

FoeBuD e.V.

Marktstraße 18, 33602 Bielefeld

Tel: 0521-175254 • Fax: 0521-61172 • eMail: presse@foebud.org

www.foebud.org // www.bigbrotherawards.de



Presseerklärung des FoeBuD e.V.

In dem beiliegenden Positionspapier von internationalen Verbraucherschutz- und Bürgerrechtsorganisationen werden die Gefahren für Privatsphäre und Bürgerrechte erläutert, die durch RFID-Etiketten (Transponder) auf und in Waren entstehen können. Das Positionspapier fordert ein Moratorium der RFID-Hersteller und der Handelsketten, bis geeignete Maßnahmen erarbeitet worden sind, um diesen Gefahren wirksam zu begegnen.

Der FoeBuD e.V., bekannt durch die Organisation der jährlichen Big Brother Awards in Deutschland, gehört zu den Unterzeichnern dieses Aufrufs. Der diesjährige BigBrotherAward in der Kategorie „Verbraucherschutz“ ging an die Metro Future Store Initiative, die RFID-Technik propagiert. Der FoeBuD e.V. ist Gewinner des mit 15.000 Euro dotierten Ideenwettbewerbs der Stiftung Bridge. Mit dem Preisgeld soll ein Gerät entwickelt werden, das versteckte RFID oder RFID-Scanner anzeigt.

Positionspapier über den Gebrauch von RFID auf und in Konsumgütern

14. November 2003 // 19. November 2003

Herausgegeben von:

Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)
Electronic Privacy Information Center (EPIC)
Privacy Rights Clearinghouse
Junkbusters
American Civil Liberties Union (ACLU)
Meyda Online
Electronic Frontier Foundation (EFF)
PrivacyActivism

Unterstützt von:

American Council on Consumer Awareness, Inc.
Foundation for Information Policy Research
Austrian Association for Internet Users
Simson Garfinkel, Author, Database Nation
British Columbia Civil Liberties Association
Edward Hasbrouck, Author, The Practical Nomad
Canadian Internet Policy and Public Interest Clinic (CIPPIC)
Massachusetts Consumers' Coalition
Center for Democracy and Technology (CDT)
National Association of Consumer Agency Associates (NACAA)
Citizens' Council on Health Care
Option Consommateurs
Computer Professionals for Social Responsibility
Privacy International
Consumer Action
Privacy Times
Consumer Assistance Council
Private Citizen, Inc.
Consumer Project on Technology
Privaterra
Electronic Frontier Canada
Virginia Rezmierski, Ph.D. Ann Arbor, Michigan
Electronic Frontier Finland
World Privacy Forum
European Digital Rights
FoeBuD e.V., Big Brother Awards Germany
und weitere



Einführung

Radio Frequency Identification (RFID) ist eine Warenmarkierungstechnologie mit gravierenden gesellschaftlichen Folgen. Wenn sie missbräuchlich genutzt werden, haben RFIDs ein großes Potential zur Gefährdung der Privatsphäre von Konsumenten, zur Verringerung oder bis hin zum Verlust der Käuferanonymität und zur Bedrohung bürgerlicher Freiheiten.

Als Organisationen und Einzelpersonen, die sich dem Schutz von Privatsphäre und Bürgerrechten verschrieben haben, haben wir uns abgestimmt, um dieses Statement über die Anwendung von RFIDs im Konsumentenumfeld herauszugeben. Auf den folgenden Seiten beschreiben wir die Technologie und ihre Anwendungsmöglichkeiten, benennen die Risiken und besprechen mögliche politische Reaktionen, mit denen die angesprochenen Probleme vermieden oder verringert werden können.

RFID-Etiketten sind winzige Computerchips mit Miniantennen, die an physischen Objekten angebracht werden können. Bei den am meisten beworbenen Anwendungen von RFIDs enthält der Mikrochip einen elektronischen Produktcode (Electronic Product Code, EPC), der lang genug ist, jedes weltweit hergestellte Produkt eindeutig zu identifizieren. Wenn ein RFID-Lesegerät ein Funksignal abgibt, antworten in der Nähe befindliche Chips, indem sie die auf ihnen gespeicherten Daten an das Lesegerät übermitteln. Bei passiven (batterielosen) RFID-Etiketten kann die Leseentfernung von ca. einem Zentimeter bis ungefähr fünf oder zehn Meter variieren, während aktive, mit einer eigenen Energiequelle ausgerüstete Etiketten eine weit größere Leseentfernung haben können. Typischerweise werden die Daten an ein System von vernetzten Computern gesandt, die zum Beispiel im Management von Versorgungsketten oder bei der Inventarkontrolle eines Lagers eingesetzt werden.

GEFAHREN FÜR PRIVATSPHÄRE UND BÜRGERRECHTE

Obwohl es sinnvolle Einsatzmöglichkeiten für RFID gibt, können Eigenschaften dieser Technologie so genutzt werden, daß Privatsphäre, Bürgerrechte und Datenschutz gefährdet sind.

