet die in den letzten Jahren stark vorangetriebene Integration von RFID-Technologie in den Warenfluss des Einzelhandels. Zwar existieren solche Systeme bereits seit mehreren Jahren in der industriellen Produktion,[11] doch durch das Einbeziehen des Kunden in diesen Kreislauf werden aus den RFID-Leservorgängen potentiell personenbezogene Daten. Der von Welthandelskonzernen wie Metro oder Wal-Mart im internationalen Maßstab geplante Einsatz solcher Systeme kann so einen ersten Vorgeschmack auf die neue Realität des Ubiquitous Computing liefern.

4 RFID und Datenschutz

RFID-Tags stellen aufgrund ihrer Identifikationsmerkmale zumindest prinzipiell ein signifikantes Datenschutzproblem dar. Von Befürwortern in dieser Hinsicht

[11] In Nischenmärkten kommen bereits heute Endverbraucher mit RFID-Tags in Kontakt, z.B. bei Skipässen, Straßenmautsystemen oder auch bei Wegfahrsperren im Auto.

gerne mit dem eher harmlosen Barcode verglichen,[12] erlauben sie nämlich im Unterschied zu diesem nicht nur eine weitaus detailliertere Identifikation[13] (d.h. Seriennummern statt generische Produktbezeichnung) sondern auch das unbemerkte Auslesen dieser Information, da die Leseeinheiten keine Sichtverbindung zum Tag benötigen. Eine technische Datenschutzlösung im RFID-Bereich muss also notwendigerweise das unbemerkte (bzw. nicht autorisierte) Auslesen der Tags verhindern, bzw. die individuellen Seriennummern durch generischere Informationen (z.B. Hersteller-ID statt Seriennummer) ersetzen. Aufgrund der zu erwartenden hohen Verbreitung der Tags stellt allerdings Letzteres nur bedingt eine Lösung dar: Selbst wenn RFID-Tags lediglich genauso viel Informationen bereitstellen würden wie heutige Barcodes, so wären dennoch durch die individuelle Kombination der Tags, sogenannten *„Constellations"* [Wei03], Personen oft eindeutig identifizierbar.

Existierende bzw. momentan diskutierte technische Lösungen im Bereich von „RFID-Datenschutz" lassen sich in zwei Ansätze unterteilen: Anonymisierung und Pseudonymisierung. Dies lässt sich entweder durch explizites Ändern der auf dem Tag gespeicherten ID erreichen (bzw. deren Löschung), durch eine explizite Zugriffskontrolle am Tag (d.h. dem Unterbinden nicht autorisierter Lesezugriffe) oder – im begrenzten Maße – auch durch das Sichern der Kommunikation auf dem sogenannten *„forward channel"*, d.h. der Kommunikation vom Leser zum Tag.[14]

4.1 „Anonymisierung" mittels Kill-Befehl

Bereits vor der durch den Benetton-Vorfall ausgelösten öffentlichen Kontroverse um RFID-Tags enthielt die 2002 publizierte Auto-ID-Spezifikation[15] [Aut02] einen sogenannten „Kill"-Befehl. Die zugrundeliegende 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/Auto-ID-Standard schreibt zwecks Deaktivierung für alle konformen Tags einen Kill-Befehl vor, der jedoch zur Ausführung ein wäh-

[12] Bei der Einführung des Barcodes in den 1970er Jahren war dieser allerdings als alles andere als harmlos angesehen, sondern wurde aufgrund seines Aufbaus wiederholt als biblisches Zeichen aus der Offenbarung und damit als Teufelszeug verdammt [Rel81].

[13] Zwar können auch Barcodes beliebig detaillierte Informationen speichern, doch benötigen sie dazu mehr Platz und sind beispielsweise durch Schmutz auf dem Code anfälliger für Lesefehler.

[14] Da das Signal des Lesegerätes nicht nur Informationen zum Tag sendet, sondern auch für die Energieversorgung der RFID-Chips nötig ist, hat es typischerweise eine bis zu zehn Mal größere Reichweite als das Antwortsignal vom Tag zum Leser.

[15] Ende 2003 wurde die Arbeit des Auto-ID Centers vom EPCglobal-Konsortium übernommen.

rend oder kurz nach der Produktion auf dem Tag gespeichertes 24-Bit-Passwort erfordert, um unautorisiertes „Einschläfern“ eines Tags (z.B. im Regal) zu erschweren.[16] Erhält ein Tag das korrekte Passwort zusammen mit dem Kill-Befehl, darf es danach laut Spezifikation in keiner Weise mehr auf Signale eines Leser reagieren [Aut03]. Wie diese Funktionalität konkret auf dem Tag implementiert wird, bleibt dem Hersteller überlassen; aus Gründen der Kosteneffizienz wird es sich allerdings in den meisten Fällen um eine softwaretechnische Lösung handeln, die dadurch – zumindest theoretisch – ein späteres Reaktivieren eines Tags durch direkten Kontakt (also durch Umgehen der dann deaktivierten Funkschnittstelle) erlauben würde.

Neben dieser unvollständigen Zerstörung des Tags gibt es zwei weitere Aspekte, die die Effektivität dieses Verfahren aus Sicht des Datenschutzes signifikant einschränken. Zum einen ist bei einer Deaktivierung an der Ladenkasse noch immer die Überwachung (*tracking*) innerhalb des Geschäftes möglich, ebenso wie eine direkte Assoziation von Kundendaten und Einkäufen spätestens an der Kasse (z.B. beim Vorlegen einer Kredit- oder Kundenkarte während des Bezahlvorgangs). Zum anderen ist der Vorgang der Deaktivierung selbst problematisch, da der Kunde nur schwerlich überprüfen kann, ob das Tag auch wirklich deaktiviert wurde. Auch der Umstand, dass alle bekannten Verfahren bisher eine softwaretechnische Deaktivierung vorsehen, obwohl eine elektromagnetische Deaktivierung analog zu heutigen Transponder-basierten Diebstahlsicherungen durchaus denkbar wäre,[17] lässt Zweifler vermuten, dass eine spätere (und für den Kunden unbemerkte) Reaktivierung der Tags möglich ist – eine Befürchtung, die bereits bei einer genauerer Untersuchung existierender Prototypen bestätigt wurde: So stellte sich beim Besuch des Metro Future-Stores durch die „RFID-Aktivistin“ Catherine Albrecht im Februar 2004 heraus, dass Metros „Deaktivatoren“ lediglich die Metro-eigene Produktnummer vom RFID-Tag löschen, das Tag mitsamt seiner Hardware-Seriennummer „aus technischen Gründen“ allerdings unberührt lassen [Foe04].

Praktiker führen darüber hinaus an, dass eine flächendeckende Ausstattung mit sogenannten „Kill Stations“ unrealistisch sei [Sta03], da Geschäfte mit kleinem Umsatz (z.B. ein Kiosk) kaum in die dazu nötige Infrastruktur investieren könnten, obwohl dort nichtsdestotrotz Produkte mit integriertem RFID-Tag verkauft würden. Ebenso sind heutige Prototypen der Kill-Stationen noch nicht in der Lage, mehrere Tags auf einmal zu deaktivieren: Kunden müssen aufgrund des Passwort-Schutzes mühsam einen Artikel nach dem anderen nach dem Einkauf manuell stumm schalten – ein Aufwand, den ein Großteil der Kunden vermutlich kaum bereit sein dürfte, zu betreiben.[18]

Nicht zuletzt geht durch ein permanentes Deaktivieren der RFID-Tags natürlich auch eine Vielzahl von sekundären Nutzungsmöglichkeiten verloren, wie z.B.

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

[17] Ein Zerschneiden oder Abreissen ist nur bei der Anbringung auf Etiketten praktikabel.

[18] Die derzeit einzige verfügbare Lösung, der NCR EasyPoint-Kiosk [NCR03], kann bisher nur jeweils ein einziges Tag pro Deaktivierungsvorgang ausschalten [RFI03]. Theoretisch sollte es allerdings möglich sein, auch mehrere Dutzend Gegenstände, z.B. eine gesamte Einkaufstasche, auf einmal zu deaktivieren.

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. Dabei könnten bei einer großräumigen Verbreitung der RFID-Technologie und nicht „gekillten" Tags nicht nur Hersteller und Einzelhandel von einem gesteigerten Konsumverhalten durch autonome Besteller in Form intelligenter Kühltruhen profitieren – auch der Kunde mag es schätzen, wenn sein Kühlschrank ihn auf bald ablaufende Milch hinweist bzw. er nicht umständlich den Kassenzettel zur Reklamation aufbewahren muss, da der Artikel selbst alle relevanten Reklamationsinformationen direkt im RFID-Tag speichert.

Schlussendlich läuft die Kritik am Kill-Tag-Ansatz also darauf hinaus, dass weder die Zerstörung für den Kunden überprüfbar ist, noch dadurch das gesamte Problem der Überwachung beseitigt wird, selbst wenn die Zerstörung verlässlich einsetzbar wäre, da vor dem Gang zur Kasse bereits Daten gesammelt werden können. Ebenso scheint ein flächendeckender Einsatz weder praktikabel noch wünschenswert: Zum einen verlangen Kill-Tags hohe Investitionen für Händler mit geringem Umsatz (da teure Kill-Stationen beschafft werden müssten) und einen hohen persönlichen Einsatz vom Kunden selbst (der nach dem Einkauf erst umständlich durch Eingabe Dutzender Deaktivierungs-Codes seine Waren stumm schalten müsste) bzw. dem jeweiligen Händler (der zwecks automatischer Deaktivierung an der Kasse ein aufwendiges Schlüsselmanagement implementieren muss). Andererseits würde durch das Abschalten der Tags ein signifikanter Anteil an nützlicher Zusatzfunktionalität – sowohl für die Industrie als auch den Verbraucher – verloren gehen.

