epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

RFID Workshop Comment P049106

FTC Workshop on

Radio Frequency Identification: Applications and Implications for Consumers

June 21, 2004

Comments of the

ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

(July 9, 2004)

Cédric Laurant, Policy Counsel
Kenneth Farrall, IPIOP Law Clerk

TABLE OF CONTENTS

Introduction

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy. EPIC supports the Federal Trade Commission's (FTC) efforts to explore uses (both current and anticipated), efficiencies, and implications for consumers associated with radio frequency identification (RFID) technology.

RFID technology represents a fundamental change in the information technology infrastructure with dramatic privacy implications. RFID technology significantly expands the range and function of global, electronic databases of all kinds. Because both the tag and the reading process can be virtually silent and invisible, RFID, if left unregulated, would permit a wide range of private and public covert, database-linked surveillance, tracking and profiling applications whose operation will not be transparent and remain unknown to the person under observation.

RFID tags are increasingly being used as a more advanced form and possible replacement of bar codes. The ever decreasing price for RFID tags and readers makes their widespread deployment increasingly economically viable. RFID tags are likely to become essential drivers of ubiquitous (or pervasive) computing. Their storage and capacity for interactive communication make them much more powerful than bar codes. They also provide for unique identification of each tagged unit, whereas bar codes are identical for every unit of the same product.

Unresolved questions still cloud this issue. It is yet unclear who should be allowed to collect data from RFID technology and to what extent. The standards and guidelines for sharing the data, either with other businesses or with the government, are still unclear. Consumers' right to either challenge the collection of data on their habit or to correct erroneous data is undefined. Additionally, consumers do not know the nature of the information that will be kept on them, or for how long it will be stored. The security of this data, that when correlated with other databases offer a granular picture of the individual, is of high concern and as of yet suspect.

These comments are divided into four primary sections: 1. RFID and Its Privacy Implications, 2. RFID and Fair Information Practice, 3. EPIC's Recommendations, and 4. EPIC's Guidelines on Commercial Use of RFID. In addition, two appendices are provided: Appendix 1, A RFID Industry and Manufacturer Survey; and Appendix 2, a paper prepared for EPIC by Washington University law student Greg Plichta: "Balancing RFID Technology and Expectations of Privacy: An Examination and Proposed Guidelines" (May 2004).

These comments demonstrate a compelling need for the Federal Trade Commission to issue industry guidelines for RFID use in consumer products, as well as recommend a comprehensive technology assessment before RFID technologies are widely deployed in the retail industry. Other US agencies, including the Food and Drug Administration (FDA), Department of Defense

(DOD), and the Department of Homeland Security (DHS) are promoting the adoption of product-level RFID tagging without considering consumer privacy implications.[1]

[1] *See* "Combating Counterfeit Drugs: A Report of the Food and Drug Administration," Food and Drug Administration report, February 2004, available at <http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html>; "DoD Announces Radio Frequency Identification Policy," United States Department of Defense Press Release, October 23, 2004, available at <http://www.dod.mil/releases/2003/nr20031023-0568.html>; and Jonathan Krim, "Embedding Their Hopes in RFID," E-Commerce Times, June 25, 2004, available at <http://www.ecommercetimes.com/story/34773.html>.

1. RFID and Its Privacy Implications

1.1. RFID Defined

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."[2]

Radio Frequency Identification (RFID) is an emerging information technology designed to facilitate the remote capture of information from physical objects. Associated data is stored on a small token (a "tag") affixed to, or embedded in, the object. Tags in use today are small enough to be invisibly embedded in products and product packaging. Data is read from these tags via radio waves transmitted by special RFID reading devices. RFID readers are often connected to computer networks, facilitating the transfer of data from the physical object to databases and software applications thousands of miles away and allowing objects to be continually located and tracked through space. Today, major uses of RFID include supply chain management, animal tracking, and electronic roadway toll collection.[3]

RFID technology represents a fundamental change in the information technology infrastructure with dramatic privacy implications. RFID technology represents the leading edge of a broader movement in computer science known as "pervasive" or "ubiquitous" computing where computers disappear into the environment and space itself becomes intelligent. Computer scientists behind the design of RFID envision a time in the not too distant future when all manmade objects on the planet bear RFID tags and information available on those tags is accessible to the global computer network -- a seamless link between the physical and virtual world.[4]

1.2. RFID and the Impending Explosion of Consumer Generated Electronic Data

---

[2] M. Weiser, "The Computer for the Twenty-First Century," Scientific American, pp. 94-10, September 1991.

[3] *See* EPIC RFID web page <http://www.epic.org/privacy/rfid/> for continually updated information on RFID developments and section on RFID *in* Privacy and Human Rights 2003 – An International Survey of Privacy laws and Developments (Cédric Laurant, ed., EPIC and Privacy International 2003), available at <http://www.privacyinternational.org/survey/phr2003/threats.htm#Radio-Frequency%20Identification>.

[4] *See* R. Want, K. Fishkin, A. Gujar, and B. Harrison, "Bridging Physical and Virtual Worlds with Electronic Tags," Proceedings of CHI'99, ACM Press, April, 1999, available at <http://pads1.cs.nthu.edu.tw/course/ISA5428/Tags.pdf>.

At the June 21, 2004 Federal Trade Commission workshop on RFID, several panelists pointed toward the importance of database management as a privacy issue. Jim Waldo, of Sun Microsystems, argued that database management is far more significant from a privacy standpoint than the issue of RFID technology itself.[5] We agree that database management is the central issue and that much of the privacy problem -- the use, processing and sharing of personal data via electronic databases -- has been around for quite some time. However, we disagree with Mr. Waldo's assertion that RFID is not life-changing and will not change the way we compute.[6]

RFID technology significantly expands the range and function of global, electronic databases of all kinds. Because both the tag and the reading process can be virtually silent and invisible, RFID, if left unregulated, would permit a wide range of public and private covert, database-linked surveillance, tracking and profiling applications whose operation will be invisible and remain unknown to the person under observation. The significance of RFID lies in the expansion of the global electronic network from a web of computers to a global web of physical objects and computers. Data generation does not require the intervention of a human agent at a keyboard or other form of terminal, only the presence of these objects in real space and the sweep of a radio wave. As a result, the class of events which could trigger the generation of data and its storage in a database expands by several orders of magnitude.

Although the use of RFID in the retail sector is now primarily in the supply chain, products with embedded RFID are beginning to appear on store shelves. Product-level tagging, if left unregulated, could facilitate unprecedented levels of consumer surveillance, tracking, and profiling.

1.3. Active, Passive, and "Class 0" Tags

When considering the technological plausibility of various privacy-threatening scenarios it is important to make a careful distinction between the types of RFID tags being considered. A common distinction between "active" and "passive" tags sometimes results in confusion. Passive tags, by definition, lack an independent power source. A sizeable class of passive RFID chips, however, allow for tag data to be supplemented and modified via the tag reader, allowing associated item information to be updated directly on the tag while it is in use. Passive tags, which do not permit data modification, are classified as "class 0" tags by the international RFID standards body EPCglobal.[7] Active tags may have on board batteries that dramatically increase their read range and functionality.

1.4. How "Class 0" Tags Can Be Tracked Via Object Name Service (ONS)

---

[5] *See* Jim Waldo, "Future Uses of RFID," June 21, 2004 presentation at FTC RFID workshop for partial reference, available at <http://www.ftc.gov/bcp/workshops/rfid/waldo.pdf>. The comment on the importance of databases does not appear in the Power Point outline available at the FTC workshop web site but it was made several times during the live presentation.

[6] Jim Waldo, *supra.*

[7] *See* EPCglobal web site at <http://www.epcglobalinc.org/>.

Even "class 0" tags, however, enable the identification and tracking of objects, and, by association, the individuals that may carry them. In the widely adopted EPCglobal RFID standard, the data imprinted on a "class 0" tag, the Electronic Product Code (EPC), provides a unique link to individual product data. The data is stored in a globally distributed, centrally managed, electronic database, known as the Object Name Service (ONS). Tag readers in remote physical locations can connect to the ONS via the Internet and then read and modify the item's ONS "dossier" throughout its lifecycle.[8] Also, the tags can be read from a distance and through a variety of substances such as snow, fog, ice, or paint, where barcodes have proved useless.[9] RFID systems enable tagged objects to speak to electronic readers over the course of a product's lifetime – from production to disposal – providing retailers with an unblinking, voyeuristic view of consumer attitudes and purchase behavior.[10]

1.5. Verisign and ONS

In January 2004 EPCglobal chose Verisign, Inc. to manage the root directory of ONS, because of similarities between the name service and Domain Name Service (DNS), which Verisign manages for the .COM and .NET top level domains.[11] This choice has raised alarm bells with privacy advocates, who note Verisign's poor track record in electronic privacy. In September 2003, Verisign was criticized for using its control over DNS root servers for .COM and .NET top-level domains to promote its own commercial services and potentially put consumer privacy at risk. Domain names that were mistyped during web browsing or email writing were redirected to Verisign servers instead of responding with standard error messages. Redirection of mistyped email address to Verisign servers made it possible for Verisign to intercept and store private personal email messages.[12] Verisign stopped the practice in October 2003 after a demand from Internet regulatory body ICANN.[13]

1.6. Current RFID Tracking Applications

RFID applications in use today employ the full range of tag technology, from cheap "class 0" tags to highly expensive miniature sensor/transponders. Animals and livestock have been tracked using RFID technology for decades, but RFID has recently become a technology of choice for

---

8 EPCglobal, "How the EPC Network Will Automate the Supply Chain," <http://archive.epcglobalinc.org/aboutthetech_idiotsguide.asp>.