- **Versteckte Anbringung von Etiketten:** RFID-Etiketten können in oder an Objekten und Dokumenten angebracht werden, ohne dass die Person, die diese Objekte erwirbt, davon Kenntnis hat oder erhält. Da Funkwellen ganz leicht und geräuschlos durch Gewebe, Plastik und andere Materialien dringen können, ist es möglich, RFID-Etiketten auszulesen, die in die Kleidung eingenäht oder auf Objekten angebracht sind, die sich in Geldbörsen und Brieftaschen befinden, in Einkaufstaschen, Koffern und anderes mehr.
- **Einzigartige Identifikationsmerkmale für alle Objekte weltweit:** Der elektronische Produktcode ermöglicht es potentiell, dass jeder einzelne Gegenstand auf der Erde seine eigene, einzigartige ID bekommt. Der Gebrauch von einzigartigen ID-Nummern könnte zur Errichtung eines globalen Registrierungssystems führen, in dem jedes physische Objekt identifiziert und



auf seinen Käufer oder Besitzer zum Zeitpunkt eines Kaufs oder einer Übergabe zurückgeführt werden kann.

- **Massenhafte Datenzusammenführung:** Der Einsatz von RFID erfordert die Errichtung riesiger Datenbanken, die die individuellen, einzigartigen Daten eines Etiketts enthalten. Diese Datensammlungen könnten verbunden werden mit Personenidentifikationsdaten, insbesondere mit den immer weiter steigenden Speicherkapazitäten und Prozessorleistungen.
- **Versteckte Lesegeräte:** Die Etiketten können aus einiger Entfernung ausgelesen werden, auch durch Sichtbarrieren hindurch, und von Lesegeräten, die unsichtbar in nahezu jeder Umgebung, in der menschliche Wesen oder irgendwelche Gegenstände versammelt sind, angebracht werden können. Man hat schon testweise RFID-Lesegeräte in Fußbodenbretter eingebaut, in Teppiche und Bodenmatten eingewebt, in Türrahmen versteckt und nahtlos an Einzelhandelsregalen und Schaltern angebracht, womit es für den Verbraucher nahezu unmöglich wurde, zu erfahren, wann oder ob er oder sie „gescannt“ wurde.
- **Individuelle Verfolgung und Profilierung:** Wenn persönliche Identität mit einer eindeutigen RFID-Etikettennummer verbunden würde, könnten Personen verfolgt und Bewegungs- und andere Profile von ihnen erstellt werden, ohne dass die Individuen davon wissen oder ihre Zustimmung dazu gegeben haben. Zum Beispiel könnte ein RFID-Etikett, das an einem Schuh angebracht ist, de facto als ein Identifikator der Person dienen, die diesen Schuh trägt. Selbst wenn die Identifikation auf Objekt- oder Produkt-Niveau beschränkt bleibt, könnte die Identifikation eines Gegenstands, den jemand an hat oder bei sich trägt, ihn zum Beispiel mit speziellen Ereignissen wie etwa Demonstrationen in Verbindung bringen.

LEITLINIEN FÜR RECHTE UND PFLICHTEN IM ZUSAMMENHANG MIT RFID

Diese Leitlinien berücksichtigen das wirtschaftliche Interesse an der Zurückverfolgung von Objekten innerhalb der Logistikkette, betonen aber das Recht des Individuums darauf, nicht in den Geschäften und nach dem Kauf eines Gegenstands weiter verfolgt zu werden. Um die potentiellen Gefahren von RFID für die Bürger und die Gesellschaft auf ein Minimum zu reduzieren, empfehlen wir drei Leitlinien. Erstens muss RFID einer formellen technologischen Untersuchung und Bewertung unterworfen werden. RFID-Etiketten sollen nicht an einzelnen Konsumgütern angebracht werden, bevor so eine Beurteilung durchgeführt worden ist. Zweitens muss die Anwendung von RFID von einem Prinzip der fairen Informationspraxis geleitet sein. Drittens sollten bestimmte Anwendungsmöglichkeiten von RFID gesetzlich verboten werden.

Technikfolgenabschätzung: RFID muss einem formellen Technologiebeurteilungsprozess unterworfen werden, der von einer neutralen Instanz geleitet wird, vielleicht ähnlich dem Modell, das durch die jetzt nicht mehr existente Abteilung für Technologiebeurteilung des US-amerikanischen Parlaments (Congressional Office of Technology Assessment) etabliert wurde. Dieser Prozess



muss multidisziplinär sein und es müssen alle Interessengruppen beteiligt sein, eingeschlossen die Verbraucher.

Prinzip der fairen Informationspraxis: RFID-Technologie und ihre Anwendung müssen geleitet sein von strengen Prinzipien fairer Informationspraxis (Principles of Fair Information Practice, FIPs). Die achteiligen *Privacy*-Richtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) geben ein brauchbares Modell vor (www.oecd.org). Wir stimmen darin überein, dass die folgenden Minimalrichtlinien, die teilweise auf diesen Prinzipien basieren, befolgt werden müssen, während die weitergreifende Beurteilung der gesellschaftlichen Implikationen von RFID durchgeführt wird:

- **Offenheit oder Transparenz:** Anwender von RFID müssen ihre Grundsätze und Praktiken, bei Nutzung und Instandhaltung von RFID-Systemen, veröffentlichen, und es darf keine geheimen Datenbanken geben. Der einzelne Bürger hat das Recht zu erfahren, ob Produkte oder sonstige Gegenstände im Umfeld des Handels RFID-Etiketten oder Lesegeräte tragen. Er hat ebenso das Recht, die technischen Spezifikationen von Etiketten oder Geräten zu erfahren. Eine Etikettierung muss deutlich und leicht verständlich angezeigt werden. Jegliches Auslesen von Etiketten, das im Bereich des Handels erfolgt, muss allen Beteiligten transparent sein. Es darf kein geheimes Auslesen von Etiketten geben.
- **Zweckangabe:** Anwender von RFID müssen die Zwecke angeben, wegen derer Etiketten und Lesegeräte eingesetzt werden.
- **Sammelbegrenzung:** Die Sammlung von Informationen soll begrenzt sein auf die Daten, die für den jeweiligen Zweck notwendig sind.
- **Verantwortung:** RFID-Anwender sind verantwortlich für den Einsatz dieser Technologie und die damit verbundenen Daten. RFID-Anwender sollen gesetzlich darauf verpflichtet werden, dass sie die Prinzipien befolgen. Dazu muss ein Verpflichtungs-Mechanismus errichtet werden. Es muss sowohl bei der Regierung als auch bei der Industrie Abteilungen geben, an die Bürgerinnen und Bürger appellieren können, wenn diese Vorgaben verletzt worden sind.
- **Sicherheitsstandards:** Es muss Sicherheit und Integrität bestehen bei der Übermittlung, bei den Datenbanken und in Bezug auf den Systemzugriff. Eine Sicherheitsbeurteilung soll durch eine neutrale Instanz erfolgen und die Ergebnisse öffentlich bekannt gegeben werden.

RFID-Anwendungen, die gesetzlich verboten sein müssen:

- Händlern muss es verboten sein, ihre Kunden zum Akzeptieren aktiver oder "schlafender" RFID-Etiketten in den Produkten, die sie kaufen, zu zwingen oder zu drängen.
- Es darf kein Verbot für Bürger geben, nach RFID-Etiketten und Lesegeräten zu suchen und RFID-Etiketten auf Gegenständen in ihrem Besitz außer Funktion zu setzen.



- RFID darf nicht zur Verfolgung von Bürgern benutzt werden ohne ausdrückliche schriftliche Zustimmung des betroffenen Subjekts. Rückverfolgung von Menschen ist unzulässig, sei es direkte oder indirekte Verfolgung, durch Kleidung, Konsumgüter oder andere Gegenstände.
- RFID darf nie in einer Weise eingesetzt werden, die es erlaubt, Anonymität zu verringern oder zu verhindern. Zum Beispiel darf RFID nicht an Geldscheinen oder Münzen angebracht werden.

AKZEPTABLER GEBRAUCH VON RFID

Wir haben mehrere Beispiele "akzeptabler" Anwendungen von RFID zusammengetragen, bei denen Konsumenten und Bürger nicht „aktiven“ RFID-Etiketten und den daraus resultierenden Risiken ausgesetzt sind.

- Rückverfolgung von Medikamenten vom Punkt der Herstellung bis zum Punkt der Ausgabe: RFID-Etiketten könnten helfen sicherzustellen, dass diese wichtigen Produkte keine Fälschungen sind, dass mit ihnen sachgemäß umgegangen wird und dass sie korrekt ausgegeben werden. RFID-Etiketten, die auf oder in Medikamentenbehältern enthalten sind, sollen physisch entfernt und dauerhaft außer Funktion gesetzt werden, bevor sie an Verbraucherinnen oder Verbraucher verkauft werden.
- Rückverfolgung von industriell hergestellten Gütern vom Punkt der Herstellung bis zu dem Ort, an dem sie zum Verkauf in die Regale gestellt werden: RFID-Etiketten können dabei helfen, sicherzustellen, dass Produkte nicht verloren gehen oder gestohlen werden, während sie die Lieferkette durchlaufen. Die Etiketten können auch sicherstellen, dass die Waren sachgemäß behandelt werden. Die Etiketten sollen ausschließlich außen an den Produktverpackungen angebracht (nicht in die Verpackung integriert) und dauerhaft zerstört werden, bevor Verbraucherinnen und Verbraucher mit ihnen in Geschäften in Kontakt kommen.
- Auffindung von Gegenständen, die toxische Substanzen enthalten, wenn sie bei der Mülldeponie angeliefert werden: Wenn zum Beispiel ein PC zu einer Mülldeponie gebracht wird, kann ein Kurzstanz-RFID-Etikett die Existenz giftiger Inhaltsstoffe an ein Lesegerät bei der Deponie übermitteln. Es ist wichtig zu unterstreichen, dass Anwendungen wie in diesem Mülldeponie-Beispiel keine individuelle Produktidentifikation erfordern und auch nicht beinhalten dürfen. Das RFID-Etikett soll vielmehr ein allgemeines Signal für das Recycling oder die Abfallvernichtung aussenden.