4.2 Pseudonymisierung mittels MetaIDs (Hash-Locks)

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) vor unerlaubtem Auslesen zu schützen. Sobald ein Produkt in den Besitz des Kunden übergeht, erhält dieser die Kontrolle über die Ausgabe des integrierten RFID-Tags und kann so selektiv entscheiden, wer welche Informationen vom Tag auslesen kann.

Das grundlegende Verfahren wurde bereits 2002 von Sarma et al. vorgestellt [SWE02]. Es basiert auf mathematischen Einwegfunktionen, sogenannten „One-Way Hashes", welche die Eigenschaft besitzen, sich relativ einfach berechnen zu lassen, jedoch ein Zurückrechnen auf die Eingabewerte der Funktion praktisch unmöglich machen. Um nun ein RFID-Tag zu „verschließen", wählt ein RFID-Leser einen beliebigen Schlüssel k, bildet mit Hilfe der Einwegfunktion den Hash dieses Schlüssels $h(k)$ (genannt „MetaID") und schreibt diesen auf das zu verschließende Tag. Um ein späteres „Aufschließen" des Tags zu ermöglichen, speichert darüber hinaus der Besitzer (bzw. dessen Lesegerät) den Schlüssel k unter der daraus erzeugten MetaID $h(k)$ in einer Datenbank ab. Tags, die mit einer solchen MetaID beschrieben wurden, antworten auf alle Leseanfragen lediglich mit dieser MetaID, nicht aber mit den „wahren" Informationen (z.B. der auf dem Tag

gespeicherten EPC-Nummer). Will der Besitzer des Tags die im Tag enthaltenen Informationen später wieder verfügbar machen, so liest er zunächst die MetaID des Tags aus, schlägt in seiner Datenbank den für diese MetaID passenden Schlüssel *k* nach und sendet diesen an das Tag. Nachdem das Tag seinerseits wieder den Hashwert $h(k)$ dieses Schlüssels *k* gebildet hat, kann es diesen mit seiner MetaID vergleichen. Bei Übereinstimmung löscht es die MetaID und gibt dadurch den vollen Zugriff auf seine Informationen wieder frei.

Eine RFID-Zugriffskontrolle mit Hash-Schlüsseln bietet mehrere Vorteile: Auch wenn im mathematischen Sinne keine absolute Sicherheit gegeben ist, so ist das Zurückrechnen auf den ursprünglichen Schlüssel mit einem solch erheblichen Aufwand verbunden, dass für alle praktischen Einsatzgebiete im Konsumentenbereich das Wissen um solch eine MetaID einem unautorisierten Leser keine Kontrolle über die wahren Tag-Informationen bietet. Gleichzeitig ist aber eine Hash-Funktionalität vergleichsweise einfach auf dem Tag zu implementieren [Wei03], liegt also auch für billigste Tags preislich im Bereich des Möglichen – ein gewichtiger Vorteil gegenüber komplexeren Ansätzen, die sich der symmetrischen oder asymmetrischen Kryptographie bedienen [NTR03] und deshalb wohl vorerst nur für hochpreisliche Tags abseits des Massenmarktes in Frage kommen.

4.3 Pseudonymisierung durch variable MetaIDs

Während MetaIDs zwar einen effektiven Schutz vor unerlaubtem Auslesen der durch sie geschützten Tag-Informationen (z.B. der EPC des Gegenstandes) bewirken, so ermöglichen sie allerdings immer noch die unauffällige Verfolgung (Tracking) von Personen. Denn auch wenn die MetaID nicht die „wahre" ID eines Gegenstandes darstellt, so eignet sie sich aufgrund ihrer relativen Dauerhaftigkeit als Identifikationsmerkmal für den Gegenstand und damit in vielen Fällen auch für den Besitzer.

Eine konsequente Weiterentwicklung in dieser Richtung stellen „Randomized Hash-Locks" dar [WSR03]. Mit ihnen soll verhindert werden, dass durch wiederholtes Auslesen einer MetaID ein Bewegungsprofil erstellt werden kann. Dazu antworten Tags nicht mehr wie zuvor direkt mit ihrer MetaID, sondern generieren diese bei jedem Auslesevorgang dynamisch neu. Ein auf dem Chip integrierter Zufallszahlengenerator liefert dazu die Zufallszahl *r*, welche verkettet mit der „wahren" ID des Tags als $hash(\mathrm{ID}\|r)$ gehasht wird. Als Antwort erhält ein Leser nun jedes Mal eine neue Zufallszahl *r* (im Klartext) sowie einen neuen Hashwert *h*. Um daraus die ID des Tags zu berechnen, muss der Leser über eine Liste aller ihm bekannten IDs verfügen – eine Bedingung, die für Privatpersonen mit einigen Hundert mit Tags versehenen Gegenständen durchaus realistisch scheint. Zusammen mit der Liste generiert der Leser einfach der Reihe nach jeweils den Hash $hash(\mathrm{ID}_i\|r)$, bis er einen übereinstimmenden Hashwert gefunden hat. Dadurch ist ihm nun implizit die ID des Tags bekannt – ein Freischalten des Tags ist nicht mehr nötig. Erst bei Weitergabe des getaggten Gegenstandes (z.B. zwecks Umtausch oder Rückgabe) würde durch Senden der wahren ID zum Tag dieser wieder freigeschaltet, analog zu dem oben beschriebenen einfachen Hash-Lock-Verfahren.

Auch wenn diese Lösung nicht kryptographisch robust ist,[19] da – zumindest theoretisch – aufgrund der Konstruktion des Hashes ein Angreifer durch wiederholtes Auslesen immer neu generierter MetaIDs Rückschlüsse auf die den Hashwerten zugrunde liegende ID ziehen könnte, so erfüllt sie dennoch zwei wichtige Voraussetzungen für RFID Privacy: Sie verhindert sowohl das unautorisierte Auslesen von auf dem Tag gespeicherten Informationen, als auch das unbemerkte Verfolgen von getaggten Gegenständen (und damit den sie tragenden Personen). Darüber hinaus erscheint sie wirtschaftlich machbar, da Zufallszahlengeneratoren bereits heute schon für Auto-ID-konforme Tags der nächsten Generation vorgesehen sind. Sobald allerdings einmal die ID eines Gegenstandes bekannt ist (z.B. bei dessen Rückgabe), kann aufgrund der Struktur dieses Verfahrens beim gezielten Durchsehen von Log-Dateien schnell der Gegenstand (und damit auch sein Benutzer) rückwirkend identifiziert werden.

Als Alternative schlagen Ohkubo et al. deshalb sogenannte *„Chained Hashes"* vor, bei denen ein Tag nach jeder Ausgabe seiner MetaID diese neu berechnet und den alten Wert überschreibt [OSK03]. Zwecks kryptographischer Robustheit kommen dabei zwei unterschiedliche Hashverfahren zum Einsatz: Das eine hasht jeweils die aktuelle MetaID, um zur nächsten MetaID zu gelangen (d.h. die neue MetaID wird als $\text{MetaID}_{i+1}=hash_{Chain}(\text{MetaID}_i)$ berechnet). Das andere Hashverfahren wird vor der eigentlichen Ausgabe noch einmal auf die momentane MetaID angewandt (d.h. an den Leser wird $hash_{Ausgabe}$(MetaID) ausgegeben), um keinerlei Rückschlüsse auf die folgende neu berechnete MetaID zu geben. Der RFID-Leser muss, wie auch schon bei dem Random-Hash-Lock Verfahren von Weis et al., über eine Liste aller ihm bekannten RFID-Tags (bzw. deren IDs) verfügen. Zur Identifikation eines Tags vergleicht der Leser dessen Ausgabewert mit der gehashten MetaID jedes ihm bekannten Tags, wobei die MetaID sich durch mehrfaches Anwenden von $hash_{Chain}$ auf die ID des Tags ergibt, also zu $hash_{Ausgabe}(hash^{i}_{Chain}(\text{ID}))$. Um nicht endlos oft $hash_{Chain}$ anwenden zu müssen, muss der Leser bzw. die Hintergrundinfrastruktur „mitzählen", wie oft die MetaID eines jeden Tags bereits neu gehasht wurde – ein Mitsenden dieses Wertes *i* vom Tag zum Leser würde das Verfahren analog zu den Random-Hash-Locks einer rückwirkend möglichen Identifikation aussetzen. Im Gegensatz zum Verfahren von Weis et al. bietet es aber (ohne das Mitsenden von *i*) den Vorteil, dass ein Bekanntwerden der MetaID zum Zeitpunkt *t* die Anonymität aller vorherigen Logeinträge dieses Tags nicht beeinträchtigt: Während bei Weis et al. jede Antwort direkt auf der „wahren" ID des Tags basiert (und damit bei der Kompromittierung der ID sich alle existierenden Logeinträge eindeutig zuordnen lassen), so müsste ein Angreifer beim Verfahren von Ohkubo jeweils eine Hash-Funktionen invertieren, um auf den unmittelbar vorausgehenden Wert des Tags zu schließen – eine

[19] Weis et al. schlagen dazu eine Erweiterung vor, welche zusätzlich zum fixen Pseudozufallszahlengenerator ein über einen geheimen Schlüssel *k* parametrisierbares Ensemble von Pseudozufallsfunktionen (PRF) auf dem RFID-Tag verwendet. Statt direkt einen Hashwert aus ID und Zufallszahl *r* zu berechnen, verknüpft das Tag seinen ID-Wert per XOR mit $f_k(r)$. Das Lesegerät muss den geheimen Schlüssel *k* kennen und kann so die passende PRF f_k ermitteln, $f_k(r)$ berechnen und dadurch den ID-Wert bestimmen. Obwohl kryptographisch robuster, sind Weis et al. skeptisch, ob sich PRF-Ensembles kostengünstig auf Massen-Tags unterbringen lassen.

solche Invertierung ist praktisch jedoch unmöglich. Einen Mittelweg favorisieren Henrici und Müller [HeM04], die jeweils die beiden letzten MetaIDs eines Tags in einer Datenbank speichern und nach jedem Auslesen eine zufällige neue MetaID auf dem Tag setzen. Mittels einer beiden Seiten bekannten *TransactionID* (TID), die nach jedem Lesevorgang um Eins erhöht wird, können Replay-Attacken verhindert bzw. die neue MetaID auf dem Rückkanal verschlüsselt werden.[20] Der Vorteil dieses Verfahrens ist die einfachere Tag-Hardware, der Nachteil liegt in der aufwendigen Datenhaltung und -synchronisation.