9 John Stermer, "Radio Frequency ID: A New Era for Marketers?," Consumer Insight magazine, Winter 2001 <http://www.acnielsen.com/pubs/ci/2001/q4/features/radio.htm>.

10 *Id.*

11 Paul Roberts, "VeriSign to Manage RFID 'Root' Server," The Industry Standard, January 13, 2004, available at <http://www.thestandard.com/article.php?story=20040113174055565>.

12 SecurityFocus, "Verisign's SiteFinder Finds Privacy Hullabaloo," The Register, September 19, 2003, available at <http://www.theregister.co.uk/2003/09/19/verisigns_sitefinder_finds_privacy_hullabaloo/>.

13 Robert Lemos, "VeriSign Calls Halt to .Com Detours," CNet.com, October 3, 2003, <http://news.com.com/2100-1032_3-5086101.html>.

tracking humans. Although these applications are in their infancy, systems using "smart cards" the size of credit cards, active RFID tag bracelets, and even tiny chips embedded in the skin, track individuals to facilitate such goals as tracking inanimate objects like books,[14] ensuring safety, protecting health, monitoring behavior and enforcing discipline.

Europe's largest amusement park, Legoland in Denmark, uses active RFID tags contained in bracelets and Wi-Fi networks to help parents track their children through the park. And if the child leaves the park, a message is sent to the parent's mobile phone, as well as to the security guards at all the park entrances and exits.[15]

The PRISM system, developed by Alanco Technologies, Inc. for use in correctional facilities, uses a tamper proof RFID-enabled wrist bracelet to monitor the location of prison inmates in real time, reducing instances of prison vandalism and other unruly behavior. "A host of management reporting tools are available that include medicine and meal distribution, adherence to pre-determined time schedules, restricted area management, and specific location, arrival and departure information."[16]

The United States Transportation Security Administration (TSA) is considering the use of RFID-tagged airline boarding passes. Head of communications security technology at the agency, Anthony "Buzz" Cerino, commented at the RFID Journal Executive Conference in Chicago in April of 2004 that RFID boarding passes would let security personnel "know people's whereabouts."[17]

Applications that are not initially designed to track individuals, such as the RFID-based electronic highway toll collection system EZ Pass, might nonetheless make human tracking possible. In the investigation of the slaying of US Federal prosecutor Jonathan P. Luna in late 2003, authorities used EZ Pass data from highway toll booths in Pennsylvania and Delaware to discover he had made repeated trips to the Philadelphia area over a period of six months.[18]

RFID manufacturer Applied Digital Solutions (ADSX) has developed a passive chip the size of a pen point which is implanted in the human body. The VeriChip Personal Identification System is designed for use in a variety of applications including financial and transportation security, residential and commercial building access, military and government security.[19] A nightclub in

---

[14] Ron Harris, "Library Officials Grilled on Plan to Put Trackers in Books," USA Today, March 5, 2004, available at <http://www.usatoday.com/tech/news/techpolicy/2004-03-05-library-rfid-hearing_x.htm>.

[15] Laurie Sullivan, "Legoland Uses Wireless and RFID for Child Security," InformationWeek, April 28, 2004, <http://www.informationweek.com/story/showArticle.jhtml?articleID=19202099>.

[16] *See* "TSI Technology: Unique, Proprietary and Patented." Alanco Technologies, Inc., corporate web site. <http://www.alanco.com/corporate.asp>. (Last visited on July 8, 2004.)

[17] Bob Brewin, "TSA Eyes RFID Boarding Passes to Track Airline Passengers," Computerworld, April 1, 2004, <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,91830,00.html>.

[18] Gail Gibson, "Blood of Second Person in Car," Baltimore Sun, December 12, 2003, available at <http://www.baltimoresun.com/news/local/crime/bal-md.luna12dec12,0,6461729.story?coll=bal-local-features>.

[19] VeriChip FAQ. <http://www.adsx.com/faq/verichipfaq.html>.

Spain began using the VeriChip system in March 2004, to improve access for VIPs and allow them to pay for drinks without cash or credit cards.[20] ADSX has begun a campaign to promote the technology with the slogan "Get Chipped," and a mobile van called the "ChipMobile" can perform the chip insertion procedure in towns that it visits.[21]

1.7. Industry Solutions for Consumer Product RFID Tagging

Opponents of RFID tags in consumer products have proposed measures to side-step the chips' relentless information-gathering, ranging from disabling the tags by crushing or puncturing them, boycotting the products of companies which use or plan to implement RFID technology, or finding ways to block the reading of a tag using special mylar bags or other technological means. The RFID industry has moved to meet this consumer demand with its own solutions, most notably the EPCGlobal standard for "killing tags" which allows for tags to be physically disabled at point of sale by the merchant.[22] Another industry-level solution has been proposed by RSA Security, Inc. which would provide a system for tag reading to be blocked in specified "privacy zones" of varying scope. RSA's blocker tags, using a technique to confuse tag readers into thinking they are scanning a large number of tags, would work in conjunction with a "privacy bit" stored in the individual tag's EPC code. Using such a system, a merchant would "flip" the privacy bit on an item (from 0 to 1) at the point of sale. The consumer could then keep one of their blocker tags in the proximity of the item whenever they want to prevent the tag from being read. If, at a later date, the consumer needed to have the tag read for some reason, they could remove the blocker tag from the presence of the RFID reader so that data could be read normally.[23]

Both "tag killing" and tag blocking are problematic solutions that have yet to be proven in the field. The EPC protocol "kill command" leaves the final step of the process, physically disabling the chip, to the individual chip manufacturer. Many technologists have admitted that real world implementations of the kill command have been shown to have bugs and do not always work.[24] Furthermore, some industry "kill" solutions involve erasing the data but not destroying the circuitry, enabling the chip to be "recycled" at a later date. In fact, some RFID proponents have publicly attested to the value of a sleep command, where a chip will be publicly unresponsive

---

[20] Chetna Purohit, "Technology Gets under Clubbers' Skin," CNN, June 9, 2004, <http://www.cnn.com/2004/WORLD/europe/06/09/spain.club/>.

[21] *See* VeriChip information at ADSX web site, <http://www.adsx.com/prodservpart/verichippreregistration.html> and <http://www.adsx.com/prodservpart/verichip.html>.

[22] Junko Yoshida, "RFID Backlash Prompts 'Kill' Feature," EETimes, April 28, 2003, <http://www.eetimes.com/article/printableArticle.jhtml?articleID=12803964&url_prefix=story&sub_taxonomyID=2251>.

[23] A. Juels, R. L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," in V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pp. 103-111 ACM Press, 2003, available at <http://www.rsasecurity.com/rsalabs/node.asp?id=2060>.

[24] *See, e.g.*, "Cryptographic Approach to "Privacy-Friendly" Tags, by Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, NTT Laboratories, available at <http://www.rfidprivacy.org/papers/ohkubo.pdf> and "Jamming Tags Block RFID Scanners," by Kim Zetter, Wired News, March 1, 2004, available at <http://www.wired.com/news/business/0,1367,62468-2,00.html?tw=wn_story_page_next1>.

(appear to be killed) until sent an encoded "revitalize" command.[25] The "blocker tag" remains, an unproven solution for many reasons. Technologists appear to disagree as to the ease with which such a system might be circumvented,[26] and it places a significant burden on consumers to make sure they protect their privacy through the duration of their ownership of a product.

2. RFID and the Principles of Fair Information Practice

2.1. Fair Information Practices (FIP) and the OECD Guidelines
2.2. Position Statement on the Use of RFID in Consumer Products
2.3. Europe's Regulatory Approach to RFID
2.4. International Data Protection & Privacy Commissioners' Resolution

2.1. Fair Information Practices (FIP) and the OECD Guidelines

RFID is, at its heart, an extension of electronic database technology that has been used in the commercial sector for decades. The impending emergence of RFID technology on consumer products and the associated explosion of consumer generated data that is likely to follow should stimulate a renewed call for *omnibus* data and privacy protection legislation. The existing principles outlined in the 1973 Principles Fair Information Practice and the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data provide an excellent model for approaching RFID regulation.

The Principles of Fair Information Practices, issued by the US Department of Housing, Education, and Welfare (HEW) in 1973 to address the use government records maintained in computer databases, can be summarized into five basic principles: notice, choice, access, security and enforcement.[27] The Code of Fair Information Practices has contributed to the development of privacy laws around the world, and the development of important international guidelines on privacy, including perhaps the most well known, the guidelines promulgated by the OECD. This Code of Fair Information Practices was rearticulated in the OECD Guidelines as a set of 8 principles: Collection Limitation (including notice and consent); Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability.[28]

---

[25] *See* Joe Best, "Zombie RFID Tags May never Die," Silicon.com, May 18, 2004, available at <http://zdnet.com.com/2100-1103_2-5214648.html>.