SCHLUSSFOLGERUNGEN

Wir fordern Hersteller und Händler auf, sich auf ein freiwilliges Moratorium bezüglich des Einsatzes von RFID-Etikettierung von Konsumgütern zu einigen, bis ein formeller technologischer Beurteilungsprozess stattfinden kann, an dem alle Interessengruppen beteiligt sind, einschließlich der Verbraucher. Darüber hinaus muss die Entwicklung dieser Technologie geleitet sein von einer Reihe strenger Prinzipien der fairen Informationspraxis, die sicherstellen, dass sinnvolle



Kontrollmöglichkeiten für die Konsumenten in die Anwendung von RFID eingebaut sind. Schließlich sind einige Anwendungsmöglichkeiten von RFID für eine freie Gesellschaftsordnung inakzeptabel und sollten ausdrücklich gesetzlich verboten werden. Öffentlichkeit und Gesellschaft sollten nicht auf eine durch RFID ausgelöste Krise warten, bis Kontrollen eingeführt werden.

Obwohl darauf in diesem Positionspapier nicht eingegangen wird, müssen wir uns auch mit den Folgen für die Bürgerrechte beschäftigen, die von einer regierungsseitigen Anwendung von RFID ausgeht. Das US-amerikanische Verteidigungsministerium hat ein RFID-Mandat an seine Zulieferer ausgegeben, Schulen und Bibliotheken in den USA haben angefangen, RFID einzusetzen, die EU und die japanische Regierung haben schon über den Einbau von RFID in ihre Zahlungsmittel nachgedacht, und die britischen Strafverfolgungsbehörden haben Interesse an RFID als Werkzeug der polizeilichen Ermittlung angemeldet. Als eine offene demokratische Gesellschaft müssen wir einen strengen Regelkatalog etablieren, der auf den Prinzipien fairer Informationspraxis beruht, um die Anwendung von RFID durch Regierungen zu leiten.

Unterzeichnende

- Katherine Albrecht, Director, CASPIAN, www.spychips.org
- Media Inquiries: (877) 287-5854, kma@nocards.org
- Liz McIntyre, Director of Communications, CASPIAN, www.nocards.org
- Media Inquiries: (877) 287-5854, liz@nocards.org
- Beth Givens, Director, Privacy Rights Clearinghouse, www.privacyrights.org
- Media Inquiries: (619) 298-3396, bgivens@privacyrights.org
- Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation, www.eff.org
- Media Inquiries: (415) 436-9333 x 102, tien@eff.org
- Barry Steinhardt, Director of the Technology and Liberty Program, American Civil Liberties Union (ACLU), www.aclu.org
- Kenneth J. Benner, President, American Council on Consumer Awareness, Inc., accous@aol.com
- Peter Kuhm, Director, Austrian Association for Internet Users, www.vibe.at
- Deutsche Vereinigung für Datenschutz (DVD), www.aktiv.org/DVD/
- Murray Mollard, Executive Director, British Columbia Civil Liberties Association, www.bccla.org
- Philippa Lawson, Executive Director, Canadian Internet Policy and Public Interest Clinic (CIPPIC), www.cippic.ca
- Paula Bruening, Staff Counsel, Center for Democracy and Technology, www.cdt.org
- Twila Brase, RN, President, Citizens' Council on Health Care, www.cchconline.org
- Susan Evoy, Managing Director, Computer Professionals for Social Responsibility, www.cpsr.org
- Ken McElDowney, Executive Director, Consumer Action, www.consumer-action.org
- Paul Schrader, Executive Director, Consumer Assistance Council, www.consumercouncil.com
- James Love, Director, Consumer Project on Technology, www.cptech.org
- Richard S. Rosenberg, Vice-president, Electronic Frontier Canada, www.efc.ca
- Ville Oksanen, Vice Chairman, Electronic Frontier Finland, www.EFFI.org
- Chris Hoofnagle, Associate Director, Electronic Privacy Information Center (EPIC), www.epic.org
- Maurice Wessling, President, European Digital Rights, www.edri.org
- Rena Tangens & padeluun, FoeBuD e.V., Big Brother Awards Germany, www.foebud.org, www.bigbrotherawards.de
- Ian Brown, Director, Foundation for Information Policy Research, www.fipr.org



- Simson Garfinkel, Author, Database Nation
- Edward Hasbrouck, Author, The Practical Nomad, travel writer and consumer advocate www.hasbrouck.org
- Jason Catlett, President and Founder, Junkbusters Corp., www.junkbusters.com
- Paul J. Schlaver, Chair, Massachusetts Consumers' Coalition, www.massconsumers.org
- Jonathan D. Abolins, Author, "Meyda Online: Info Security, Privacy, and Liberties Studies," www.meydaonline.com
- Kathleen Thuner, President, National Association of Consumer Agency Associates (NACAA), www.nacaanet.org
- Jacques St Amant, Privacy Analyst, Option Consommateurs, www.option-consommateurs.org
- Deborah Pierce, Executive Director, PrivacyActivism, www.privacyactivism.org
- Simon Davies, Director, Privacy International, www.privacyinternational.org
- Evan Hendricks, Editor, Privacy Times, www.privacytimes.com
- Robert Bulmash, President & Founder, Private Citizen, Inc., www.privatecitizen.com
- Robert Guerra, Managing Director, Privatererra, www.privatererra.org
- Virginia Rezmierski, Ph.D., Ann Arbor, Michigan
- Pam Dixon, Executive Director, World Privacy Forum, www.worldprivacyforum.org
- Pam Dixon, Executive Director, World Privacy Forum, www.worldprivacyforum.org

Das Original ist unter www.spychips.com und www.privacyrights.org einzusehen.

http://www.spychips.com/jointrfid_position_paper.htm

<http://www.privacyrights.org/ar/RFIDposition.htm>



RFID Positionspapier, 1. Anlage

Grenzen der RFID-Technologie? Mythen werden entlarvt.