Einen anderen Weg gehen Inoue und Yasuura [InY03], die statt eines fixen Verfahrens zur Berechnung der MetaID einfach eine vom Benutzer völlig frei wählbare private ID vorschlagen. Wie schon beim Hash-Lock-Verfahren ist die „wahre" Information auf dem Tag gesperrt, solange eine private ID gesetzt ist. Zum Setzen bzw. Löschen einer privaten ID schlagen die Autoren einen physisch gesicherten Kanal vor, z.B. direkten Kontakt bzw. eine unmittelbare Nähe von nur wenigen Zentimetern zum Lesegerät. Obwohl sie dadurch die Komplexität des Tags niedrig halten und ohne jegliche Hardware-Modifikationen auskommen, erhöht sich durch den nun notwendigen physikalischen Zugriffsschutz der Aufwand für den Benutzer. Solange die selbst gewählte private ID bestehen bleibt, ist, anders als beim Random-Hash-Lock-Verfahren, eine Nachverfolgung des Tags möglich – ein besorgter Besitzer müsste also regelmäßig die private ID neu setzen.[21] Dafür können bei frei gewählten privaten IDs Logdateien nicht mehr nachträglich durchsucht werden, solange der Besitzer nicht selbst eine Liste der verwendeten privaten IDs anlegt und diese (ungewollt) einem Angreifer zur Verfügung stellt. Um die Komplexität auf dem Tag weiter zu vermindern, geben die Autoren noch eine Variante ihres Verfahrens an, welche sich mit Nur-Lese-Tags implementieren lässt. Dazu muss allerdings der weltweit eindeutige EPC auf zwei Tags pro Produkt verteilt werden (indem z.B. die ID von Hersteller und Produkt auf der Umverpackung, die Seriennummer aber am Produkt selbst angeheftet wird), um dann beim Verkauf an den Kunden durch Entfernen des Hersteller-Tags eine nicht mehr eindeutige Rest-Seriennummer im Produkt zu belassen. Während so die direkte Zuordnung des verbleibenden Tags zum Produkt verhindert wird (also z.B. das berühmt-berüchtigte Beispiel von der ausgelesenen Unterwäsche), gelten die Benutzeridentifikationsprobleme einer fixen MetaID aber weiterhin.[22]

---

[20] Das Tag speichert dazu zusätzlich zur aktuellen TID die TID der letzten erfolgreichen Transaktion und sendet die Differenz zwischen den beiden zusätzlich zur (gehashten) TID als Teil seiner Antwort an das Lesegerät. Diese Differenz erlaubt es der Datenbank, bei verloren gegangenen Nachrichten die gespeicherte TID mit der auf dem Tag gespeicherten TID zu vergleichen.

[21] Dies allerdings jeweils nur ausserhalb der Reichweite eines Lesegerätes und komplett für alle mitgeführten Tags, da sonst die Umbenennung einfach nachverfolgbar wird.

[22] Neugierige Zeitgenossen könnten sich allerdings immer noch einen Spass daraus machen, die Liste der an mir auslesbaren Tags mit meinen sichtbaren Kleidungsstücken zu vergleichen, um so festzustellen, wie *lange* ich meine nicht-sichtbaren Kleidungsstücke schon am Stück trage…

4.4 Distanz-basierte Zugriffskontrolle

Einen anderen Weg zur Authentisierung von Lesegeräten gehen Fishkin und Roy [FiR03]: Basierend auf dem Prinzip *Distance implies Distrust* schlagen sie vor, in Abhängigkeit von der Signalstärke eines Lesegerätes dynamisch mehr oder weniger detaillierte Informationen vom Tag zurück zu liefern. Als Beispiel geben sie fünf verschiedene Informationsniveaus an: Bei Level 0 antwortet das Tag lediglich mit „Ich bin ein Objekt", bei Level 1 liefert es generische Klassenattribute (z.B. bei einem Hemd Farbe und Art des Stoffes) zurück, während bei Level 4 beispielsweise detaillierte Kaufinformationen (Preis, Zeit und Ort des Erwerbs) preisgegeben würden. Zur Distanzmessung selbst schlagen die Autoren verschiedene Methoden vor, die jeweils über unterschiedliche Vor- und Nachteile verfügen. Die verlässlichste Möglichkeit ist die der Triangulation, d.h. mindestens drei (zeitsynchronisierte) Tags müssen ihr empfangenes Signal an eine Basisstation melden, welche dann durch Ermittlung der Laufzeitunterschiede den relativen Ort des Lesegerätes ermitteln kann und entsprechend die Tags informiert.

Der immense Infrastrukturbedarf einer solchen Lösung (eine vertrauensvolle Basisstation, ein kryptographischer Schutz vor illegalen Lesegeräten, zeitsynchronisierte Tags und schließlich eine komplette Signalanalyse auf dem Tag) scheint kaum für einen realistischen Einsatz zu sprechen, auch wenn man statt einer kompletten Signalanalyse alternativ lediglich die Variationen in der Signalstärke betrachten kann (was weniger aufwendig, allerdings auch weniger genau ist). Ohne jede Infrastruktur kommt schliesslich die dritte Alternative aus, die Analyse des Signal-Rauschabstandes: je höher dessen Standardabweichung, desto weiter ist ein Tag vom Lesegerät entfernt. Diesen Wert könnten Tags jeweils individuell berechnen, wobei allerdings die Variationen erheblich wären, da das Niveau des Hintergrundrauschens von einer Vielzahl von Faktoren abhängig ist und sich dementsprechend bei gleicher Distanz zwischen Lesegerät und Tag stark ändern kann.

Auch wenn das Grundprinzip dieses Ansatzes einfach ist, ist dessen praktische Umsetzung heikel. Zum einen ist die Signalstärke an einem Tag stark abhängig von dessen Orientierung – ändert sich die Lage des Tags relativ zum Lesegerät, so erscheint dieses plötzlich weiter entfernt als es in Wahrheit ist, was zwar unter Datenschutzgesichtspunkten tolerierbar wäre, eine verlässliche Anwendung aber nahezu unmöglich macht.[23] Auch verzerren metallische Gegenstände und Wasser[24] das Energiefeld einer Antenne erheblich, was verlässliche Signalstärkemessungen außerhalb einer Laborumgebung signifikant erschwert. Zwar sind die Autoren hoffnungsvoll, dass eine Kombination der obigen Verfahren, zusammen

[23] Ein gutes Beispiel sind die heutzutage bereits weit verbreiteten RFID-basierten Zugangskontrollen in Skigebieten: Um zu vermeiden, dass versehentlich das Tag des Nebenmannes ausgelesen wird, müssen die Leseradien der Gatter relativ klein gehalten werden – ein Umstand, der die Skifahrer oft zu einer Reihe kreativer Bewegungen zwingt, bis der in der Jacke oder Hose mitgeführte RFID-Skipass erkannt wird.

[24] Da der Mensch zu 45-60 % aus Wasser besteht, „stören" natürlich auch schon Personen den Empfang von RFID-Antennen.

mit aufwendiger konstruierten Antennen auf den Tags,[25] solch einen Ansatz praktikabel machen, doch dürften sowohl die mangelnde Verlässlichkeit einer solchen Lösung als auch deren erhöhte Kosten weder Kunden noch Hersteller zufrieden stellen. Denn selbst wenn eine einigermaßen stabile Positionierung der Lesestation durch die Tags mögliche wäre, würde sich aller Voraussicht nach die „Bedienung" eines solchen entfernungsbasierten Authentisierungssystems durch den Besitzer der getaggten Gegenstände schwierig gestalten, da ohne jegliches Feedback ein Nachvollziehen des Datenflusses zwischen Tag und Lesestation praktisch unmöglich ist und so ein versehentliches Ausgeben von Daten bereits aufgrund einer unachtsamen Bewegung droht. Nicht zuletzt bleibt es natürlich auch fraglich, ob die von den Autoren vorgeschlagene streng hierarchische Aufteilung von Tag-Informationen in vielen Fällen überhaupt sinnvoll ist.

4.5 Abhörsichere Antikollisionsprotokolle

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 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

Dies ist vor allem dann kritisch, wenn die Tag-ID selbst darunter ist, wie es bei gängigen, auf Binärbäumen basierenden Antikollisionsprotokollen der Fall ist [LLS00]. Bei einer weit verbreiteten Variante dieser Protokolle bestimmt z.B. ein vom Leser ausgesendetes ID-Präfix, welche Tags antworten sollen. Solange es zu einer Kollision kommt (d.h. solange zwei oder mehr Tags mit diesem Präfix im Empfangsbereich des Lesegerätes sind) erhöht der Leser die Länge des Präfixes (indem er z.B. eine „1" anhängt), bis sich ein einzelnes Tag „singularisieren" lässt. Anschließend ersetzt er das zuletzt angehängte Bit durch das Inverse und fährt – falls bei diesem Präfix ebenfalls Kollisionen auftreten – mit dem Erhöhen des Präfixes fort.

Sollten sich beispielsweise die Tags „1001" und „1011" in Reichweite befinden, würde infolge der ersten Kollision vom Leser zunächst das Selektions-Präfix „1" gesendet. Da beide Tags dieses Präfix teilen, kommt es erneut zu einer Kollision. Das Präfix „11" würde im Anschluss auf keinen der Tags passen und das Lesegerät würde alternativ das Präfix „10" prüfen. Hier kommt es wieder zu einer Kollision. Erst beim Präfix „100" und dem anschließenden Präfix „101" würde sich jeweils nur ein einziges Tag melden. Durch diese explizite Partitionierung des Suchraumes lässt sich eine beliebige Anzahl von Tags einzeln selektieren.