[26] *See* Scott Mace, "RFID Blocker Tag Concerns," Information Manager Journal, March 5, 2004 <http://scottmace.typepad.com/imanager/2004/03/rfid_blocker_ta.html>.

[27] U.S. Department of Health, Education & Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records Computers and the Rights of Citizens (MIT 1973), available at <http://www.epic.org/privacy/1974act/>.

[28] OECD, Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (1981), available at <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>.

We first review the eight principles in detail and their relation to RFID practice.

The OECD Principles and their application to RFID:

> ***Collection Limitation Principle***: it requires limits to the collection of personal information and the obtaining of any data by lawful and fair means with the knowledge or consent of the subject. The collection of information should be limited to that which is necessary for the purpose at hand. This principle is a consumer's first line of defense and is essential to enable negotiation about the terms of use and disclosure of personal information.
>
> Because of the potentially ubiquitous and transparent nature of RFID systems, notice and consent are particularly important factors for privacy-sensitive RFID practice. The consumer has a right to know if RFID tags or readers are present in retail sales environments or in products they purchase. Consumers should be able to easily remove RFID tags from products they buy in order to freely and confidently exercise their consent. Further, association of personally identifiable information with information identifying an object should be avoided whenever possible. In the event that this association is integral to a particular application, the consumer must be notified of the purpose and scope of the associated data and do so only with the consumer's express written consent. Participation in an RFID application should be strictly voluntary. Covert capture of information should not be permitted. Informed consent is the primary tool available to individuals to protect their privacy from technological invasion.
>
> ***Data Quality Principle***: personal data should be relevant to the purposes for which they are to be used and should be accurate, complete and up-to-date.
>
> ***Purpose Specification Principle***: the purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to fulfill those purposes.
>
> ***Use Limitation Principle***: personal data should not be disclosed, made available, or otherwise used for purposes other than those specified under the Purpose Specification Principle, except with consent or by legal authority.
>
> ***Security Safeguards Principle***: personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure. These safeguards should be verified by outside, third-party, and publicly disclosed assessment.[29]

[29] Security is important for even basic, "class 0" RFID tags. Without encrypting a tag's EPC code or requiring secure authentication before a tag transmits data, any technologically equipped third party could theoretically scan and identify the contents of an individual's bag or pockets.

> ***Openness Principle***: there should be a general policy of openness about developments, practices and policies with respect to personal data.

In RFID practice, openness should extend beyond simple communication of policies and practices to complete transparency of operation for any RFID application. RFID users must make public their policies and practices involving the use and maintenance of RFID systems, and there should be no secret databases. Individuals have a right to know when products or items in the retail environment contain RFID tags or readers. They also have the right to know the technical specifications of those devices. Labeling must be clearly displayed and easily understood. Any tag reading that occurs in the retail environment must be transparent to all parties. There should be no tag-reading in secret.

> ***Individual Participation Principle***: an individual should have the right to ascertain or confirm whether a data controller has data relating to him or her, and to challenge that data.

> ***Accountability Principle***: A data controller should be accountable for complying with measures that have been established pursuant to these data protection principles.

RFID users are responsible for implementation of this technology and the associated data. RFID users should be legally responsible for complying with the principles. An accountability mechanism must be established. There must be entities in both industry and government to whom individuals can complain when these provisions have been violated.

2.2. Position Statement on the Use of RFID in Consumer Products

On November 20, 2003, more than 20 consumer privacy and civil liberties groups, including EPIC, released an RFID Position Statement.[30] The policy position calls for RFID practice to follow the Code of FIP and identifies additional practices that should be prohibited in order to fully protect consumers:

> Merchants must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they buy.

> There should be no prohibition on individuals to detect RFID tags and readers and disable tags on items in their possession.

---

[30] RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, November 20, 2003, available at <http://www.privacyrights.org/ar/RFIDposition.htm>.

RFID must not be used to track individuals absent informed and written consent of the data subject.

Human tracking is inappropriate, either directly or indirectly, through clothing, consumer goods, or other items.

RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency.

2.3. European Union's Regulatory Approach to RFID

Although the European Union does not have specific regulations applying to RFID, the EU Data Protection Directive and the Privacy and Electronic Communications Directive do codify the Principles of Fair Information Practice into law and are applicable to the processing of personal data through the use of RFID technologies. The directives apply to both the issue of individual tracking and the association of data with personal identification. As a result, any use of RFID tags that involves the processing of personal data is likely to be subject to a number of data protection obligations.[31] Article 8 of the EU Data Protection Directive of 1995, for example, prohibits the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[32] Further, the more recent Privacy and Electronic Communications Directive states that "location data may only be processed when it is made anonymous or with the consent of the individual."[33]

At the World Summit on the Information Society (WSIS) in Geneva (Switzerland) in the fall of 2003, three researchers from the UK, Switzerland and Sweden discovered that the security system used to control access to the United Nations Summit included hidden RFID tags embedded in the official Summit badges. The researchers revealed the intrusive manner in which individual attendees could be identified and tracked as they moved through the conference. The researchers argued that "procedures of how personal data is being handled during WSIS break the principles of the Swiss Federal Law on Data Protection of June 1992, the European Union Data Protection Directive (1995/46/EC) and the United Nation Guidelines concerning Computerized Personal Data Files adopted by the General Assembly on December 1990."[34]

---

[31] Eduardo Ustaran, "Data Protection and RFID Systems," 3/6 Privacy & Data Protection 6, available at <http://www.berwinleighton.com/download/PDP-RFIDtagsimplications.pdf>.

[32] EU Data Protection Directive 95/46/EC, O.J.E.C., L. 281, 23.11.1995, p. 31, available at <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett>.

[33] EU Directive on Privacy and Electronic Communications 2002/58/EC, O.J.E.C., L 201, 31.07.2002, p. 37, available at <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>.

[34] Alberto Escudero-Pascual, Stephane Koch, and George Danezis, "The Physical Access Security to WSIS: a Privacy Threat for the Participants." Press Release. December 12, 2003, available at <http://www.nodo50.org/wsis/>.

2.4. International Data Protection & Privacy Commissioners' Resolution

A joint resolution on RFID, proposed by data protection authorities in Germany, Spain and Switzerland and adopted at the International Conference of Data Protection & Privacy Commissioners in Sydney (Australia) on November 20, 2003, asserted that "all the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology." The resolution called for implementers of RFID systems to carefully weigh the necessity for collecting personal information or profiling customers and to do so only in an open and transparent manner. Further, the resolution stipulated that individuals must have the ability to delete data stored on RFID tags and to disable or destroy the tags. The International Working Group on Data Protection in Telecommunications expressed support for their resolution at its September 2 and 3, 2003 meeting in Berlin.[35]

With the Sydney resolution and the existing directives on data protection and privacy and electronic communications, Europe seems to have a legal framework to address the use of RFID tagging in the retail sector. No country or region, however, has formally adopted a clear set of guidelines or laws that address the unique properties of RFID.

About the EPIC Recommendations and Guidelines

EPIC has developed guidelines for the use of RFID in consumer manufacturing and retail industry that rearticulate the OECD guidelines as they apply to RFID practice and includes additional prohibitions from the November RFID position statement. These guidelines can also serve as a basis for further legislation.

---

[35] *See* International Conference of Data Protection & Privacy Commissioners "Resolution on Radio-frequency Identification," Final Version, November 20, 2003, available at <http://www.privacyconference2003.org/resolutions/res5.DOC>.

3. EPIC Recommendations

Summary

1. **Issue immediate ruling requiring any and all item-level tagging of consumer retail products to be clearly labeled and easily removable.**
2. **Issue a set of federal guidelines for manufacturers of consumer products and retailers to follow when making use of RFID technology in the course of business (*see* EPIC guidelines).**
3. **Recommend a comprehensive assessment of RFID technology and global practice, followed by expert determination of the need for additional legislation specifically targeting the use of RFID.**
4. **Publish and disseminate documents that educate the general public about RFID technology and with the purpose of educating businesses about RFID technology and the importance of protecting an individual's privacy.**

EPIC Recommendations for Federal Trade Commission action are based on the following findings of fact on RFID technology and practice, described in detail below:

Significance of RFID – RFID technology represents a fundamental change in the information technology infrastructure with tremendous privacy implications. RFID dramatically improves the range and power of global, electronic databases on many types while rendering the process of data generation and collection virtually transparent to the individual consumer.

RFID and Tracking – Even the simplest, cheapest tags can be tracked through space when their unique identifying number is associated with data stored in a globally accessible database. (*See* "How "Class 0" Tags can be Tracked Via Object Name Service (ONS)" *in* the "RFID and Its Privacy Implications" section.)

Inadequacy of Current Technological Solutions – The tag killing protocols and blocker tags are problematic and obscure solutions to address RFID privacy concerns in the retail environment. (*See* "Industry Solutions for Consumer Product RFID Tagging" in the "RFID and Its Privacy Implications" section.)