Die folgenden technischen Grenzen von RFID sind als Gründe ins Gespräch gebracht worden, warum sich Verbraucher zum jetzigen Zeitpunkt keine Sorgen über den Einsatz von FRID zu machen bräuchten. Wir betrachten jede scheinbare Grenze einzeln und erklären, warum diese Beschränkungen nicht als verlässlicher Schutz der Verbraucher gegen die oben beschriebenen Risiken angesehen werden können.

1. Leseentfernungen reichen für Konsumentenüberwachung nicht aus

RFID-Etiketten haben verschiedene Entfernungen, in denen sie ausgelesen werden können, abhängig von der Größe ihrer Antenne, ihrer Sendefrequenz und davon, ob sie eine eigene Energieversorgung (aktiv) haben oder nicht (passiv). Manche passiven RFID-Etiketten haben eine maximale Leseentfernung von weniger als 2 cm. Andere passive RFID-Etiketten können noch aus Entfernungen von 5 Metern oder mehr ausgelesen werden. Aktive RFID-Etiketten haben theoretisch sehr große Leseentfernungen. Zur Zeit sind die meisten RFID-Etiketten, die bei Konsumgütern zum Einsatz kommen sollen, passiv und können auf eine Entfernung von maximal 1,5 Metern ausgelesen werden.

Entgegen einiger Beteuerungen sind Etiketten mit niedriger Leseentfernung nicht notwendigerweise weniger effektiv bei der Verfolgung von Menschen oder mit ihnen verbundenen Gegenständen. Tatsächlich kann eine kürzere Lesedistanz in einigen Fällen sogar effektiver sein. Wenn es zum Beispiel ein Interesse daran gibt, Individuen durch ihre Schuhe zu identifizieren, wenn sie in den Bereich eines im Fußboden eingebauten Lesegeräts kommen, wäre eine Distanz von 2–3 Zentimetern einer Distanz von einem halben bis einem Meter vorzuziehen. Solche Auslesung auf kurze Distanz würde Interferenzen durch andere in der Nähe befindliche Etiketten minimieren und es ermöglichen, dass wirklich nur das Etikett, das sich direkt am Lesegerät befindet, erfasst wird.

2. Lesegeräte sind nicht weit genug verbreitet, um nahtlose Verfolgung von Menschen zu ermöglichen

Die Entwickler von RFID-Technologie haben eine Welt vor Augen, in der RFID-Lesegeräte ein „umfassendes globales Netzwerk“ aufbauen. Es bedarf keines allumfassenden Geräte-Netzwerks, um Objekte oder die Menschen, die mit ihnen zu tun haben, zu verfolgen. Zum Beispiel können Autos auf einer Autobahn verfolgt werden, ohne dass alle paar Meter ein RFID-Lesegerät angebracht wird. Sie brauchen nur jeweils an den Auf- und Abfahrten installiert zu werden. In gleicher Weise ist es nicht notwendig, in den Städten alle 3 Meter ein Lesegerät zu positionieren, um eine Person zu verfolgen, solange Lesegeräte an strategischen Punkten angebracht sind, wie zum Beispiel Hauseingängen.

3. Begrenzte Informationsmengen auf den Etiketten



Manche RFID-Befürworter verteidigen diese Technologie mit dem Hinweis, dass die Etiketten auf den meisten Konsumgütern nur eine Seriennummer beinhalten werden. Diese Nummer kann allerdings als eine Referenznummer genutzt werden, die mit Informationen auf einer oder mehreren vernetzten Datenbanken korrespondiert. Das bedeutet, dass die Datenmenge, die mit dieser Nummer in Verbindung gebracht werden kann, theoretisch unbegrenzt ist und aufgefüllt und vervollständigt werden kann, sobald neue Informationen gesammelt wurden.

Wenn ein Verbraucher zum Beispiel ein Produkt kauft, das ein RFID-Etikett mit einer standardisierten Warennummer enthält, könnten Informationen über den Verbraucher, der es gekauft hat, dieser Datenbank automatisch hinzugefügt werden. Weitere Informationen können in die Datei eingetragen werden, während der Konsument seiner Arbeit nachgeht. „Betritt Gerichtsgebäude in Atlanta um 12:32 mittags“, „Auf einer ‚Mobil‘-Tankstelle um 14:14“, und so weiter. Solche Daten sind für jeden verfügbar, der Zugriff auf so eine Datenbank hat, ob er nun dazu autorisiert oder auch nicht.

4. Passive Etiketten können nicht durch Satelliten geortet werden

Die passiven RFID-Etiketten, die man sich für die Kennzeichnung der meisten Konsumgüter vorstellt, haben keine eigene Energieversorgung, das heißt, dass sie erst aktiviert und von in der Nähe befindlichen Leseapparaten kontaktiert werden müssen. Daher haben passive Etiketten selbst keine Möglichkeit, mit und durch Satelliten zu kommunizieren.