[25] Sogenannte 2D-Antennen besitzen eine „L"- bzw. „X"-förmige Antenne und können weitgehend unabhängig von ihrer zweidimensionalen Ausrichtung relativ zum Lesegerät ausgelesen werden, auch wenn immer noch Signalstärke-Variationen in Abhängigkeit ihrer räumlichen Ausdehnung auftreten.

Aufgrund der für die Energieversorgung der Tags nötigen starken Sendeleistung der Lesestationen kann ein Angreifer so allerdings, je nach Kombination der Tags, jeweils die Präfixe der selektierten Tags mitprotokollieren – bei Tags mit fortlaufenden Seriennummern wären dies im Allgemeinen die kompletten IDs.

Weis et al. [WSR03] schlagen zur Abhilfe vor, den Leser statt eines kompletten Präfixes lediglich das Kommando „Sende nächstes Bit" an die Tags senden zu lassen. Solange sich die jeweiligen Präfixe der Tags nicht unterscheiden (d.h. alle senden den gleichen Bitwert) tritt keine Kollision auf und der Leser kann sich die den Tags gemeinsame Bitfolge merken. Tritt an Stelle *i* eine Kollision auf, wählt der Leser mittels eines „Select"-Befehls wie gewohnt einen Teilbaum aus, allerdings ohne wie oben das gesamte Präfix (also Bits 1-*i*) zu senden, sondern indem er Bit_{i-1} und Bit_i mit XOR verknüpft und den resultierenden Wert an die Tags sendet. Die Tags bilden nun ihrerseits das XOR ihres Bit_{i-1} (welches ja mit dem Bit_{i-1} des Lesers identisch ist) und dem gesendeten Wert und vergleichen diesen mit ihrem Bit_i. Bei Übereinkunft betrachten sie sich als selektiert und antworten mit ihrem nächsten Bit_{i+1}. Der Angreifer, dem lediglich der Vorwärtskanal (d.h. die Befehle des Lesegeräts, nicht aber die Antworten der RFID-Tags) zur Verfügung steht, kann Bitstellen ohne Kollision nicht abhören (da die Lesestation lediglich ein „Sende nächstes Bit" verschickt und die Antworten der Tags auf große Distanz nicht empfangen werden) und auch keine Rückschlüsse über den selektierten Teilbaum machen, da durch das XOR mit einem ihm unbekannten Wert (Bit_{i-1}) der selektierte Bitwert an Position *i* ebenso unbekannt bleibt.[26] Damit sich die Tags die jeweils aktuelle Bitstelle merken können müssen sie allerdings auch mit (teurem) dynamischem Speicher ausgerüstet werden.

Eine alternative Antikollisionsmethode kann potentiell ohne Informationsverbreitung auf dem Vorwärtskanal auskommen: Bei den auf dem Aloha-Modell basierenden Verfahren antwortet jedes Tag mit einer individuellen, zufälligen Zeitverzögerung auf das Signal des Lesegerätes [Vog02]. Je nach Größe des zur Verfügung stehenden Zeitraumes (die das Lesegerät den Tags mitteilt), verteilen sich so die Antworten zufällig und können im besten Fall völlig kollisionsfrei zurückgeliefert werden. Um die Performanz dieses Verfahrens zu verbessern, besteht allerdings in einigen Protokollen die Möglichkeit, alle fehlerfrei erkannten Tags explizit „stumm zu schalten", damit bei einigen wenigen Kollisionen nicht die gesamte Tag-Population wiederholt ausgelesen werden muss. Falls nicht alternative Selektionsmechanismen (z.B. ein Hashwert oder eine dem Tag bekannte Zufallszahl) verwendet werden, wäre ein entfernter Angreifer natürlich in der Lage, die kompletten IDs der erkannten und stumm geschalteten Tags mitzuprotokollieren.

Die aktuelle Auto-ID/EPCglobal Tag-Spezifikation [Aut03] beinhaltet deshalb einen Zufallszahlengenerator auf dem Tag, welcher sowohl aus Effizienzgründen wie auch aus Sicherheitsgründen eingesetzt wird. Statt mit der wahren ID (typischerweise dem EPC) antworten Tags gemäß dieser Spezifikation innerhalb eines Lesezyklus jeweils mit einer neu generierten Zufallszahl und werden auch über

[26] Die drei Tags *00101*, *00001* und *00110* würden beispielsweise mittels folgender Befehle (die abgehört werden könnten) vom Leser identifiziert: *GetNext*, *GetNext*, *GetNext* (Kollision Tag_1 und Tag_2), *Select(1)* (Kollision Tag_1 und Tag_3), *Select(0)* (Tag_1 identifiziert), *Select(1)* (Tag_3 identifiziert), *Select(0)*, *GetNext* (Tag_2 identifiziert).

diese (wie oben besprochen) stumm geschaltet. Um die wahre ID schlussendlich auszulesen, kann nach vollständiger Erfassung aller Tags über diese temporäre Zufalls-ID die volle ID vom Tag angefordert werden. Dadurch wird nicht nur einem entfernten Angreifer die Möglichkeit genommen, auf dem Vorwärtskanal die wahren IDs der singularisierten Tags mitzuhören, sondern auch die Geschwindigkeit des Antikollisionsprotokolls erheblich erhöht, da die Zufallszahl mit deutlich weniger Bits (12) auskommen kann als die global eindeutige EPC-ID (96) und so kürzere Übertragungszeiten möglich sind.[27]

4.6 Das Blocker-Tag

Die wohl einfachste vorgeschlagene Zugriffskontrolle für RFID-Tags baut auf dem oben beschriebenen Binärbaum-basierten Singularisations-Protokoll auf und verfolgt einen Denial-of-Service-Ansatz [JRS03]. Juels et al. schlagen vor, ein sogenanntes *Blocker-Tag* mitzuführen, welches auf jede mögliche ID reagiert und durch sein ständiges Antworten nicht nur ein schnelles Scannen unmöglich macht (da nun praktisch mehrere Billiarden Tags präsent zu sein scheinen und von einem binärbaumbasierten Antikollisionsprotokoll eins nach dem anderen ausgelesen werden müssen), sondern auch tatsächlich vorhandene Tags effektiv in dieser Masse von virtuellen Tags versteckt. Der Vorschlag der Autoren sieht vor, das Blocker-Tag mit zwei separaten Antennen auszustatten, die auf jede Präfix-Singularisation sowohl mit „0“ als auch mit „1“ antworten, also eine Kollision verursachen, bzw. bei der schlussendlichen Singularisation einer einzelnen ID diese ID zu simulieren. Ein Leser, der auf ein solches Blocker-Tag stößt, würde effektiv blockiert[28] bzw. müsste nach dem Auslesen einiger tausend solcher virtuellen Tags abbrechen.

Um diesen Effekt in der Praxis nutzbar zu machen, schlagen Juels et al. vor, mit Blocker-Tags nur bestimmte Teilbäume – also z.B. alle Tag-IDs, die mit „1“ beginnen – so zu blockieren. Statt an der Kasse mit einem Kill-Befehl permanent deaktiviert zu werden, könnten erworbene Gegenstände durch Umschreiben ihrer ID von „0...“ auf „1...“ in diese vom Blocker-Tag ihres Besitzers geschützten Zone „einsortiert“ werden.[29] Analog zu den von Fishkin und Roy [FiR03] vorgeschlagenen unterschiedlichen Informationszonen könnten durch solch ein Verfahren verschiedene Privatheitszonen implementiert werden, indem Präfixe mit zwei oder mehr Bits verwendet werden und diese entweder mit mehreren physischen Blocker-Tags einzeln blockiert bzw. mit einem einzelnen, aber konfigurierbaren Blocker-Tag dynamisch freigegeben werden.

Damit Lesegeräte nicht „aus Versehen“ solch einen geschützten Teilbaum abfragen und dadurch ungewollt blockiert werden, könnte ein einfaches Signalisationsverfahren die Präsenz eines Blocker-Tags und dessen geschützten Teilbaum

[27] Dies gilt natürlich nur, falls sich viele Tags im Feld des Lesegerätes befinden, da ansonsten der Aufwand für das separate Auslesen der EPC-ID zu groß wird.

[28] Ein komplettes Auslesen von z.B. 2^{64} Tags würde selbst bei einer Leserate von über 100 000 Tags pro Sekunde mehr als 4 Millionen Jahre benötigen.

[29] Um den Aufwand für Kunden zu minimieren, könnten Händler Blocker-Tags bereits in die für Kunden bereitgestellten Tragetaschen integrieren.

ankündigen, z.B. über eine reservierte Tag-ID, die vor Beginn eines eigentlichen Lesevorgangs von Lesestationen abgefragt würde. Weiterhin besteht das Problem, dass Blocker-Tags nicht nur die persönlichen Tags einer einzelnen Person schützen, sondern bei physischer Nähe auch ungewollt Tags anderer unlesbar machen. Juels et al. schlagen hierfür vor, hunderte von Privatheitszonen einzurichten, um so die Wahrscheinlichkeit zu minimieren, dass zwei Personen ihre persönlichen Tags in die gleiche Zone eingeteilt haben. Je mehr unterschiedliche Zonen (und damit individuelle Blocker-Tags) es jedoch gibt, desto besser lassen sich Blocker-Tags selbst zur Identifikation einer einzelnen Personen verwenden.

