

# RFID vs. Privatsphäre – ein Widerspruch?

## Die Autoren

Oliver Günther  
Sarah Spiekermann

Prof. Oliver Günther, Ph. D.  
Dr. Sarah Spiekermann  
Humboldt-Universität zu Berlin  
Institut für Wirtschaftsinformatik  
Spandauer Straße 1  
10178 Berlin  
030 2093-5742  
{guenther | sspiek}@wiwi.hu-berlin.de

RFID – vor einem Jahr nur Spezialisten bekannt, neuerdings in aller Munde. Das Kürzel *RFID* steht für *Radio Frequency Identification*, eine Technik, die es erlaubt, ohne Sichtkontakt und über eine gewisse Distanz hinweg Objekte automatisch zu erfassen. Basis hierfür sind die so genannten *RFID-Tags*, zu deutsch *Funketiketten*, kleine Chips, die an Personen oder Gegenstände angeheftet werden und eine weltweit eindeutige Kennung, den *Electronic Product Code (EPC)*, nach außen kommunizieren können.

Nachdem die Technologie im Prinzip schon seit Mitte der 1960er Jahre bekannt ist und bereits in vielen Bereichen eingesetzt wird (z. B. bei Zugangskontrollen in Skigebieten oder in Bibliotheken), führen die stetig sinkenden Produktionskosten pro RFID-Tag neuerdings zu ganz neuen Anwendungsperspektiven. Während die Kosten pro *WORM-Chip* (*WORM = write-once-read-many*) derzeit in einer Größenordnung von 30 bis 50 Cents lie-

gen, sind Billigchips für 3 bis 5 Cents in den nächsten 5 Jahren wahrscheinlich. Damit wird es interessant, die Technologie auch auf Produktebene einzusetzen – der Handel plant die Einführung dieses so genannten *item-level tagging* bereits für 2006. Der wesentlich weniger flexible Barcode würde damit weitgehend überflüssig.

Die positiven Potenziale der RFID-Technologie sind offensichtlich; siehe hierzu auch den Artikel von Fleisch und Dierkes in *WIRTSCHAFTSINFORMATIK* 45 (2003) 6, S. 611–620. Für die Wertschöpfungskette, das weiß der Handel aus weitreichenden Feldversuchen, ergeben sich insbesondere durch die verbesserte Warensicherung und Warenverfügbarkeit beträchtliche Einsparungen. Marketing kann mit RFID-Daten stark segmentspezifisch erfolgen; so führten Tests der Firma Gap zur gezielten Bewerbung zu Umsatzsteigerungen um 15 Prozent. Des Weiteren erwartet man Effizienzgewinne *nach* dem Verkauf an den Endkunden – z. B. bei Reklamationen und beim Recycling – sowie beim Markenschutz.

Im Handel zeichnen sich aber auch ganz praktische Vorteile für den Kunden ab. So ist zum Beispiel denkbar, dass die Gewinne an Effizienz und Kontrolle innerhalb der Wertschöpfungskette in Kombination mit der branchentypischen intensiven Konkurrenz letztlich zu niedrigeren Preisen führen. Ferner ermöglichen es die RFID-Tags, den Verbraucher rechtzeitig auf einen eventuellen Beschaffungsbedarf hinzuweisen („intelligenter Kühlschrank“). Produktinformation – z. B. über den Einsatz von Gentechnik bei Lebensmitteln – lässt sich effizient vermitteln, und der Bezahlvorgang kann einfacher gestaltet werden. Kundenpräferenzen können mit dem Einverständnis des Kunden erfasst und zu Empfehlungen verarbeitet werden. Kurz gesagt: Einkaufen könnte schneller und bequemer werden.

Große Handelsunternehmen wie Metro oder Wal-Mart, aber auch staatliche Stellen wie das amerikanische Verteidigungsministerium haben die Potenziale der RFID-Technologie längst erkannt und arbeiten mit Hochdruck an diversen Anwendungen. Was den Handel angeht, so sind insbesondere auf der Zuliefererseite der Wertschöpfungskette wohl schon für das Jahr 2004 erste Maßnahmen zu erwarten. Mehrere Unternehmen denken daran, ihre Zulieferer mittelfristig zum Einsatz von RFID zu verpflichten – wobei es zunächst nicht um die Auszeichnung von einzelnen Gütern geht, aber immerhin um die Etikettierung von größeren Losgrößen wie Paletten und Gebinden.