EPIC's Recommendations for the Federal Trade Commission

1. A first step in addressing the significant concerns that RFID raises for the FTC is to articulate a clear set of guidelines for RFID in the private manufacturing and retail sector. The Federal Government must legislate responsible use and acquisition of consumer data before RFID tags are implemented and standardized.

2. Further, the FTC should issue a ruling that any item-level tagging of consumer products in the retail sector must be conspicuously labeled and easily removable. The nature of RFID technology would make it easy for such activity to develop without consumers being aware of any changes. By issuing a ruling it will send a signal to all members of the retail and manufacturing industry that hidden RFID or coercive RFID applications will not be tolerated in the marketplace.

3. In order for privacy to be protected, the FTC must require a period of careful discussion and deliberation regarding the design and implementation of RFID systems before item-level tagging is introduced into retail consumer products. The FTC should require that the RFID technology undergo a formal technology assessment to determine which risks the deployment of such technology could raise for consumers' privacy. This assessment must be made by an independent entity and involve all stakeholders, including consumers through consumer protection groups. Once this assessment is complete it should determine the necessity for legislation specifically addressing RFID technology.

4. The FTC should pay special attention to the operation of the RFID database system known as Object Name Service (ONS). Abuse of data in the ONS could severely endanger the personal privacy of millions of American citizens.

5. The FTC should publish and disseminate documents that educate the general public about RFID technology and with the purpose of educating businesses about the importance of protecting consumers' privacy. The documents shall, *e.g.*, describe RFID technology; how companies, marketers and government agencies can use RFID technology to collect an individual's nonpublic personal information; advocate privacy protection; and explain how businesses must conform their actions to comply with the provisions of this Act.

6. The FTC should establish appropriate standards for the RFID Users taking into account the guidelines proposed in this submission.

4. EPIC Guidelines on Commercial Use of RFID

4.1. Introduction

The guidelines are proposed to guide the use of RFID technology in order to protect both private enterprise interests and consumer privacy interests. This means that these guidelines do not address protection of consumer privacy from any governmental action. Rather, they seek to protect consumer privacy from private enterprises. Further, these guidelines focus on use in the retail and manufacturing industry where retailers and manufacturers are beginning to implement item-level RFID tagging to facilitate supply chain efficiency, inventory control, and similar applications.

These guidelines primarily address commercial, private applications which may use RFID tags to draw conclusions about consumers without their knowledge or consent, or that might generate data which could be used for entirely different purposes at a later date.

These guidelines are divided into three parts. Part A addresses the duties of private enterprises that use RFID technology. It imposes minimum requirements on RFID users, recognizing the advantages that RFID technology can provide while at the same time addressing privacy concerns. Part B addresses practices in which the RFID Users should never engage, including tracking, snooping, and coercing consumers to accept live RFID tags or associate their personal data with an RFID application. Finally, Part C states the rights of consumers who are exposed to RFID technology and incorporates some of the Users' duties stated in Part A.

4.2. Definitions

"RFID" means Radio Frequency Identification, *i.e.*, technologies that use radio waves to automatically identify individual items.

"Tag" means a microchip that is attached to an antenna and is able to transmit identification information, *i.e.*, capable of receiving data from, or transmitting data to, a Reader.

"Reader" means a device, capable of reading data from a tag or transmitting data to a RFID tag.

"RFID Subject" or "Individual" means a consumer, customer, or any other such individual that comes in contact with a product that has attached to it, or contains, an RFID tag.

"RFID User" means an RFID operator, such as a store, warehouse, hospital, and the like, who employs RFID technology, including RFID readers and tags.

"Premises" means a store, a warehouse, a hospital, or any other such equivalent space that encompass the tags and the readers that communicate with RFID tags.

"Consent": means the freely given, specific and informed indication of a RFID subject's wish to have his/her personal information processed by the means of RFID technologies.

4.3. RFID Guidelines

A. What RFID Users Must Do:

*1. **NOTICE***. Give notice to a RFID Subject of:

a. ***Tag presence***, whether through labels, logos, or equivalent means, or through display, either at the place where a tagged item is stored, such as a shelf or counter, or at point of sale, such as a cash register. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

b. ***Reader presence***, whether through labels, logos, or equivalent means, or through display, whenever tag readers are present. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

c. ***Reading activity***. RFID Users must use a tone, light, or other readily observable and recognized signal whenever a tag reader is in the act of drawing information from an RFID tag anywhere on the sales floor.

2. *REMOVAL*. Attach tags to items in such a way as to allow for the easiest possible removal of tags.

3. *ANONYMITY PRIORITY*. Any RFID user -- before linking RFID tags to personal information -- should first consider alternatives which achieve the same goal without collecting personal information or profiling customers. If personal information must be collected and associated with tag data, the RFID user must satisfy the following five requirements:

a. ***Consent***. Obtain written consent from an individual before any personally identifiable information of the individual, including name, address, telephone number, credit card number, and the like, is attached to, stored with, or otherwise associated with data collected via the RFID System.

b. ***Purpose***. Before obtaining written consent, the RFID User must inform the RFID subject about the purpose of associating gathered data with personal information, and specify that purpose before such attaching, storing, or association.

c. ***Use limitation***. Before obtaining written consent, the RFID User must inform individuals about the scope of use of gathered data, whether the use is limited to the person's own interests or whether the data will be disclosed to third parties. Keep data only as long as it is necessary for the purpose for which the data was associated with personal information.

d. ***No third party disclosure***. Not disclose, directly or through an affiliate, to a nonaffiliated third party an individual's personally identifying information in association with RFID tag identification information.

e. ***Data quality***. Keep gathered data accurate, complete and up-to-date, as is necessary for the purposes for which it is to be used.

4. ***SECURITY***. Take reasonable measures to ensure that any data processed via an RFID system is transmitted and stored in a secure manner, and that access to the data is limited to those individuals needed to operate and maintain the RFID system.

5. ***OPENNESS***. RFID Users must make readily available to individuals, through the Internet or other equivalent means, specific information about their policies and practices relating to its handling of personal information. Any personally identifiable information itself shall be provided upon written request of the individual in a secure manner.

6. ***ACCOUNTABILITY***. Designate someone who is accountable for the RFID User's compliance with these guidelines.

B. What RFID Users Must NOT Do:

1. ***TRACK***. Track the movement of RFID subjects at any time without their written consent to all tag reading events. RFID users shall not track individuals via tagged items on the premises or outside the premises where an RFID system is employed to obtain individual shopping habits or any other such information obtainable through tracking, even upon suspicion of such activities as fraud or shoplifting.

2. SNOOP. Record or store tag data from tags that do not belong to the RFID User for any reason except for the processing of returns or warranty service and upon the consumer's request. RFID users shall not collect RFID data from objects on, or carried by, an individual person for the purpose of generating a consumer profile, even if the profile is assigned anonymously.

3. COERCE. Coerce or force individuals to keep tags turned on after purchase for such benefits as warranty tracking, loss recovery, or compliance with smart appliances; and not require individuals to provide unnecessary personal information as a precondition of a transaction. RFID

Users must allow individuals who so desire to enroll anonymously in any RFID data-gathering scheme.

C. RFID Subjects' rights:

1. ***ACCESS***. RFID Subjects must have the right to access data containing personally identifiable information collected through an RFID system, and have the opportunity to make corrections to that information.

2. ***REMOVAL***. RFID Subjects have the right to get tags removed from tagged items.

3. ***ACCOUNTABILITY***. RFID Subjects have the right to challenge the compliance of persons employing RFID systems when practice contradicts the guidelines set forth above.

Appendix 1: Industry and Manufacturer Survey[36]

General Summary

EPIC recently surveyed developers and manufacturers of RFID technology, as well as retailers who have begun to employ RFID in the supply chain and in the retail setting. EPIC asked about their use of RFID tags in the retail environment and requested details about how they were enabling customers to disable tags (a process known as "tag killing") or remove tags from retail merchandise.

It is clear from the responses so far that there is no standard for tag killing in the industry today. Many applications do not include the option at all and, when it is included, the actual mechanism for disabling the tag varies widely. Some retailers and manufacturers note proudly that no personal information is stored on the tag. This is largely irrelevant considering the ease with which a tag's unique identifier could be associated with personal data at the database level.

Further, it is clear that several applications are being developed which read RFID tags on an individual's person without their explicit knowledge and consent. Government and employer applications, for example, may silently read tags without notifying the individual carrying them.
Manufacturers and retailers, such as Alien Technology and Wal-Mart, tell us that consumers rarely take home products with RFID tags since they are predominantly used in the supply chain on cases and shipping pallets. They further add that when consumers do take home products with RFID, they are clearly labeled and only embedded in packaging that can be easily removed. However, Wal-Mart stated that "Consumers may wish to keep RFID tags on packaging to facilitate returns and warranty servicing." This suggests that, in the future, customers may have difficulty benefiting from refund and warranty services if they do not hold on to live tags.