Die Informationen, die ein passives RFID-Etikett trägt, können aber von in der Nähe befindlichen Lesegeräten aufgenommen werden, die dann ihrerseits ihre Anwesenheit und Position an Satelliten senden können. Diese Technologie ist schon benutzt worden, um in Echtzeit eine Ortung von Gütern vorzunehmen, die auf bewegten Fahrzeugen durch die nordamerikanischen Versorgungswege transportiert wurden.

Außerdem können aktive RFID-Etiketten, die eine eigene Energieversorgung besitzen, für den direkten Satellitenkontakt ausgerüstet werden. Zum jetzigen Zeitpunkt sind solche Etiketten viel zu teuer, um sie auf den meisten Konsumgütern anzubringen, aber diese Nutzung ist nicht unvorstellbar, wenn man im Auge behält, dass die Technologie sich weiterentwickelt und die Preise fallen.

5. Hohe Kosten der Etiketten verbieten weitverbreitete Anwendung

RFID-Entwickler weisen auf die „hohen Kosten“ von RFID-Etiketten hin, um auf diese Weise die Befürchtungen von Konsumenten bezüglich der Fähigkeiten dieser Etiketten zu lindern. Wenn allerdings die Technologie sich weiter entwickelt und die Preise fallen, sagen wir voraus, dass mehr und mehr Konsumgüter Etiketten tragen werden und dass diese Etiketten kleiner werden und leistungsfähiger. Wir sagen voraus, dass die Entwicklung den Trends anderer technischer Produkte wie Computer oder Taschenrechner folgen wird.



RFID Positionspapier, 2. Anlage

Eine Kritik der von der Industrie vorgeschlagenen Lösungen

Die RFID-Industrie hat eine Reihe von Vorschlägen gemacht, um den Gefahren zu begegnen, die von der RFID-Etikettierung von Konsumgütern ausgehen. Darunter gibt es Ideen wie die Zerstörung der Etiketten zum Verkaufszeitpunkt, der Gebrauch von „Blocker-Etiketten“, sowie das „Geschlossene System (closed system)“. Wir kommentieren diese Strategien im folgenden.

Zerstörung der Etiketten beim Verkauf

Es wurde vorgeschlagen, dass man das Problem der RFID-Etiketten lösen könnte, indem man sie zum Zeitpunkt des Verkaufs einer Ware außer Funktion setzt. Es gibt verschiedene Gründe, warum wir nicht der Ansicht sind, dass allein diese Maßnahme die Privatsphäre von Konsumenten ausreichend schützen könnte.

Die Zerstörung von RFID-Etiketten nach dem Einkauf löst nicht das Problem der Verfolgung eines Kunden im Geschäft.

Bisher hat annähernd jede Verletzung der Privatsphäre, die mit RFID-Etikettierung von Konsumgütern verbunden war, im Bereich der Verkaufsräume stattgefunden, lange bevor die Konsumenten die Kassenschalter erreicht hatten, wo die Chips zerstört würden. Einige Beispiele:

- Es wurden Nahaufnahmen von Konsumenten gemacht, als sie RFID-etikettierte Gillette-Rasierklingen aus Ladenregalen nahmen, die mit einem „Auto-ID Center“ ausgerüstet waren — sogenannte „smart shelf technology“ („intelligentes Regal“). [1]
- Eine Videokamera, die auf ein Kosmetikregal in einem „Wal Mart“ in Oklahoma gerichtet war, ermöglichte es Managern von Procter & Gamble, Kunden ohne deren Wissen zu beobachten, während sie RFID-etikettierte Lippenstifte ausprobierten. [2]
- Es liegen Pläne vor, Bücher und Magazine mit RFID-Chips zu etikettieren, um Kunden beim Durchblättern detailliert beobachten zu können. [3] Diese Möglichkeit wurde kürzlich auf der Internationalen Buchmesse 2003 in Tokio demonstriert. Wir zitieren die japanischen Nikkei Electronic News: „Indem Etikettenlesegeräte auf den Regalen von Buchhandlungen angebracht werden, erlaubt das neue System es Buchhändlern, Informationen zu sammeln wie zum Beispiel die Bandbreite an Titeln, die ein Käufer durchgeblättert hat, wie oft ein bestimmter Titel angefasst wurde und sogar die Zeit, wie lange in jedem Buch herumgeblättert wurde.“

Wir erkennen das Bedürfnis der Händler an, Ladendiebstahl zu kontrollieren und allgemeine Beurteilungen zu erstellen, um z.B. Arbeitsabläufe zu verbessern. Doch eine detaillierte Überwachung und Aufnahme des Kundenverhaltens, sogar ohne deren Zustimmung, verstößt gegen die Prinzipien der fairen Informationspraxis.



Etiketten können nur scheinbar zerstört worden sein, während sie in Wirklichkeit nur "schlafen" und reaktiviert werden können.

Manche RFID-Etiketten besitzen einen „Schlummer-“ oder „Schlaf-Zustand“, der für den durchschnittlichen Konsumenten so aussieht, als sei das Etikett zerstört worden. Händlern und anderen könnten behaupten, sie hätten ein Etikett zerstört, während sie es in Wirklichkeit nur auf den „Schlaf-Modus“ gesetzt haben. Damit wäre es später möglich, ein „schlummerndes“ Etikett zu reaktivieren und auszulesen.