Der größte Vorteil des Blocker-Tag-Ansatzes ist sicherlich der geringe Infrastrukturaufwand, da Tags nahezu unverändert und Lesegeräte mit nur minimalen Softwareänderungen verwendet werden könnten. Dem gegenüber steht allerdings die geringe Verlässlichkeit des Verfahrens: Implementiert man Blocker-Tags kostengünstig als passive Systeme, kann eine ungünstige Lage zur Leseantenne schnell die vermeintlich geschützten Tags sichtbar machen. Will man Privatheitszonen verwenden, müssen Tags darüber hinaus mit wiederbeschreibbarem Speicher ausgerüstet werden, was die Preise in die Höhe treibt. Auch Störungen durch das eigene Blocker-Tag bzw. Blocker-Tags Dritter scheinen vorprogrammiert: mein automatisches Waschprogramm schlägt fehl, weil ich mein Blocker-Tag in der Hosentasche vergessen habe, und mein Kühlschrank übersieht die Hälfte meiner Einkäufe, weil mein Nachbar (mit störendem Blocker-Tag) mir beim Einräumen meiner Lebensmittel hilft. Darüber hinaus ist es natürlich auch denkbar, dass eine genaue Analyse des Energiefeldes es einem speziellen Lesegerät erlauben würde, eine künstlich hervorgerufene Kollision (bzw. eine lediglich virtuell präsente ID) von einer echten (d.h. aufgrund der tatsächlichen Anwesenheit eines Tags erzeugten Kollision bzw. ID) zu unterscheiden, da in diesem Falle zwei oder mehr verschiedene Tags antworten.

4.7 RFID in Banknoten

Als aus Datenschutzsicht besonders heikel gilt die Idee, RFID-Tags in Banknoten zu integrieren. Bereits vor dem Start des Euro-Bargelds im Januar 2002 kündigte die Europäische Zentralbank (EZB) an, solch eine Maßnahme zur Verbesserung der Fälschungssicherheit bzw. Geldwäschekontrolle bis spätestens 2005 zu erwägen [Yos01]. Auch bei Lösegeldforderungen stünde so eine unauffällige Möglichkeit zur Verfügung, Banknoten zu kennzeichnen und deren Auftauchen im Geldmarkt frühzeitig zu registrieren.

Anders als bei der Kennzeichnung von Konsumgegenständen sind die oben skizzierten Lösungen wie Kill-Tags oder Hash-Lock-basierte Verfahren nicht einsetzbar: Eine vollständige Kontrolle des Besitzers über den RFID-Tag eines Geldscheins würde der ursprünglichen Idee hinter der Banknotenkennzeichnung zuwider laufen. Dennoch sind die Kassandra-Rufe der Konsumentenschutzgruppen womöglich verfrüht: Auch wenn Banknoten in Zukunft für einzelne Nennwerte (z.B. für 200 und 500 Euro-Scheine) oder sogar komplett mit RFID-Tags ausgerüstet würden, so wäre es für Diebe keineswegs ein Leichtes, die Geldbörsen ahnungsloser Passanten zu durchleuchten, um unauffällig ein möglichst lohnendes

Opfer ausfindig zu machen. Zum einen sind RFID-Tags mit einer großen Reichweite für die Anforderungen von Zentralbank und Sicherheitsorganen nicht nötig, wenn nicht sogar kontraproduktiv, da die bei größeren Leseabständen nötigen Antikollisionsprotokolle die Lesegeschwindigkeit vermindern und den Preis der Tags in die Höhe treiben würden. So haben beispielsweise die von der EZB u.a. in Betracht gezogenen µ-Chips von Hitachi [Mar03] in ihrer Grundkonfiguration lediglich eine Reichweite von wenigen Millimetern – kaum ausreichend, um unbemerkt in der Brieftasche ausgelesen zu werden. Zum anderen ist es ein Leichtes, Geldbörsen mit einem Einsatz aus Aluminiumfolie herzustellen, welche skeptischen Zeitgenossen die Nichtauslesbarkeit ihrer mitgeführten Bargeldbestände quasi garantieren würden.

Auch das oft angeführte Ausspionieren des Bargelds durch clevere Marketingfachleute, die einzelne Banknoten ihren jeweiligen Kunden zuzuordnen versuchen, scheint bei näherer Betrachtung kaum praktikabel. Soll das Kaufverhalten einzelner Kunden studiert werden, bietet heute bereits die an der Kasse vorgezeigte Kundenkarte alle Möglichkeiten. Um ein globales Kaufverhalten von Kunden – analog zu den heutigen Kreditkartentransaktionen – mit RFID-Bargeld zu analysieren, wäre nicht weniger nötig als ein zentrales Bargeldregister aller weltweiten (oder zumindest nationaler) Bargeldbewegungen – bei der Vielzahl der dabei involvierten Parteien ist dies weder wirtschaftlich noch gesellschaftlich realistisch. Auch ein in [JuP03] als Beispiel angeführter lokaler Zusammenschluss einzelner Händler zwecks (heimlichen) Ausspionierens gemeinsamer Kunden wäre nicht nur fast überall ein schweres Vergehen gegen geltendes Datenschutzrecht, sondern würde sich im Rahmen eines händlerübergreifenden Kundenkartensystems wie z.B. Payback [Loy04] weitaus einfacher und verlässlicher implementieren lassen.

Sieht man von Schreckensvisionen der Verschwörungstheoretiker ab, welche Strafverfolgungsbehörden die Bewegungen individueller Banknoten durch den flächendeckenden Einsatz von Lesegeräten in Echtzeit verfolgen lassen,[30] gibt es nur wenige Gründe, die einen Einsatz von RFID-Tags in Banknoten rechtfertigen könnten. Sicherheitstechnische Zusatzinformationen, wie beispielsweise digitale Signaturen von Seriennummern, um Fälschern das Erfinden von Seriennummern zu verunmöglichen, lassen sich ebenso gut als 2D-Barcodes direkt auf die Banknote drucken (hier würden RFID-Tags höchstens ästhetische Zwecke erfüllen). Allenfalls wäre ein Auslesen dieser Informationen mittels RFID geringfügig einfacher (wenn auch nicht notwendigerweise verlässlicher), doch würde die Gefahr des unerlaubten (und unbemerkten) Auslesens diese Erleichterung in der gesellschaftlichen Diskussion mehr als aufwiegen. Ebenso wären aufgrund der hohen Packungsdichte von Banknoten automatische Inventarisierungen etwa bei Banken, analog zur Lagerinventur beim Einzelhandel, mit heutiger RFID-Technologie wohl kaum durchführbar [Eco02]. Und ein Aufspüren von „heißen“ Banknoten, beispielsweise aus einem Bankraub oder einer Entführung, wäre mit den oben

[30] Ein solches System würde sich, wie erwähnt, durch den Einsatz einer wenigen Cent teuren Aluminiumfolie leicht sabotieren lassen. Auch die von Albrecht [Alb02] befürchteten Banknoten mit „Gedächtnis“, welche auf ihren RFID-Chips ihre Aufenthaltsorte speichern, um sie später den Sicherheitsorganen zugänglich zu machen, sind praktisch unmöglich verlässlich (und wirtschaftlich) zu implementieren.

erwähnten optischen IDs fast ebenso praktikabel (oder unpraktikabel) wie mit funkbasierten, vorausgesetzt Einzelhändler würden Lesegeräte einsetzen, die einen automatischen Abgleich mit gesuchten Seriennummern ermöglichen. Die Tatsache, dass ein Funkchip sich dem Nachdrucken bzw. Kopieren entziehen würde und auf dem grauen Markt kaum zu beschaffen wäre, könnte allerdings existierende Sicherheitsmerkmale in dieser Richtung (z.B. eingewobene Silberstreifen) verstärken helfen, da so Verkaufsautomaten (nicht aber Menschen) Fälschungen leichter erkennen könnten.

Auch wenn also funkbasierte Seriennummern auf Banknoten noch kaum den erheblichen Aufwand rechtfertigen würden, den eine Einführung von RFID-Chips mit sich bringen würde: falls deren Einsatz erfolgt, muss Sorge getragen werden, dass eine zu Strafverfolgungszwecken installierte Infrastruktur nicht ungewollte Datenspuren erzeugt, unabhängig von der verwendeten Technologie. RFID-Chips ohne externe Antenne, ähnlich dem seit einiger Zeit verfügbaren 0,6x0,6 mm großen µ-Chip von Hitachi, mit mehreren hundert Bits WORM-Speicher[31] und einem Leseradius von nur wenigen Millimetern, würden zwar die Fälschungssicherheit erhöhen, ohne die viel zitierten (Allmachts-)Visionen einer Echtzeitverfolgung von Erpressern und Geldwäschern Wirklichkeit werden zu lassen, wären aber bezüglich Daten- und Konsumentenschutz wohl eher bedenkenlos einsetzbar. Eine darauf aufbauende Verfolgung der Bargeldströme durch den Einzelhandel wäre zwar prinzipiell machbar, doch erscheint ein derartiges Anliegen (zumindest heutzutage) weder politisch noch wirtschaftlich durchsetzbar, unabhängig davon, ob WORM-RFID-Chips oder optisch erkennbare Seriennummern auf Geldscheinen angebracht sind.

4.8 RFID in Reisepässen

Im Gegensatz zu den nur vage bekannten Plänen, RFID-Tags in Banknoten zu integrieren, ist die Ausstattung von Reisepässen mit Funkchips bereits beschlossene Sache. Die im Mai 2004 vom *International Civil Aviation Organization* (ICAO) verabschiedete Spezifikation für maschinenlesbare Reisedokumente (MRTD – *Machine Readable Travel Documents*) verlangt die digitale Speicherung des Passbildes in jedem Reisepass. Optional dürfen passausgebende Behörden auch Fingerabdrücke und Irisbilder in die zur Speicherung vorgeschriebenen RFID-Chips einbringen[32] [Küg05]. Während die Authentizität der Informationen durch eine digitale Unterschrift gewährleistet sein muss, ist die Verschlüsselung des Auslesevorgangs zur Gewährleistung der Vertraulichkeit optional. Um das unerlaubte Auslesen des Chips zu verhindern, ermöglicht ein optionaler Mechanismus die Verwendung eines optisch auszulesenden Zugriffsschlüssels, ähnlich des von Juels und Pappu [JuP03] im Zusammenhang mit Banknoten vorgeschlagenen Verfahrens. Um sich gegenüber dem RFID-Tag zu authentisieren, benötigt

[31] Write-Once-Read-Many, d.h. einmal von der Zentralbank beschrieben, würde sich die Information nicht mehr ändern lassen.