Industry responses as of 6/23/2004 come from: Royal Philips Electronics, Wal-Mart, Alien Technology, SAP, and Vanguard I.D.

Royal Philips Electronics - Jeroen Terstegge - Corporate Privacy Officer

(This statement cannot be considered Philips's official position.)

Key points: Smart-card RFID generally does not support killing, but smart-label RFID chips do. There are several instances of applications where an individual might not be

[36] A continually updated version of the industry survey is available at <http://www.epic.org/privacy/rfid/survey.html>.

aware of when tag reading occurs. Philips Privacy Code does not apply to RFID tags used by Philips' customers, but applies to Philips' internal data processing only.
Tag killing option is only used in certain chip families, which are mainly used in retail and logistics. Smart-card RFID chips, used in ID-cards, loyalty cards, tickets, do not have a kill option but use strong encryption techniques and have range limitation features. Mr. Terstegge can neither confirm nor deny whether Philips produce chips with "deep sleep" mode. Near Field Communications (NFC) protocol is secure and has very limited (10 cm / 3.9 inch or less) read range. NFC is currently used in highly secure RFID cards. Philips envisions future entertainment applications using NFC enabling easy, intuitive and – if necessary – secure data transfers between devices over short ranges.
Philips supports the International Conference of Data Protection & Privacy Commissioner's Resolution on Radio-Frequency Identification. "If data stored on RFID-chips are used to identify consumers, *i.e.* by linking the data with a CRM-database, the consumer must be informed and provided with the possibility to object, which in many countries is a legal obligation. Philips offers a variety of security and privacy protection features, but it is the customer's responsibility to actually implement and use them."
Philips acknowledges several ranges of applications where tag reading may occur without individual knowledge or confirmation such as workplace applications in the public and private sectors. Philips also suggests applications where opening a door triggers a tag reading event without individual notification.

Alien Technology - Paul Drzaic, Ph.D. - Vice President, Advanced Development

Key points: No RFID tags will be embedded in consumer products (other than packaging) for years. If packaging has RFID, it is clearly labeled.
"For the next few years, nearly all RFID implementations in retail settings are aimed at tagging cases and pallets of goods, not individual items. The items that do pass into consumers hands will be on the outside of packaging, and will be clearly marked as EPC tags consistent with EPCglobal policy. Consumers will not be exposed to RFID tags on large numbers of individual retail items for some time, which allows for the development of industry best-practices that will be acceptable to all."

SAP - Roland A. Edwards - Manager Product Public Relations Global Communications

Key points: Representative says its tag-killing feature at Metro stores physically disables tag, but this is contradicted by CASPIAN. Personal information is not stored on chip but is likely associated in store databases.
SAP representative says that the item-level tag-killing feature it provides to Metro "is performed in such a way that even the chip manufacturer would have no chance to reactivate the chip." Further, they "physically destroy" the chip. *(Note: This contradicts a*

CASPIAN report[37] *that the tag "killing" only overwrites the bar code information with zero's and not the tags individual ID.)*

Personal information is not stored on chip. However, the SAP statement suggests RFID data is associated with personal information at the database level: "If personal information is needed to perform a certain business process, it will require special authorization levels to perform this action."

Vanguard ID - Nick Martino

Key points: One tag "killing" solution involves data alteration, not physical destruction. One form of tag disabling they use is to write a disabling code over the chip which masks its unique identifier.

Wal-Mart Stores, Inc. - Pauline Tureman - Investor Relations

Key points: No tag-reading is done on the sales floor. Consumer-level tags are used only on packaging, are easily removable, and are not used without clear labeling. RFID will not be used to collect additional data about consumers.

Virtually all RFID tags are on case and pallet level. Only three products in Dallas pilot store, two printers and a scanner, have RFID on packaging that a consumer might take home (in this case, shipping cases and end user packaging are one and the same.) Any RFID-enabled packaging that a consumer might take home is and will be clearly labeled (on the shelf and on the product) and easily removable by the consumer. No RFID labels are embedded in the products themselves. Consumers may wish to keep RFID tags on packaging to facilitate returns and warranty servicing.

". . . [W]e do not have any readers on our sales floors. We have also publicly stated that we will not use RFID to collect any additional data about consumers."

[37] Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN). "Scandal: The 'Undead Machine' RFID Tag Deactivation Station that Does not Deactivate Tags" <http://www.spychips.com/metro/scandal-deactivation.html>.

Appendix 2: Greg Plichta, "Accommodating RFID Technology and Expectations of Privacy: An Examination and Proposed Guidelines" (May 2004)

Accommodating RFID Technology and Expectations of Privacy: An Examination and Proposed Guidelines[38]

Radio Frequency Identification (RFID) is a rather old technology that has raised new issues in the area of privacy. The main risk to privacy is the ability of the technology to track individuals. Such tracking can be accomplished by monitoring objects with attached transponders ("tags") to them, whether it be in a store, a warehouse, or beyond these premises. By tracking objects, it is possible to track individuals who have substantial contact with such objects. Such tracking includes monitoring what individuals are purchasing and where individuals are moving about. However, tracking can also be accomplished directly by embedding individuals with tags. Thus, a need has arisen to examine how the use of RFID technology can be accommodated with an individual's expectation of privacy.

In examining the tension between RFID technology and privacy, this paper is divided into five parts. In part I, a brief history of RFID technology is given. In part II, the current state of the technology is examined. Part III, which analyzes privacy issues concerning RFID technology, is divided into four subparts. First, the tracking of objects is considered, which is the typical scenario. This scenario considers various uses of RFID technology, from the garden variety retail use to the more exotic embedding of RFID tags in money and tires. Second, the direct tracking of people is considered, in

[38] I would like to thank Chris Hoofnagle, Associate Director of the Electronic Privacy Information Center (EPIC), for his insightful comments on this paper. *See* http://www.epic.org/epic/staff/hoofnagle/.

contrast to tracking of objects (and the tracking of people via objects). Third, tracking by the private sector is examined, which is mainly done for economic streamlining reasons. And fourth, tracking by the government is examined, and to what extent the government is engaged in the RFID and privacy struggle. In part IV, conclusions are drawn regarding the state of the RFID and privacy developments. Finally, in part V of this paper, general recommendations are made as to how RFID technology can continue to create new efficiencies while accommodating individuals' privacy rights. The main concern of this paper is to survey how each side, whether industry groups or privacy advocates, is trying to push forward its agenda while trying to assess the current state of the debate. Thus, this paper attempts to gain an objective understanding (to the extent one individual can be "objective") of the RFID/privacy debate, without advocating for either side.

At the end of this paper, proposed guidelines are offered that attempt to strike a balance between the legitimate use of RFID technology to advance the state of technology and increase economic efficiency and an individual's expectation of privacy. This balance is struck based on the assumption that RFID technology is here to stay and that it will only expand in its applications, and that an individual's expectation to privacy cannot be compromised for the sake gaining the most efficient or most cost effective means to employ the tracking of everyday objects.

The History of RFID [39]

The history of RFID goes back 14 billion years to the "Big Bang." It is with the Big Bang, as current scientific theory tells us, that electromagnetic energy was created, which now serves as the source of RFID technology. Fundamental understanding of electromagnetic energy was not developed until the beginning of the 1800's, where scientists like Faraday, Maxwell, and Hertz laid the groundwork for the concept of electromagnetic energy as electromagnetic waves, or radio waves. Only towards the end of the 19th century, Marconi was able to successfully transmit radio waves across the Atlantic.

Then, approximately in 1922, radar technology was born. Radar sends out radio waves to detect and locate an object by reflecting these waves off of the object. Such reflection can determine the position and speed of an object by using simple trigonometry. This fundamental idea underlies RFID technology. However, probably the first work exploring RFID technology as it is understood today, was Harry Stockman's landmark paper "Communication by Means of Reflected Power," in October of 1948. It is interesting to note that it would take another thirty years after Stockman's paper for RFID technology to fully realize its potential. The problem was that other developments in technology were needed first, namely, the development of the transistor, the integrated circuit, the microprocessor, communication networks, and the like. Thus, the development of RFID technology was anything but linear and logical—it depended to a large extent on the vagaries of surrounding technology.

---

[39] The history of RFID in this section is based on a publication by Dr. Jeremy Landt, *Shrouds of Time. The history of RFID*, The Association for Automatic Identification and Data Capture Technologies (AIM), *at* http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf. Landt was one of the original five scientists at Los Alamos National Laboratories who developed RFID technology for the federal government.

The 1950's ushered in an era of exploration and laboratory experimentation of RFID technology, which was still based on the developments in radio and radar in the 1930's and 1940's. Related technologies such as the long-range transponder system for aircraft further assisted in the development of RFID. The 1960's saw commercial activity and companies like Checkpoint and Sensomatic were formed. These companies developed electronic article surveillance (EAS) equipment to counter theft. This equipment was rather primitive by today's standards since it could only detect the presence or absence of a tag attached to an object. However, EAS technology was arguably the first and most widespread commercial use of RFID.
The 1960's in many ways were a prelude to the explosion of RFID technology in the 1970's.