Die Option der Etiketten-Zerstörung könnte von Regierungsseite verhindert werden.

Es würde ein leichtes sein, wegen eines geringen Sicherheitsrisikos oder einer Änderung in der Regierungspolitik die Option der Zerstörung der Etiketten außer Kraft zu setzen. Wenn man zulässt, dass RFID-Etiketten überall in und auf Konsumgütern verwendet werden, könnte die Aussetzung einer Verpflichtung zum Zerstören der Etiketten direkt in einen Überwachungsstaat führen.

Der Einzelhandel könnte Hürden oder Anreize einführen, um Verbraucher von der Zerstörung von RFID-Etiketten abzuhalten.

Verbrauchern, die die Zerstörung der Etiketten wünschen, könnten zu diesem Zweck umständliche oder lästigen Verfahren auferlegt werden — wie zum Beispiel das Anstehen vor einem sogenannten „killer kiosk“ [4], also einem Extraschalter, wo die Etiketten zerstört werden. Es könnte weiter von ihnen verlangt werden, dass sie die Zerstörung selbst vornehmen müssen. Kunden, die sich dafür entscheiden, die Etiketten zu zerstören, erhalten möglicherweise nicht dieselben Rabatte oder Sonderangebote wie andere Kunden, oder ihnen werden nicht dieselben Umtauschkonditionen zugestanden. In vielen Bereichen der Privatgesetzgebung wird diesen Anreizen durch den Einzelhandel begegnet, und es gibt gesetzliche Verbote dagegen, die Kunden zur Aufgabe ihrer privaten Rechte zu verführen. [5]

Die Schaffung von zwei Klassen von Konsumenten

Wenn die Zerstörung von RFID-Etiketten eine bewusste Anstrengung auf Seiten des Konsumenten erfordert, werden viele davon keinen Gebrauch machen, sei es aus Furcht, Unwissenheit oder Zeitmangel. Viele werden sich dafür entscheiden, die Etiketten nicht zu zerstören, wenn dies unbequem ist. (In den momentan gängigen "killer kiosks" muss jedes Stück einzeln aufgelegt werden, ein langwieriger und zeitraubender Vorgang.) Dies würde zwei Klassen von Konsumenten hervorbringen, die einen, die sich „genug kümmern“, um RFID-Etiketten in ihren Waren zu zerstören, und die andern, die das nicht tun. Die Zugehörigkeit zu einer, egal welcher, dieser Gruppen könnte negative Folgen haben.

Blocker Tags

„RFID blocker tags“ sind elektronische Geräte, die die Übermittlung von allen oder einigen Informationen auf RFID-Etiketten stören sollen. So ein Blocker-Tag könnte in eine Einkaufstasche eingebaut sein, in eine Geldbörse, oder auch eine Armbanduhr, und wird dann in die Nähe von Etiketten gehalten, die Informationen enthalten, die der Kunde blockieren möchte. [6]

Blocker-Tags sind bisher nur Theorie



Soviel wir wissen, existieren Blocker-Tags noch nicht. Bis ein Blocker-Tag entwickelt und getestet worden ist, gibt es keine Möglichkeit zu wissen, wie effektiv er sein wird und ob er technisch außer Kraft gesetzt werden kann.

Blocker-Tags fördern den Einsatz von RFID-Etiketten

Ein Blocker-Tag könnte die Verbreitung der RFID-Technik befördern, indem er den Konsumenten ein falsches Gefühl von Sicherheit vermittelt. Während so eine Erfindung eine ziemlich geniale Idee ist, ist sie doch auch eine, deren Nutzung verboten oder mit zunehmender Trägheit vernachlässigt werden könnte. Es ist außerdem möglich, dass so ein elektronisches Gerät seinen Effekt verlieren könnte, sei es durch absichtliche Einwirkung oder weil es einfach aufhört zu funktionieren.

Blocker-Tags könnten verboten werden, durch Gesetze oder Geschäftspolitik des Handels

Die Konsumenten könnten das Recht zum Gebrauch des Blocker-Tags verlieren, wenn die Regierung annimmt, dass es für die nationale Sicherheit notwendig ist zu wissen, welche Kleidung die Leute tragen oder was sie sonst bei sich haben. Sie könnte die Geräte grundsätzlich verbieten oder einzelne Orte auswählen, wo sie nicht benutzt werden dürfen. Man kann sich zum Beispiel leicht ein Verbot solcher Apparate auf Flughäfen oder in öffentlichen Gebäuden vorstellen.

Einzelhandelsunternehmen könnten Blocker-Tags verbieten, wenn sie glauben, dass die Geräte dazu benutzt werden könnten, Sicherheitsmaßnahmen zu umgehen, oder wenn sie annehmen, dass Detailwissen über ihre Kunden für das Marketing wertvoll sind.

Wenn RFID-Etiketten erst einmal allgegenwärtig sind, würde ein generelles oder teilweises Verbot eines „Datenschutzgeräts“, z.B. eines Blocker-Tags die Konsumenten schutzlos dem Einbruch in ihre Privatsphäre aussetzen.