Infolge dieser Entwicklungen ist die RFID-Technologie in starkem Maße in das öffentliche Bewusstsein gerückt – allerdings keineswegs nur aufgrund der beschriebenen Vorteile, sondern auch vor dem Hintergrund der potenziellen Gefahren für den Datenschutz. Erste Reaktionen der Öffentlichkeit auf den verstärkten Einsatz von Chiptechnologie in Ausweisen und Gütern lassen darauf schließen, dass diese Gefahren vom Verbraucher außerordentlich ernst genommen werden. So sprachen sich z. B. in einer Ende April 2004 durchgeführten Online-Umfrage der Rheinzeitung 57,4% der Teilnehmer dafür aus, man sollte die RFID-Technologie „komplett verbieten“. 26,5% schlossen sich dem Vorschlag an „Erst gesetzlich regeln – dann einführen“, und nur 16,1% der Teilnehmer fanden die Technologie „praktisch und wünschenswert“.

Und in der Tat, die Zuordnung von Personendaten zu Objektdaten kann signifikante Verletzungen der Privatsphäre zur Folge haben. Erste Anwendungen zum Zweck der Terroristenabwehr und der inneren Sicherheit seitens des Staates nähren solche Befürchtungen. So ist beispielsweise geplant, die Eintrittskarten für die Fußballweltmeisterschaft 2006 mit RFID-Tags zu

versehen. Ziel ist u. a., notorische Hooligans am Eingang zum Stadium automatisch zu registrieren und ggf. gesondert zu überwachen. Mehrere Länder erwägen den Einsatz von RFID in Ausweisdokumenten. Zukünftig wäre also denkbar, Spielplätze nicht mehr mit Videokameras zu überwachen, sondern gleich mit identifikationsgenauen Überwachungssystemen. Aber auch die absehbaren Einsatzmöglichkeiten im Handel führen zu Ängsten auf Seiten der Verbraucher. In der Presse finden sich zunehmend Szenarien, die auf Möglichkeiten zum unkontrollierten Auslesen von RFID-Daten verweisen und so Schreckensvisionen vom gläsernen Menschen eine neue Dimension verleihen. Warum sollte man seine Kunden nicht, wie etwa im Film „Minority Report“ dargestellt, persönlich begrüßen, wenn das Lesegerät am Ladeneingang die vor einiger Zeit dort erworbenen Schuhe erkennt? Amazon-Käufer werden im Internet schon heute aufgrund von Cookie-Daten persönlich begrüßt, was von den meisten Kunden positiv vermerkt wird. Ebenso denkbar wäre es, dass Einzelhändler die RFID-Daten nutzen, um die Finanzkraft vorbeilaufender Passanten zu ermitteln. Aus technischer Sicht ist dies alles ohne größere Probleme realisierbar.

Nun ruft die Vorstellung, dass sämtliche Gegenstände im persönlichen Umfeld unbemerkt identifiziert und lokalisiert werden, selbst beim abgebrühten Beobachter Unbehagen hervor. Wer wollte schon jederzeit anhand der von ihm mitgeführten Gegenstände von unbekanntem Dritten räumlich und zeitlich verfolgt werden können? Sollte es nicht, wie vom Bundesdatenschutzbeauftragten Peter Schaar kürzlich gefordert, einen „Aus-Schalter für RFID-Etiketten“ geben?

Als technische Antwort auf diese Bedenken ist in den vorliegenden Tag-Spezifikationen die Möglichkeit vorgesehen, den RFID-Tag mit dem Verkauf an den Endverbraucher zu invalidieren („Kill-Funktion“) (auch der hauseigene Mikrowellenherd ist hierfür ein probates Mittel). Damit büßt man jedoch die Vorteile ein, die RFID nach dem Verkauf auch für den Kunden offeriert. Eine mögliche Lösung dieses Dilemmas wäre ein passwortbasierter Schutz der RFID-Information, wodurch die Informationsnutzung vollständig vom Kunden kontrolliert werden könnte. Damit ließe sich nicht nur das Auslesen der EPC kontrollieren, sondern es ließe sich auch die Frage der Zugriffsrechte auf die mit der EPC befragbaren Datenbanken angehen. Nötig wäre hier ein Rollenkonzept, wonach die verfügbare Information von der

(passwortgeschützten) Rolle abhängt, die der Anfrager einnimmt. Insgesamt steht man mit der Entwicklung von derartigen *Privacy Enhancing Technologies (PETs)* für RFID jedoch noch am Anfang. Insbesondere die Nutzung von sicheren kryptographischen Verfahren stößt aufgrund des Kostendrucks für massenmarktfähige RFID-Tags schnell an Grenzen.