In the 1970's both the private and the public sectors were intimately involved in RFID technology. Applications for animal tracking, vehicle tracking, and factory automation burgeoned. A 1973 conference sponsored by the International Bridge Turnpike and Tunnel Association (IBTTA) and the United States Federal Highway Administration concluded that there was no national interest in developing a standard for electronic vehicle identification, and this was "an important decision since it would permit a variety of systems to develop, which was good, because RFID technology was in its infancy."[40]

The 1980's were a decade of RFID implementation. But, different parts of the world emphasized different aspects of RFID technology. For example, in the United States, transportation, personnel access, and to a lesser extent, animal tracking were of interest. In Europe, on the other hand, the greatest interest was in short-range systems

---

[40] *Id.*

for animals and industrial and business applications. Moreover, in the Americas, some associations were active in RFID initiatives dealing with railroads and container handling.

The 1990's saw wide scale deployment of electronic toll collection technology in the United States. In 1991, in Oklahoma, the world's first open highway electronic tolling system opened. Under this system, vehicles could pass toll collection points at highway speeds without having to stop at toll booths. On the Kansas turnpike, a system was installed with readers that could read tags of an Oklahoma system, thus RFID technology had spread across state boundaries. Furthermore, in Georgia an improved system could read not only its own tags but also those of the system installed in Kansas. This meant that RFID technology could cope with multiple protocols of toll collection systems. However, tolling applications were not limited to the United States. Such applications appeared in Argentina, Australia, Canada, Brazil, China, Europe, Hong, Japan, Kong, Malaysia, Mexico, Philippines, Singapore, South Africa, South Korea, and Thailand.

RFID technology spread not only across different countries but also across different business segments. A single tag could now be used for toll collection, parking lot access and fare collection, and gated community access and campus access. The significant expansion of the functionality of RFID technology was in part due to technological developments. Schottky diodes fabricated on CMOS integrated circuits permitted for construction of microwave RFID tags that contained only a single integrated circuit. At the same time, many new companies entered the marketplace to take advantage of the increasing capability of RFID technology.

At the beginning of the 21st Century, the future of RFID technology looks bright. Now that the cost of RFID technology is rapidly decreasing, its spread across numerous

sectors of the economy[41] and national borders[42] looks more and more inevitable.[43] At present, RFID is in the midst of being deployed on a wide scale in the retail sector.[44] From 1999 until 2003, the Massachusetts Institute of Technology was working with industry partners, in a research group called Auto-ID Center, to develop and field test a new breed of computer network that can track the location of everyday objects, through an elaborate system of RFID microchips and readers.[45] This partnership has now resulted in a new joint venture, called EPCglobal, which is made up of the Uniform Code Council and EAN International, which oversee global barcode standards. EPCglobal will

---

[41] Numerous leading technology companies are starting to apply RFID technology to various uses. Generally, *see* CNET News.com Staff, *Survey: IT managers say they'll increase spending*, CNET News.com (May 10, 2004), *at* http://news.com.com/2100-1022_3-5209435.html (reporting that "[t]hirty-one percent of companies, mostly manufacturing and retail and wholesale companies, said they would increase RFID … deployment through the year"); Specifically, *see* Alorie Gilbert, *Oracle update gets tailored to industries*, CNET News.com (Jan. 28, 2004), *at* http://zdnet.com.com/2100-1104_2-5149550.html; Alorie Gilbert, *PeopleSoft gussies up inventory tools*, CNET News.com (Feb. 23, 2004), *at* http://zdnet.com.com/2100-1104_2-5163677.html; News, *Gillette Confirms RFID Purchase*, RFID Journal (Jan. 7, 2003), *at* http://www.rfidjournal.com/article/articleview/258/1/1/; Matt Hines, *HP debuts RFID services*, CNET News.com (May 10, 2004), *at* http://news.com.com/2100-1011_3-5209394.html; Matt Hines, *RSA polishes RFID shield*, CNET News.com (Feb. 24, 2004), *at* http://news.com.com/RSA+polishes+RFID+shield/2100-1029_3-5164014.html; Adam Zawel, *IBM, Sun put RFID to the test*, ZD Net News (Apr. 29, 2004), *at* http://zdnet.com.com/2110-1103_2-5202069.html; Marguerite Reardon, *Microsoft hops on the RFID bandwagon*, ZD Net News (Jan. 26, 2004), *at* http://news.com.com/2100-7343-5147145.html; Alorie Gilbert, *VeriSign chosen to run RFID tag network*, CNET News.com (Jan. 13, 2004), *at* http://news.com.com/2100-1011_3-5140552.html; News, *Sony, Philips to Test RFID Platform*, RFID Journal (May 8, 2003), *at* http://www.rfidjournal.com/article/articleview/404/1/1/.

[42] Numerous countries are also starting to apply RFID technology: E.g., *see* News Software, *China gears up for RFID*, CNET News.com, Feb. 6, 2004, *at* http://news.com.com/2100-1008_3-5154776.html; Alorie Gilbert, *RFID tags get a push in Germany*, CNET News.com, Jan. 12, 2004, *at* http://zdnet.com.com/2100-1104_2-5139627.html;

[43] Brad Stone, *In Your Cereal?*, Newsweek (Sept. 29 issue), *available at* http://msnbc.msn.com/id/3068859/ (reporting that RFID firms say they've already manufactured several hundred million chips over the past decade).

[44] Jo Best, *Retailers make waves for RFID*, Silicon.com (April 29, 2004), *at* http://zdnet.com.com/2100-1103_2-5201866.html; Alorie Gilbert, *Major retailers to test 'smart shelves'*, CNET News.com (Jan. 8, 2003), *at* http://news.com.com/2100-1017-979710.html; Barnaby J. Feder, *Wal-Mart Plan Cost Suppliers Millions*, The New York Times Online, *available at* http://www.nytimes.com/2003/11/10/technology/10radio.html; Andy McCue, *U.K. retailer tests radio ID tags*, CNET News.com (Oct. 16, 2003), *at* http://news.com.com/2100-1039_3-5092460.html.

[45] Alorie Gilbert, *MIT winds down radio tag activity*, CNET News.com (Oct. 23, 2003), *at* http://news.com.com/2100-1008-5095957.html.

develop the coordination of technical standards and specifications for RFID technology.[46]

In short, what these above listed developments suggest is that RFID technology has matured over decades and it is so well established that reasonable privacy legislation will not end the development of RFID.[47] Whatever difficulties RFID will encounter may be due to its own internal struggles as much as external forces.[48] Legislation dealing with RFID privacy issues is just beginning to be introduced, and it will determine to what extent RFID technology will impinge on an individual's expectation of privacy.[49]

The Technology of RFID [50]

As one writer put it, RFID technology is "essentially a new and vastly improved barcode."[51] The barcode has become ubiquitous and familiar, with its field of bars and

---

[46] *Id.*

[47] See footnotes 4 and 5. *Cf.* Thomas Claburn, *Privacy Fears May Slow RFID Progress*, InformationWeek (Mar. 8, 2004), *at* http://informationweek.securitypipeline.com/news/18311264 ("Without a comprehensive understanding and approach to the legislation of such technologies [as RFID] ... legislators risk ineffective and perhaps detrimentally reactionary legislation.").

[48] Matt Hines, *Roadblocks could slow RFID*, CNET News.com (Feb. 19, 2004), *at* http://news.com.com/2100-1008-5161278.html (reporting that companies may need to rethink their software infrastructure in order for RFID to work properly; one example is making sure that back-end databases and business applications can handle the massive amounts of information generated by RFID-enabled systems); Ron Coates, *Setback for Wal-Mart's RFID project*, Silicon.com (Mar. 29, 2004), *at* http://zdnet.com.com/2100-1103_2-5181244.html; Matt Hines, *Companies' RFID plans fuzzy so far*, CNET News.com (Apr. 15, 2004), *at* http://news.com.com/2100-1012_3-5192080.html?type=pt&part=inv&tag=feed&subj=news.

[49] As discussed later on in this paper, states like California, Missouri, and Utah have introduced RFID legislation. *See* Mark Roberti, *The Law of the Land*, RFID Journal (Mar. 1, 2004), *at* http://www.rfidjournal.com/article/articleview/811/1/2/. Federal legislation protecting consumer privacy may also be on the way. *See* Grant Gross, *RFID and privacy: Debate heating up in Washington*, InfoWorld (Mar. 28, 2004), *at* http://www.infoworld.com/article/04/05/28/HNrfidprivacy_1.html.

[50] This section (II) is generally based on Klaus Finkenzeller's introductory text to RFID technology: Klaus Finkenzeller, RFID HANDBOOK: FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS AND IDENTIFICATION (Rachel Waddington trans., John Wiley & Son, Ltd. 1999).

[51] Munir Kotadia, *Government may regulate RFID use*, ZD Net News, *at* http://news.zdnet.co.uk/business/legal/0,39020651,39115376,00.htm. *Cf.* EPIC's observation that the RFID

gaps arranged in parallel configuration. But, whereas the barcode has had success[52] over the past twenty years, its shortcoming has been its low storage capacity and the fact that it cannot be reprogrammed.[53] Only with recent the technological developments discussed above, has RFID technology been considered a replacement for barcodes. However, as it becomes apparent from the discussion below, RFID technology is much more than an "improved barcode," not only because it does have high storage capacity and ability for reprogramming, but also because of its miniature size and the accompanying tracking ability.