[32] Die Mitgliedsstaaten der EU haben sich im Dezember 2004 darauf geeinigt, ebenfalls Fingerabdrücke in EU-Reisepässe aufzunehmen [Pou04].

ein Lesegerät einen in der maschinenlesbaren Zone[33] abgelegten Schlüssel, der zunächst optisch ausgelesen werden muss [Küg05]. Aus dem so abfragbaren Geburtsdatum, der Passnummer und dem Ablaufsdatum des Passes wird der Zugriffsschlüssel *K* berechnet, welcher vom Lesegerät an das RFID-Tag gesendet werden muss, um einen mehrstufigen dynamischen Schlüsselfindungsprozess zu starten. Die auf dem Tag gespeicherten Daten können danach mit dem soeben vereinbarten dynamischen Schlüssel ausgelesen werden. Dies verhindert das selbst von Sicherheitsexperten oft befürchtete Auslesen von Passdaten aus einer Menschenmenge: *„[P]ickpockets, kidnappers, and terrorists can easily – and surreptitiously – pick Americans or nationals of other participating countries out of a crowd“* [Sch04]. Ein Angreifer, der es auf eine ganz bestimmte Person abgesehen hat, könnte allerdings die zur Berechnung des Schlüssels nötigen persönlichen Informationen in Erfahrung bringen, um dann gezielt nach einem auf diesen Schlüssel antwortenden Reisepass zu suchen. Dies setzt natürlich voraus, dass die gesuchte Person den Reisepass ungeschützt, d.h. ohne beispielsweise einen Umschlag aus Aluminiumfolie, bei sich trägt. Auch in diesem Fall scheint es sowohl billigere als auch verlässlichere Methoden zu geben (z.B. die Gesichtserkennung per Kamera).
Eine weitere Komplikation stellen die weiterführenden Pläne der EU für den Einsatz von RFID bei Visa dar. Genauso wie der enge Kontakt von Banknoten ein Auslesen der dicht zusammengerückten RFID-Tags verunmöglicht, würde ein mit mehreren RFID-Visa ausgestatteter RFID-Reisepass kaum verlässlich lesbar sein [Let04].

4.9 Allgemeine Sicherheitsaspekte

Unabhängig vom Potential zur Überwachung und Verfolgung von Privatpersonen sind RFID-Lösungen im industriellen Bereich natürlich auch unter sicherheitstechnischen Gesichtspunkten zu evaluieren. Einzelhändler laufen durch die umfassende Kennzeichnung aller ihrer Produkte Gefahr, nicht nur ihre eigene Inventur zu vereinfachen, sondern auch der Konkurrenz die genaue Überwachung ihres Warenbestands zu ermöglichen: Ein morgendlicher Besucher mit verstecktem Lesegerät könnte mit einem einfachen Rundgang durch die Regalreihen leicht die Warenbewegungen von Tag zu Tag aufnehmen. Ebenso sind automatisierte Zahlungssysteme und Diebstahlsicherungen, welche auf RFID-Tags basieren, durch gefälschte RFID-Tags, einfache Störsender und Abschirmfolien leicht zu umgehen. [BSI04] beschreiben eine Reihe verschiedener Angriffsarten, die die Integrität eines RFID-Systems gefährden können: das Fälschen von Inhalten, das Fälschen von Tag-Identitäten, das Fälschen von Reader-Identitäten, das Deaktivieren von Tags, das physische Ablösen von Tags, das Abhören der Kommunikation und das Blocken bzw. Stören des Auslesens. Weis et al. [WSR03] schlagen zum Schutz einer kommerziellen RFID-Infrastruktur eine Kombination aus Lesegerätsdetektoren (zum Aufspüren unautorisierter Lesegeräte), „vokaler“ Kill-

[33] Die maschinenlesbare Zone (MRZ – *Machine Readable Zone*) bezeichnet die beiden optisch auslesbaren Textzeilen heutiger Reisepässe, in denen der Name, das Geschlecht, die Passnummer, und das Ausstellungs- und Ablaufsdatum des Passes vermerkt sind.

gerätsdetektoren (zum Aufspüren unautorisierter Lesegeräte), „vokaler“ Kill-Standards (gerade deaktivierte Tags machen auf einer speziellen Frequenz auf ihre Abschaltung aufmerksam, um ein unbemerktes Deaktivieren zu verhindern) und aufgedruckte Zugriffsschlüssel, welche z.B. manuelle Umschaltung zwischen Hash-Lock- und Randomized-Hash-Lock-Modus bzw. bei Schlüsselverlust eine Freischaltung des Tags ermöglichen. Umgekehrt sollten Lesegeräte Antworten von Tags mit anomalen Charakteristiken (z.B. Signalstärke, Antwortzeit) ignorieren, um ein Tag-Spoofing zu verhindern. Auch die Verwendung von Frequency-Hopping wird empfohlen (indem z.B. der Leser dem Tag jeweils die zu verwendende Frequenz vorgibt), um eine Verbindungsübernahme durch unautorisierte Lesegeräte zu verhindern.[34] Weiterhin helfen Maßnahmen wie die oben beschriebenen abhörsicheren Antikollisionsprotokolle, auf dem Vorwärtskanal nicht unbeabsichtigt Informationen über die gerade ausgelesenen Tags weiterzugeben.

5 Zusammenfassung und Beurteilung

Mit dem Kill-Befehl steht das wohl am weitesten fortgeschrittene technische Schutzverfahren für RFID-Tags zur Verfügung, welches wirkungsvoll, wenn auch nicht unbedingt immer überprüfbar, einen Großteil der Gefahren für den Datenschutz beim Einsatz von RFID beseitigt. Der momentan vorgesehene Passwortschutz scheint jedoch kaum praktikabel – der für das Passwortmanagement nötige Aufwand steht in keinem Verhältnis zu den Vorteilen eines solchen Verfahrens, nämlich ein unerlaubtes Deaktivieren der Tags zu verhindern. Ein effektiver Diebstahlschutz lässt sich weitaus einfacher auf operationeller Ebene realisieren, indem beispielsweise selbst mit Tags versehene Waren auch weiterhin offen in einen Einkaufswagen gelegt werden müssen, statt es dem Kunden zu erlauben, diese bereits im Laden z.B. in die Jackentasche zu stecken. Ein Entfernen bzw. Zerstören der Tags geschieht dabei allerdings nicht nur auf Kosten der Hersteller und Händler, die dadurch auf Folgenutzungen ihrer Identifikationssysteme verzichten müssen, sondern auch zu Ungunsten des Verbrauchers, der in Zukunft vielleicht selbst ein Interesse an einer automatischen Identifikation etwa von Lebensmitteln oder Kleidern durch seine smarten Haushaltsgeräte haben könnte. Nichtsdestotrotz wird aber wohl anfangs die Option, ein Produkt mit einem leicht entfernbaren bzw. automatisch deaktivierten RFID-Tag erwerben zu können, allein schon aus ethischen Gründen dem Konsumenten angeboten werden müssen. Dies entspricht dem in vielen Ländern üblichen datenschutzrechtlichen Grundsatz, dass, wenn immer möglich, eine Service-Variante angeboten werden muss, die ohne bzw. nur mit minimaler Datenerhebung auskommt.[35] Eine gemeinsame Entschließung der Teilnehmer an der Internationalen Konferenz der Datenschutzbeauftragten im November 2003 zum Thema RFID wies nachdrücklich darauf hin,

[34] Frequency-Hopping für RFID-Tags ist im US-amerikanischen 915 MHz Band bereits vorgeschrieben [Aut03].

[35] So wurde beispielsweise beim Bau des ersten vollautomatischen Highway-Mautsystem Kanadas, dem Expressway 407, in Zusammenarbeit mit dem Privacy Commissioner von Ontario eine vollständig anonym nutzbare Abrechnungsalternative entwickelt [Cav98].

dass die Grundsätze des Datenschutzrechtes auch für RFID-Systeme gelten und dass die Prinzipien der Datensparsamkeit, Transparenz, Zweckbindung und Wahlmöglichkeit gegeben bleiben müssen [DPC03].

MetaID-Verfahren erlauben es statt dessen, trotz aktiviert gebliebenem RFID-Tag die „wahre" Identifikation des Gegenstandes, also z.B. seine EPC, gegenüber nicht autorisierten Lesegeräten zu verbergen – einem unbemerkten Auslesen der Unterwäschenmarke auf offener Strasse wäre dadurch ein Riegel vorgeschoben. Schutz vor einer unerlaubten bzw. unbemerkten Personenverfolgung (Tracking) ist damit allerdings nicht möglich, ebenso wenig wie mit graduellen Zugriffsverfahren, welche je nach Zugriffslevel mehr oder weniger detaillierte Informationen zurückliefern (also etwa Produkt-Typ vs. Seriennummer). Denn selbst ohne eindeutige IDs bleiben aufgrund der bestimmten Kombination („Constellation") von Tags Personen immer noch eindeutig identifizierbar.[36] Variable-MetaID-Verfahren bieten zwar durch die ständig wechselnden IDs einen effektiveren Schutz vor Tracking, gehen aber mit einem erhöhten strukturellen Aufwand in den Bereichen Lesegeräte und Datenbanken einher. Auch kann der ID-Wechsel selbst in vielen Fällen trivial nachvollzogen werden, wenn z.B. keine oder nur wenige andere Personen in der Nähe sind. Nicht zuletzt muss man natürlich beachten, dass sich durch ein Verfahren wie den Randomized-Hash-Locks der Sicherheitsbereich vom Tag hin zum smarten Haus des Besitzers verschiebt. Denn sobald die in den eigenen Lesegeräten gespeicherten IDs bzw. Schlüssel bekannt sind, kann sowohl in Echtzeit als auch nachträglich in Log-Dateien die gesuchte Person durch ihre Gegenstände identifiziert werden.