Parallel zu diesen überfälligen Arbeiten muss intensiver darüber nachgedacht werden, wie sich das positive Potenzial der RFID-Technologie mit den Ängsten und Präferenzen der Kunden in Einklang bringen lässt. Hier ist nicht nur der Gesetzgeber gefragt, welcher sich heute mit der Forderung nach Produktkennzeichnung konfrontiert sieht (RFID – der rote Punkt?). Auch die an RFID interessierten Industrien haben Anlass, sich mit den Ängsten ihrer Kunden auseinander zu setzen, und zwar unabhängig davon, inwieweit diese aus rationaler Sicht gerechtfertigt sind. Ein offensiver Umgang gerade auch mit den möglichen Gefahren der Technologie scheint der beste Weg, um die gewünschte Akzeptanz für einen regulierten Einsatz zu erzeugen. Mit dem „Kaputtreden“ einer Technologie hat dies nichts zu tun.

Gefragt ist an erster Stelle Aufklärung. Der Bürger muss in klarer und verständlicher Form darüber informiert werden, was mit RFID *technisch möglich* ist, was hiervon *legal* ist und welche *Vorkehrungen* getroffen wurden, um einem illegalen Einsatz der Technologie vorzubeugen. Des Weiteren ist es im Interesse aller Beteiligten, die Datenschutzpräferenzen der Kunden bzw. der Bürger weiter zu erkunden und diese in die Planung einfließen zu lassen. Dabei ist zu beachten, dass diese Datenschutzpräferenzen in besonderem Maße kontextabhängig sind. Firmenkunden werden andere Präferenzstrukturen als Indivi-

dualkunden haben, es gibt branchenspezifische Unterschiede, und schließlich sind Datenschutzfragen auch in extremem Maße kulturbedingt – man denke nur an die starken Unterschiede zwischen Deutschland und den USA in dieser Frage. Nur die technischen Rahmenbedingungen sind weltweit identisch. Kulturelle, ökonomische und juristische Aspekte sind demgegenüber in starkem Maße situationsabhängig.

Der notwendige Kompromiss zwischen dem technischen Potenzial der RFID-Technologie, den rechtlichen Rahmenbedingungen und den Datenschutzpräferenzen der Nutzer muss für jede konkrete Situation neu ausgehandelt werden. Zur Implementierung sollte stets eine Kombination von vertraglichen und technischen Maßnahmen in Betracht gezogen werden. Der Einsatz von ausschließlich vertraglichen Regelungen reicht in dem derzeitigen, von einem tief greifenden Misstrauen geprägten Klima oft nicht aus. Dass es im Regelfall Lösungen zum Nutzen *aller* Beteiligten gibt, vorausgesetzt sie beruhen auf klar definierten gesetzlichen und vertraglichen Vereinbarungen sowie verlässlichen Technologien, scheint uns wahrscheinlich. Wichtig ist allerdings ein behutsames Eingreifen der Legislative und Judikative, welche die technischen Innovationen sorgfältig verfolgen und prüfen müssen. Wissenschaft und Wirtschaft sind aufgerufen, den Entscheidungsprozess kompetent zu begleiten und zu unterstützen. Das von der Standardisierungseinrichtung EPCglobal (<http://www.epcglobalinc.org>) mitgetragene Independent Policy Advisory Council zur Diskussion von Datenschutzfragen im RFID-Kontext ist ein wichtiger Schritt in diese Richtung.

Prof. Oliver Günther, Ph. D.  
Dr. Sarah Spiekermann

## ■ In eigener Sache I

Die Herausgeber unserer Zeitschrift üben ihr Amt für eine begrenzte Zeit aus. Endet eine Mitgliedschaft im Herausgeberkreis, bestimmt das Gremium neue Mitglieder durch geheime Wahl. Wir begrüßen als neue Herausgeber Rudolf Bauer, IBM Deutschland GmbH, Stuttgart, sowie Dr. Peter Zencke, SAP AG, Walldorf, und freuen uns auf eine spannende und erfolgreiche gemeinsame Arbeit. Gleichzeitig danken wir Dr. Michael Teufel, RWE Systems AG, Essen, der aus dem Herausgebergremium ausgetreten ist, für die vertrauensvolle Zusammenarbeit.

Prof. Dr. Wolfgang König  
Geschäftsführender Herausgeber