Any RFID system is always made up of two components: (1) a transponder (i.e., a "tag") and (2) an interrogator (i.e., a "reader").[54] The tag is located on the object to be identified, and the reader is the device that reads and/or writes unto the tag. *See* Figure 1 below.[55] The reader typically contains a transmitter and a receiver to send and receive data, respectively, a control unit to manipulate the data, and a coupling element

---

technology represents a "fundamental increase in the complexity of cyberspace or as an extension of the Internet and electronic computer networks, rather than as an improvement over bar codes. Although the use of RFID to overcome the logistical limitations of the bar code system has been a major driver of commercial implementation, RFID applications clearly go far beyond anything ever envisioned in supply chain and inventory management."

[52] Brad Stone, *In Your Cereal?*, Newsweek (Sept. 29 issue), *available at* http://msnbc.msn.com/id/3068859/ (reporting that barcodes save the food industry $17 billion per year, or 50 times the savings initially forecast).

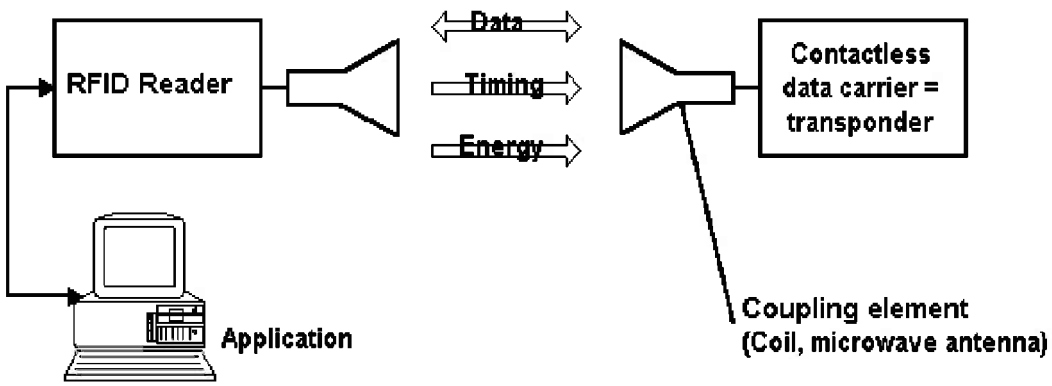
[53] FINKENZELLER, at 1.

[54] For a quick introduction to RFID technology, *see* Raghu Das, *RFID Explained*, Free IDTechEx White Paper, *at* http://www.idii.com/wp/IDTechExRFID.pdf.

[55] The "Energy" arrow in Fig. 1, represents energy that is being supplied to a passive tag. Tags with batteries may not need this, or at least need not rely solely on the Reader to provide energy. For an introduction to the distinction between passive and active RFID technology, *see Part 1: Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility*, *at* http://www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf (Active RFIDs can have a range of 100 meters or more, while passive RFIDs typically have a range of 3 meters or less), Alorie Gilbert, *RFID goes to war*, CNET News.com (Mar. 22, 2004), *at* http://news.com.com/2008-1006_3-5176246.html ("On the passive side, the reader read best at about 30 feet .... On the active side, it is already reading at 300 yards").

to communicate with a tag. Moreover, the reader can forward the data it receives to another system such as a computer where the data can be analyzed by a user.[56]

Figure 1. The reader and transponder/tag are the main components of every RFID system



> The tag typically contains a coupling element to communicate with the reader, and an integrated circuit to manipulate and store the data. The reader first sends energy to the tag. The reason for sending energy is to provide "power" to the tag so it can operate and send data back. Some tags already have a battery, in which case such energy is not needed. Depending on the kind of RFID system, the reader can also read and/or write data to the tag. It is this reading and/or writing ability of the reader and the data storing and sending ability of the tag that constitute the heart of any RFID system. Such a setup allows the reader to communicate with a tag and thus obtain information about the object to which the tag is attached. Since the tag can only store the data that the reader writes unto it (or the data that was originally stored unto it in a factory), such information is rather limited to the most basic aspects of the object to which the tag is attached—the kind of object it is, its price, etc. But importantly, the reader can track an object by tracking the tag. Tracking is based on the reader having the ability to read a tag in its vicinity.
>
> Typically, such tracking occurs up to distances of five meters,[57] although optimal tracking is on the order of tens of centimeters.[58] The reader can read the tag's data in

[56] Finkenzeller, at 8.

about half a second and the tag can store anywhere from 16 to 64 kilobytes of data. The readability of the data is considered good and it is not greatly affected by dirt, covering, direction or position.[59] The frequency range of most RFID systems is between 100kHz to around 30 MHz.[60] Moreover, readability of such data by people and unauthorized copying or modification is considered very difficult.[61] Of course, these specifications are true as of today's state of technology, and it is not clear that unauthorized copying or modification will not be feasible in the future, where rogue readers might corrupt targeted tags.

However, to prevent any such corruption, secure RFID systems employ authentication protocols. Such protocols work by checking knowledge of a secret (cryptographic) key. Appropriate algorithms can be used to prevent the secret key from being cracked.[62] Thus, secure RFID systems can provide defenses against such practices as the unauthorized reading of a tag in order to duplicate and/or modify data, or the eavesdropping on radio communications between a reader and a tag.[63] And yet, it is worth noting that even if a transmission is encrypted, the transmission may be commercially valuable as it could be used to uniquely identify people and things.[64]

---

[57] *Cf.* footnote 18 (citing articles that give ranges of 100 meter and 300 yards for active tags, and anywhere from 3 meters to 30 feet ≈ 10 meters for passive tags).

[58] *Id.* at 7 and 276.

[59] Although, RFID technology doesn't work well around metals and liquids. Alorie Gilbert, *RFID goes to war*, CNET News.com (Mar. 22, 2004), *at* http://news.com.com/2008-1006_3-5176246.html.

[60] FINKENZELLER, at 7. But, according to *Part 1: Active and Passive RFID...* in footnote 18, active RFID readers operate up to the range of 2400 MHz.

[61] *Id.* at 7. Finkenzeller actually considers unauthorized access to data "impossible" in Table 1.1., but that may be overstating it.

[62] *Id.* at 151.

[63] *Id.* at 151.

[64] I would like to thank Chris Hoofnagle for making this suggestion.

These are just the basic features of a typical RFID system. High-end RFID systems have more sophisticated features that are beyond the scope of this paper. However, the basic features discussed above are the key to understanding the debate RFID technology has initiated with respect to privacy concerns.

Lastly, today a typical RFID tag costs about $0.50,[65] but prices vary depending on the sophistication of the tag—for example, whether the tag can be reprogrammed or whether it can only be read. Towards the end of this decade, RFID tags are expected to cost a fraction of this price.[66] The market for RFID technology has been estimated at one to two billion dollars at the beginning of this decade and is expected to surpass ten billion dollars at the close of the decade.[67]

Analysis of Privacy Issues Concerning RFID

Privacy is one of the hottest issues surrounding RFID technology today.[68] The main concern is the technology's ability to track the objects that tags are attached to.[69]

---

[65] Tom Krazit, *Despite cost pressures, RFID tags gaining*, InfoWorld (Jun. 8, 2004), *at* http://www.infoworld.com/article/04/06/08/HNrfidtagsgain_1.html.

[66] John Carroll, *The Wonders of RFID*, ZD Net News (Jan. 12, 2004), *at* http://zdnet.com.com/2100-1107_2-5139151.html (reporting that the current price of $0.20 cents per tag, which doesn't include the cost of the antenna and packaging for the chip, will go down to $0.05 cents per tag); Matt Hines, *Wall-Mart Turns on Radio Tags*, Apr. 30, 2004, CNET News.com (Apr. 30, 2004), *at* http://news.com.com/2100-1012_3-5202240.html (reporting that "tags have dropped from an average of 60 cents per unit to roughly 20 cents per tag over the last year, and .. [the] EPC standards adoption [is expected] to drive that price down even further").

[67] Jack M. Germain, *RFID Tags and the Question of Personal Privacy*, TechNewsWorld, *at* http://www.technewsworld.com/story/32161.html, Finkenzeller, at 1, Jay Cline, *RFID Privacy Scare is Overblown*, Computerworld (Mar. 15, 2004), *at* http://www.computerworld.com/securitytopics/security/story/0,10801,91125,00.html; *Cf.* Matt Hines, *HP debuts RFID services*, CNET News.com (May 10, 2004), *at* http://news.com.com/2100-1011_3-5209394.html (HP estimates that the RFID market will grow to more than $3 billion by 2008).

[68] It certainly seems that way, in large part to the efforts of many privacy advocate groups. There are, of course, other issues that are just as important on the technological side of RFID, but which don't capture the public imagination to the same extent. *See* Mark Palmer, *Overcoming the challenges of RFID*, ZD Net News (Feb. 27, 2004), *at* http://zdnet.com.com/2100-1107_2-5165705.html (arguing that realizing the benefits of RFID technology requires addressing three key issues: 1) The need to change business processes that RFID deployments will prompt, 2) software architectures require an overhaul to deal with the influx of RFID generated data, and 3) RFID standards, both industry and de facto, have to mature).