Energiebasierte Verfahren sind aufgrund ihrer einfachen Heuristik – Distanz bedingt Misstrauen – zwar attraktiv, doch scheinen sie nicht nur wegen der damit verbundenen technischen Probleme unpraktikabel, sondern auch infolge ihres für den Benutzer nur schwer intuitiv fassbaren Verhaltens (bei welcher Distanz werden welche Daten ausgegeben?). In ihrer einfachsten Ausprägung könnte der Ansatz allerdings eine gute Richtschnur bieten für die Konzeption RFID-basierter Lösungen: Wähle die Reichweite der eingesetzten Tags so niedrig wie möglich. So sollten RFID-Tags für Banknoten, die die Fälschungssicherheit erhöhen sollen, über eine Lesedistanz von nur wenigen Millimetern verfügen – jede höhere Reichweite verstärkt die Gefahren für die Privatsphäre, ohne dem Zweck des Systems besser zu dienen. Analog dazu kämen für die Identifikation von Paletten und Kartons Tags mit großer Reichweite in Frage, für die eigentlichen Produkte solche mit überaus geringer (also einige wenige Zentimeter – ausreichend, um im Reklamationsfall die Kaufdaten auszulesen bzw. in Regalen den Bestand zu überwachen, aber nicht, um von der Straße aus in Häusern Diebesgut aufzustöbern).

Blocker-Tags sind auf den ersten Blick durch ihren einfachen aber effektiven Aufbau eine interessante Alternative für den Kill-Befehl, vor allem in ihrer

[36] Unter „Tracking" ist dabei weniger eine Echtzeit-Verfolgung als eine A-posteriori-Suche in verteilten Log-Dateien zu verstehen, um z.B. einen bestimmten Tathergang zu rekonstruieren. Auch wenn Überwachungen in Echtzeit denkbar sind, so wäre die Zusammenführung der Informationen in einem zentralisierten System, beispielsweise von den Strafverfolgungsbehörden betrieben, nicht nur äusserst kostspielig, sondern im Vergleich zu traditionellen Überwachungsmethoden auch weitaus unzuverlässiger.

Grundvariante ohne komplizierte Privatheitszonen. Sie könnten Verwendung finden eingebettet in Papiertüten von Supermärkten und anderen Geschäften, um Kunden ein „sorgenfreies“ Nachhausetragen ihrer Einkäufe zu ermöglichen, wenn auch eine mit Aluminiumfolie ausgelegte Tasche dieses verlässlicher (und womöglich billiger) erreichen könnte. In der Form von Uhren oder Gürtel könnten sie, als aktive Variante mit größerer Reichweite, allerdings durchaus Käufer finden. Doch der erhöhte Aufwand für den Konsumenten, je nach Situation die richtige Einstellung für seinen Blocker-Tag zu finden, um nicht Probleme bei der Nutzung von ihm gewünschter Dienste zu bekommen, dürfte wohl den Großteil der Bevölkerung davon abhalten und lässt deshalb die standardisierte Einführung dieses Verfahrens kaum realistisch erscheinen.

Allen technischen Verfahren gemein ist der Aufwand für den Einzelnen, der sich so vor unerlaubten Leseversuchen bzw. Personenverfolgungen zu schützen versucht. Ein Hauptkritikpunkt aller dieser Möglichkeiten ist deshalb auch, dass sie die Verantwortung vom Hersteller und Händler auf den Kunden abwälzen, der nun selber sehen muss, dass die von ihm erworbenen Gegenstände ihm nicht zum Nachteil gereichen. Weitaus kundenfreundlicher sind hingegen legislative Ansätze, die bereits im Voraus die Sammlung solcher Daten verbieten würden, sodass es gar nicht erst zu einer unautorisierten Nutzung kommen darf. Bestehende Datenschutzgesetze in vielen Ländern, allen voran die der Europäischen Union, aber auch in Kanada oder Australien, verbieten schon heute viele der möglichen Szenarien, vor denen Konsumentengruppen beim Einsatz von RFID warnen. Ein heimliches Überwachen zu Marketingzwecken wäre darüber hinaus kaum zu verbergen – weitaus wahrscheinlicher ist eine Entwicklung analog zu den heute bestehenden Kundenkarten, bei denen der Kunde vorher in einer expliziten Einverständniserklärung den Händlern die Überwachung etwa im Austausch für Rabatte erlaubt. Doch auch dann bleibt angesichts der Dimensionen einer solchen Datensammlung die Möglichkeit bestehen, dass der Gesetzgeber früher oder später explizite Grenzen für die Erhebung zieht.

Wie werden wir also in einer Zukunft voller smarter Alltagsgegenstände, intelligenter Umgebungen und mit Tags versehenen Lebensmitteln leben? Viele der oben beschriebenen technischen Verfahren zum Schutz vor unerlaubtem Auslesen von RFID-Tags werden sich wohl kaum am Markt durchsetzen können. Statt komplizierter Kill-Tags dürfte sich so beispielsweise anfangs eher die physische Entfernung bzw. Zerstörung der Tags etablieren (d.h. sie werden auf Umverpackungen bzw. Anhängern angebracht werden), später könnte die drahtlose Entwertung integrierter Tags an der Kasse hinzukommen – allerdings ohne dass deren Abschaltung durch ein Passwort geschützt würde.[37] Allenfalls Verfahren, die sich ohne größeren Mehraufwand (sowohl preislich, wie auch in der Bedienung) in existierende Protokolle integrieren lassen, haben eine reale Chance (und praktische Berechtigung), sich in technischen Spezifikationen wie denen von EPCglobal wieder zu finden – wie beispielsweise einige der oben vorgestellten

[37] Bereits heute können viele auf einfachen RFID-Tags basierende Diebstahlsicherungen mit einem ausreichend starken Magnetfeld heimlich deaktiviert werden. Mittels Kameraüberwachung und stichprobenartigen Kontrollen durch Angestellte werden wohl auch in Zukunft solche Art Diebe ermittelt werden müssen. Dies bedingt natürlich auch, dass in absehbarer Zukunft Lebensmittel immer noch offen in einen Einkaufskorb gelegt werden müssen, statt bereits am Regal in unseren Jackentaschen zu verschwinden.

EPCglobal wieder zu finden – wie beispielsweise einige der oben vorgestellten abhörsicheren Antikollisionsprotokolle: Statt totaler Sicherheit durch komplexes Schlüsselmanagement also eher die Nutzung verbesserter Protokolle zur Begrenzung der Sendereichweite von Tag-IDs. Ein gezieltes Ausspionieren einzelner Personen wird also immer noch möglich bleiben, in Anbetracht des erheblichen Aufwandes allerdings analog zur heutigen individuellen Beschattung eher die Ausnahme sein als die Regel. Darüber hinaus wäre allerdings eine solche gezielte Überwachung sogar leichter zu bemerken als beispielsweise heutige Teleobjektive und Richtmikrofone, da sich das elektromagnetische Feld eines RFID-Lesers vor geeigneten Messinstrumenten nicht verbergen lässt. Natürlich bleibt die Gefahr des Zusammenführens verschiedener Logdateien, doch hier ist weit mehr der Gesetzgeber als der Entwickler gefordert, der rechtzeitig Rahmenbedingungen für die Speicherdauer und die etwaige Offenlegung solcher Datensammlungen festlegen muss.

Nicht zuletzt bietet sich sogar die Gelegenheit, durch die konsequente Integration der *Fair Information Practices* in technische Protokolle auf lange Sicht hinaus den heutigen Schutz der Privatsphäre vielleicht sogar noch zu verbessern. So könnten zukünftige Lesegeräte etwa als Teil des Ausleseprotokolls ihre eigene Identität melden und dadurch Verbrauchern die Gelegenheit geben, nachzuvollziehen, wer wann welche Informationen ausgelesen hat. Als Teil eines vom Gesetzgeber geforderten Standards wäre so die Kontrolle unerlaubter Lesevorgänge durch unabhängige Datenschützer deutlich vereinfacht und damit der Verbraucherschutz gestärkt [FSL04].

RFID-Tags sind dabei allerdings nur ein Aspekt einer umfassend informatisierten Zukunft [BCL03], wenn auch wohl momentan in der medialen Diskussion einer der prominentesten [Bor04]. Sie machen jedoch deutlich, dass rein technische Lösungen allein wohl kaum in der Lage sein werden, eine Welt voll von unsichtbaren Computern und deren oft unbemerkter Kommunikation untereinander wirkungsvoll zu gestalten – erst im Zusammenspiel mit rechtlichen und sozialen Komponenten können unterstützende technische Maßnahmen eine Umgebung schaffen, die unseren Vorstellungen von Privatsphäre entspricht [Lan01]. Gleichzeitig wird aber auch klar, welchen Einfluss der Entwurf technischer Protokolle und Systeme auf die gesellschaftlichen Möglichkeiten hat, und zwar nicht nur im Bereich des Datenschutzes [Les99]. Wenn wir es schaffen, dieses Zusammenwirken zwischen sozialem Diskurs, gesellschaftlichen Normen und technischer Entwicklung innerhalb des Ubiquitous Computings zu erkennen und uns nutzbar zu machen, dann sollte eine „Diktatur der Technik“,[38] wie sie beispielsweise Steven

[38] Der damalige Bundesverfassungsgerichtspräsident Ernst Benda fasste in einem Interview nach dem Volkszählungsurteil seine privaten Gedanken so zusammen: „Das Problem ist die Möglichkeit der Verselbständigung der Technik, dass die Gegebenheiten und Zwangsläufigkeiten der Technik so eine Art eigene Diktatur errichten. Also nicht die Diktatur von Menschen über Menschen mit Hilfe der Technik, sondern die Diktatur der Technik über die Menschen“ [Rei01].

Spielberg in seiner düsteren Hollywood-Vision *Minority Report*[39] aufzeigt, auch weiterhin Fiktion bleiben.