Blocker-Tags burden den Verbrauchern die Initiative auf

Ein Blocker-Tag verlagert die Last des Schutzes der Privatsphäre weg von den Herstellern und dem Handel, und legt sie auf die Schultern der Konsumenten. Außerdem könnten vielbeschäftigte Verbraucher einfach vergessen, das Blocker-Gerät mit sich zu führen oder es einzusetzen, besonders wenn es noch weiterer Handlungsschritte bedarf, um sie wirksam zu machen.

Blocker-Tags schützen Verbraucher nicht mehr, sobald die Produkte vom Blocker-Tag entfernt werden

Blocker-Tags funktionieren theoretisch nur dann, wenn sie in der Nähe der Gegenstände sind, die sie vor den RFID-Lesegeräten „verstecken“ sollen. Sobald Gegenstände sich außerhalb der Reichweite des Blockier-Geräts befinden, wären die Verbraucher schutzlos dem Eindringen in ihre Privatsphäre ausgesetzt. Eine Konsumentin könnte z.B. einen Pullover kaufen und glauben, dass die Information auf dem eingearbeiteten RFID-Etikett geschützt wäre, weil sie ihn in einer Einkaufstasche nach Hause trägt, die mit einem Blocker-Gerät ausgestattet ist. Sobald sie allerdings den Pullover aus der Tasche nimmt, ihn anzieht und in der Nähe einer Leseapparatur trägt, könnten Informationen aus dem Etikett gelesen werden.



Die Erschaffung von zwei Klassen von Konsumenten

Genau wie die Etikettenzerstörung wird ein Blocker-Tag wahrscheinlich zwei Klassen von Konsumenten schaffen: die einen, die Etiketten blockieren, und die, die das nicht tun.

Geschlossenes System

Industrievertreter argumentieren, dass RFID-Applikationen sich auf geschlossene Systeme beschränken könnten, dann wären die Daten nur für die, die sich innerhalb dieses Systems befinden, und für Leute mit einem Regierungsmandat zugänglich (vielleicht durch ein Gesetz wie der US-amerikanische *Communications Access to Law Enforcement Act*, CALEA). Damit, so sagen sie, wäre eine Profilerstellung und Verfolgung durch den gesamtgesellschaftlichen Raum unwahrscheinlich. Ein Beispiel für den schon stattfindenden Einsatz von RFID in geschlossenen Systemen ist die Nutzung in Bibliotheken. „Die Früchte des Zorns“ in Bibliothek X hat einen anderen Code als derselbe Titel in Bibliothek Y.

Obwohl RFID-Applikationen heute auf geschlossene Systeme beschränkt sind, wird es große Nachfrage nach standardisierter Etikettierung geben. Verleger zum Beispiel könnten eines Tages Bücher an Bibliotheken und Buchhandlungen ausliefern, die beschreibbare Etiketten haben. Jedes Exemplar von „Die Früchte des Zorns“ würde dann einen Teil seines Standard-Warencodes tragen, der derselbe ist wie der auf jedem anderen Exemplar. Die Bibliothek wird in der Lage sein, den restlichen Code anzupassen, so dass sie ihren eigenen Zwecken der Inventarkontrolle nachkommen kann.

Selbst wenn geschlossene Systeme geschlossen bleiben, macht ihr Mangel an Transparenz sie beunruhigend vom Standpunkt der Privatsphäre aus. Weil bestimmte Details über geschlossene Systeme möglicherweise nicht leicht erhältlich sind, hätten Konsumenten große Schwierigkeiten bei der Beschaffung der Informationen, die sie benötigen, um Gefährdungen ihrer Privatsphäre einschätzen und sich schützen zu können.

Schlussfolgerung

Wir erkennen an, dass die Industrie sich bemüht, die Sorgen um die Privatsphäre von Konsumenten und Bürgerrechte wahrzunehmen, die mit RFID-Technologie zu tun haben. Dennoch: Obwohl wir glauben, dass die vorgeschlagenen Lösungen im richtigen Geiste vorgetragen werden, bieten sie doch nur ungenügenden Schutz. Bis angemessene Lösungen entwickelt werden und man sich über sie geeinigt hat, glauben wir, dass es falsch ist, Konsumenten den Gefahren der RFID-Technologie durch Etikettierung auf dem Objekt-Niveau auszusetzen.

[1] Alorie Gilbert, "Cutting edge 'smart shelf' test ends." CNET News, August 22, 2003.

http://news.com.com/2100-1008_3-5067253.html

[2] Howard Wolinsky, "P&G, Wal-Mart store did secret test of RFID." The Chicago Sun Times, November 10, 2003.

<http://www.suntimes.com/output/lifestyles/cst-nws-spy09.html>



[3] Winston Chai, "Tags track Japanese shoppers." CNET News, May 8, 2003.

<http://news.zdnet.co.uk/business/0,39020645,2134438,00.htm>

[4] "NCR prototype kiosk kills RFID tags." RFID Journal, September 25, 2003.

<http://www.rfidjournal.com/article/articleview/585/1/1/>

[5] Vergleiche z.B.: California Senate Bill 27, Gesetz 1798.84 (a).

http://info.sen.ca.gov/pub/bill/sen/sb_0001-0050/sb_27_bill_20030430_amended_sen.html

[6] "RFID blocker tags developed." Silicon.com, August 28, 2003.

<http://www.silicon.com/software/applications/0,39024653,10005771,00.htm>