Literatur

[Alb02] Albrecht K (2002) Supermarket Cards – The Tip of the Retail Surveillance Iceberg. Denver University Law Review 79(4): 534-539, 558-565, www.nocards.org/AutoID/overview.shtml

[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 Press Release, 4. April 2003, www.benetton.com/press/sito/_media/press_releases/rfiding.pdf

[BeS03] Beresford AR, Stajano F (2003) Location Privacy in Pervasive Computing. IEEE Pervasive Computing 2(1): 46-55

[BCL03] Bohn J, Coroama V, Langheinrich M, Mattern F, Rohs M (2003) Allgegenwart und Verschwinden des Computers: Leben in einer Welt smarter Alltagsdinge. In: Grötker R (Hrsg) Privat! Kontrollierte Freiheit in einer vernetzten Welt. Heise-Verlag, Hannover

[Bro39] Brougham HP (1839) Historical Sketches of Statesmen Who Flourished in the Time of George III (1): 52. Zitiert in: Platt S (Hrsg., 1989) Respectfully quoted: a dictionary of quotations requested from the Congressional Research Service. Library of Congress, Washington D.C., www.bartleby.com/73

[Bor04] Borchers D (2004) Medien und Informatik: Frischkäse bitte bei Kasse 3 melden: Funketiketten wecken diffuse Ängste. Neue Zürcher Zeitung, 5. März 2004

[BSI04] Bundesamt für Sicherheit in der Informationstechnik (2004) Risiken und Chancen des Einsatzes von RFID-Systemen: Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. SecuMedia, Ingelheim

[Cav98] Cavoukian A (1998) 407 Express Toll Route: How You Can Travel the 407 Anonymously. Information and Privacy Commissioner / Ontario. Toronto, Kanada www.ipc.on.ca/userfiles/page_attachments/407-e.pdf

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

[Coc01] Cochrane, P (2000) Head to Head. Sovereign Magazine Spring 2000: 56-57, www.cochrane.org.uk/opinion/archive/articles/prof.htm

[39] Aufbauend auf einem Roman von Philip K. Dick [Dic57] und nach intensiven Diskussionen mit namhaften Zukunftsforschern entwirft Spielberg eine Antivision unserer Zukunft, die halb Polizeistaat, halb Werbehölle ist.

[Coh00] Cohen JE (2000) Examined Lives: Informational Privacy and the Subject as Object. Stanford Law Review 52(1373). Zitiert in [Sol03]

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

[COE04] Council of Europe (2004) Legal Affairs: Data Protection, www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection

[Cus03] Cushman R (2003) Privacy / Data Protection Project: Fair Information Principles and Practices, http://privacy.med.miami.edu/glossary/xd_fair_info_principles.htm

[Dic57] Dick PK (1957) Minority Report. Fantastic Universe

[Dow03] Downes L (2003) Don't fear new bar codes. USA Today: 23A, 25. September 2003, www.usatoday.com/usatonline/20030925/5532478s.htm

[DPC03] Resolution on Radio Frequency Identification. 25th International Conference of Data Protection and Privacy Commissioners, November 2003, www.privacyconference2003.org/commissioners.asp

[Eco02] The Economist (2002) Science and Technology: Where's the Smart Money? 9.-15. Februar 2002, www.economist.com/printedition/index.cfm?d=20020209

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

[FMB03] Fleisch E, Mattern F, Billinger S (2003) Betriebswirtschaftliche Applikationen des Ubiquitous Computing: Beispiele, Bausteine und Nutzenpotentiale. HMD – Praxis der Wirtschaftsinformatik 229: 5-15

[FSL04] Flörkemeier Ch, Schneider R, Langheinrich M (2004) Scanning with a purpose – supporting the Fair Information Principles in RFID protocols. Proceedings of the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan, November 2004

[FiR03] Fishkin KP, Roy S (2003) Enhancing RFID Privacy via Antenna Energy Analysis. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org

[Foe04] FoeBud – Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (2004) FoeBuD deckt auf: Versteckte RFID in Metro-Payback-Kundenkarte, www.foebud.org/texte/aktion/rfid

[HeM04] Henrici D, Müller P (2004) Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In: Ferscha A, Mattern F (Hrsg.) Proceedings of the 2nd International Conference on Pervasive Computing (Pervasive 2004). Springer-Verlag, LNCS 3001, pp 219-224

[InY03] Inoue S, Yasuura H (2003) RFID Privacy Using User-controllable Uniqueness. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org

[JuP03] Juels A, Pappu R (2003) Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In: Wright R (Hrsg.) 7th International Conference on Financial Cryptography (FC 2003), Guadeloupe, French West Indies, Springer-Verlag, LNCS 2742

[JRS03] Juels A, Rivest RL, Szydlo M (2003). The Blocker Tag: Selective Blocking of RFID-Tags for Consumer Privacy, www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker

[Küg05] Kügler D (2005) Risiko Reisepass. c't, (3): 84–89

[Lan01] Langheinrich M (2001) Privacy by Design: Principles of Privacy-Aware Ubiquitous Systems. In: Abowd GD, Brumitt B, Shafer S (Hrsg.) Proceedings of Ubicomp 2001. Springer-Verlag, LNCS 2201, pp 273-291

[Lau03] Laurant C (2003) Privacy and Human Rights 2003. Privacy International, London, UK, www.privacyinternational.org/survey/phr2003

[LLS00] Law C, Lee K, Siu KY (2000) Efficient Memoryless Protocol for Tag Identification. Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, pp 75-84. Boston, USA, http://portal.acm.org/citation.cfm?id=345865&dl=ACM&coll=portal

[Les99] Lessig L (1999) Code and Other Laws of Cyberspace. Basic Books, New York

[Let04] Lettice J (2004) EU biometric RFID scheme unworkable, says EU tech report. The Register, December 23, www.theregister.co.uk/2004/12/23/eu_rfid_visa_trashes_self/

[Loy04] Loyalty Partner GmbH (2004) PAYBACK Bonusprogramm und Loyalty Partner, www.payback.de

[Luc99] Lucky RW (1999) IEEE Reflections Column: Connections. IEEE Spectrum 36(3), www.boblucky.com/spectrum.htm

[Mar03] Mara J (2003) Euro Scheme Makes Money Talk. Wired News, 9. Juli 2003, www.wired.com/news/privacy/0,1848,59565,00.html

[May98] Mayer-Schönberger V (1998) Generational Development of Data Protection in Europe. In: Agre PE, Rotenberg M (Hrsg.) Technology and Privacy: The New Landscape. MIT Press, Cambridge, USA, pp 219-242

[NCR03] NCR (2003) Will RFID Automate the Point of Sale? NCR Provides Systems to Test Wireless Tags at Checkout, www.ncr.com/media_information/2003/sep/pr091203.htm

[NTR03] NTRU Cryptosystems Inc. (2003) GenuID. www.ntru.com/products/genuid.htm

[OSK03] Ohkubo M, Suzuki K, Kinoshita S (2003) Cryptographic Approach to „Privacy-Friendly“ Tags. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, USA, www.rfidprivacy.org

[OEC80] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2004) Organization for Economic Co-operation and Development (OECD). Deutsche Übersetzung unter www.datenschutz-berlin.de/gesetze/internat/bde.htm

[Pou04] Poulsen K (2004) EU goes on biometric LSD trip. The Register, 3. Februar 2004, www.theregister.co.uk/2005/02/03/biometric_lsd_trip/

[PRC04] Privacy Rights Clearinghouse (2004) A Review of the Fair Information Principles: The Foundation of Privacy Public Policy, www.privacyrights.org/ar/fairinfo.htm

[Rei01] Reissenberger M (2001) 50 Jahre Bundesverfassungsgericht: Volkszählung. DeutschlandRadio, Sendung vom 4. Januar 2004, www.dradio.de/homepage/schwerpunkt-verfassungsgericht-010904.html

[Rel81] Relfe MS (1981) When Money Fails. League of Prayer, Montgomery, USA

[RFI03] RFID Journal (2003) NCR Prototype Kiosk Kills RFID-Tags, 25. September 2003, ww.rfidjournal.com/article/view/585

[Rös01] Rössler B (2001): Der Wert des Privaten. Suhrkamp Verlag, Frankfurt/Main

[Rös02] Rössler B (2002) Den Wert des Privaten ergründen. digma: Zeitschrift für Datenrecht und Informationssicherheit 2(3): 106-113

[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

[Sch04] Schneier B (2004) RFID Passports, Schneier on Security Weblog, 4. Oktober 2004, www.schneier.com/blog/archives/2004/10/rfid_passports.html

[Sha03] Shabi R (2003) The Card Up Their Sleeve. The Guardian, 19. Juli 2003, www.guardian.co.uk/weekend/story/0,3605,999866,00.html

[SoR03] Solove DJ, Rotenberg M (2003) Information Privacy Law. Aspen Publishers, New York

[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

[Vog02] Vogt H (2002) Efficient Object Identification With Passive RFID Tags. In: Mattern F, Nagshineh M (Hrsg.) Proceedings of the 1st International Conference on Pervasive Computing (Pervasive 2002). Springer-Verlag, LNCS 2414, pp 98-113

[WaB90] Warren S, Brandeis L (1890) The Right to Privacy. Harvard Law Review 4(193)

[Wei03] Weis SA (2003) Security and Privacy in Radio-Frequency Identification Devices. Masters Thesis, Massachusetts Institute of Technology, Cambridge, USA, Mai 2003, http://theory.lcs.mit.edu/~sweis

[WSR03] Weis SA, Sarma SE, Rivest RL, Engels DW (2003) Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. 1st International Conference on Security in Pervasive Computing, Boppard, März 2003. Springer-Verlag, LNCS 2802, pp 201-212

[Wes67] Westin, A (1967) Privacy and Freedom. Atheneum, New York

[Yos01] Yoshida J (2001) Euro Bank Notes to Embed RFID Chips by 2005. EETimes, 19. Dezember 2001, www.eetimes.com/story/OEG20011219S0016

[Zei04] Zeidler M (2004) RFID: Der Schnüffel-Chip im Joghurtbecher. Westdeutscher Rundfunk, Köln, 8. Januar 2004, www.wdr.de/tv/monitor/beitrag.phtml? bid=554& sid=108