By tracking objects, RFID readers can also track people who have contact with these objects, for example, the shirts or shoes people wear, the wallets they carry, and so on. Of course, such trackable tags are not limited to being attached to objects, because they can also be implanted in people. The small size of RFID tags—some on the order of a *grain of sand* [70]—makes their intrusion in the human body minimal. Based on these facts, privacy advocates have expressed legitimate concerns regarding the threat to privacy that RFID technology presents.

A. Tracking Objects: The Typical Scenario

RFID is typically used to track objects. Tracking permits retailers to slim inventory levels and reduce theft, which by some estimates reaches $50 billion per year.[71] Thus, tracking is performed out of economic considerations and not the invasion of privacy. Yet, the *potential* abuse in tracking objects, and thus people, has given rise to spirited debate regarding RFID technology.

A seemingly innocuous example of involves tracking books in a library. Some libraries have already, and some are only in the planning stages, of introducing RFID technology to track books and other library items. The advantages of such an

---

[69] For an sound analysis of privacy issues surrounding location-tracking technology, *see* James C. White, *People, Not Places: A Policy Framework for Analyzing Location Privacy Issues*, Masters Memo Prepared for the Electronic Privacy Information Center, 2003.

[70] In numerous articles, the size of an RFID tag is described as being on the order of a "grain of sand," but this is somewhat misleading. While the integrated circuit of an RFID tag can be on the order of a grain of sand, its coupling element, namely, the antenna, is typically a lot bigger. *See Future RFID technology - Real Soon Now* in RFID TAG PRIVACY CONCERNS, *at* http://www.spy.org.uk/cgi-bin/rfid.pl (showing pictures of RFID integrated circuits, the relative size of the circuits to their antennas, and pointing out that "The RFID chips, although physically 'like grains of sand' need much larger antennas to grab enough electrical energy to power them up and to transmit their serial ID information."). And yet, as Chris Hoofnagle points out, tags may shrink even further, despite antenna limitations, because the product itself could become an antenna.

[71] Declan McCullagh, *RFID tags: Big Brother in small packages*, CNET News.com (Jan. 13, 2003), *at* http://news.com.com/2010-1069-980325.html.

implementation are easy to recognize: helping staff to track library items, whether missing or misplaced, deterring theft and helping patrons check out books faster.[72]

However, a concern that arises is what happens when the tagged items leave the library? Theoretically, tags can be deactivated once they leave a library, but, as critics point out, if such devices can be turned off, they can also be turned on. This means that anybody from small-time computer hackers to law-enforcement could track the whereabouts of patrons who just checked out the "The Communist Manifesto," or "Mein Kampf," or a book on bomb-making.[73] As Lee Tien, an attorney with the Electronic Frontier Foundation points out, "what one reads is often something that society in general will make judgments on."[74] On the heels of such judgments could follow greater surveillance of library patrons thus threatening the privacy of such patrons.[75]

Tracking through books might be considered only a mild threat to privacy, since people typically don't carry their books everywhere with them. But money is a different issue. People typically carry their wallets everywhere with them. Money now poses a risk to privacy because governments are considering embedding RFID tags in currency. The main reason for embedding tags in currency would be to combat counterfeiting and

---

[72] Joe Garofoli and Pamela J. Podger, *Ethics of library tag plan doubted*, The San Francisco Chronicle (Oct. 6, 2003), *available at* http://www.worthingtonlibraries.org/Trends/TrendTrackingDetails.cfm?id=50

[73] *Id.*

[74] *Id.*

[75] Obviously, anytime a patron checks out any library items, such a transactions is stored somewhere in a database and thus this information is subject to misuse by the same hackers and law enforcement officials as when RFID technology is involved. However, the difference is that RFID technology allows for those interested to follow patrons after they have left the library and not merely at the point of check-out. Furthermore, laws or opinions of attorneys general in all 50 states provide some protection for library circulation records from police inspection. *See* Chris Jay Hoofnagle, *Digital Rights Management: Many Technical Controls on Digital Content Distribution Can Create A Surveillance Society*, 5 Colum. Sci. & Tech. L. Rev. (Forthcoming Spring 2004).

money laundering, but it could also be used in other situations such as kidnappings and ransoms, or to help out blind people.[76]

The European Central Bank is interested in such currency-cum-tags because such tags could contain a note's serial number and date and place of origin, not to mention have the ability to be tracked as a note travels around Europe.[77] The applications of such money are seemingly boundless. For example, there is speculative talk of GPS-enabled Euros which vibrate discreetly when a taxi driver is taking a customer for ride, or self-destructing currency for compulsive gamblers, or stress-sensitive currency when a note has been rolled tighter than a pre-determined radius indicating drug use.[78]

US currency could also be embedded with such RFID tags, according to a Federal Reserve official.[79] Tracking technology would allow the government to tax possession of dollar bills. Thus, the longer a person would hold currency without depositing it in a bank account, the less cash value the note would have. Put another way, dollars would have automatic expiration dates. Such possession taxation would arguably discourage "hoarding" currency, deter black market and criminal activities, and boost economic stability during deflationary periods when interest rates approach

---

[76] Lester Haines, *EC moots trackable cyber euro*, The Register (May 23, 2003), *at* http://www.theregister.co.uk/2003/05/23/ec_moots_trackable_cyber_euro/. As the article points out, such tagged money could be further enhanced to talk to blind people and confused octogenarians: "No dear, I'm a fifty. Put me back in your purse and look for a five."

[77] *Id.*

[78] *Id.*

[79] Declan McCullagh, *Cash and the 'Carry Tax'*, Wired News (Oct. 27, 1999), *at* http://www.wired.com/news/politics/0%2C1283%2C32121-1%2C00.html.

zero.[80] Yet, despite the economic efficiencies of these creative[81] uses of money, the loss of anonymity in using cash raises troubling privacy issues.

A person can always leave his wallet behind if he does not want to be tracked through his currency. However, by embedding RFID tags in tires, avoidance of tracking is made a lot more difficult. In wake of the Firestone/Ford Explorer debacle, US Congress passed the Transportation, Recall, Enhancement, Accountability and Documentation Act (TREAD). This act mandates that car makers track closely tires from the 2004 model year onward. As a result of this act, Michelin decided to embed RFID tags in tires to make tracking easier. The tags store the tire's unique ID, which can be associated with the vehicle's identification number. But the tag can also store information about when and where a tire was made, its maximum inflation pressure, size, and so on.[82]

People who spend a significant amount of their time in the car could easily be tracked through their tires—not to mention other car parts that will also probably posses their own individual tags. Of course, the tag by itself will not be able to tell who is driving the car, but by cross referencing other tags that a driver possess, say, her currency or the books she just checked out from the library, even driver identification would seem possible. Yet, for all these wonderful possibilities, such tracking remains years if not decades in the future—assuming it will happen at all. As of today, it does not appear

---

80 *Id.*

81 These uses are "creative" in the sense that they may not be practicable. As one author observes that "[t]he technical problems presented in trying to discriminate each individual RFID tag in a stack of banknotes are formidable. How do you stop the RFID antennas from interfering with each other when hundreds of them might be stacked one on top of the other ? Random placement of RFID tags in a banknote would surely cause lots of counterfeit false alerts, they will have to be in a standard position, only separated by the two halves of the thickness of adjacent pieces of banknote paper i.e. much less than the wave length of the radio signals." *RFID in banknotes unlikely to work as feared* in RFID TAG PRIVACY CONCERNS, *at* http://www.spy.org.uk/cgi-bin/rfid.pl.

82 News, *Michelin Embeds RFID Tags in Tires*, RFID Journal (Jan. 17, 2003), *at* http://www.rfidjournal.com/article/articleview/269/1/1/

technologically nor economically feasible to track people through objects they are near to.[83] However, this does not mean that individuals interested in protecting their privacy should not take a preemptory approach before such RFID uses become entrenched.

Tracking People: A Controversial Proposition

It one thing to track objects, and through those objects to track people, but tracking people directly raises more serious privacy risks. Tracking people directly is already happening in hospitals and in the work place. In Singapore, in wake of the SARS scare, hospitals began tracking visitors, patients, and staff in order to determine with whom a suspected SARS patient had contact.[84] This kind of tracking uses cards with embedded RFID tags. Readers are placed around the hospitals, which is divided into several interrogation zones. When a card carrying individual walks around the hospital, his every movement is tracked. However, in this particular case, since the incubation period for SARS is 10 days, the RFID system stores information on visitors up to 21 days, after which time the tracking information is deleted.

Carrying an RFID card may can be invasive with respect to privacy to the extent that a person decides to carry such a card (or is required to do so for employment reasons or for practical reasons such as entering government buildings, patronizing bars and restaurants, or traveling in rented cars, trains, or airplanes). But, going a step further, one RFID company wants to tag people directly.[85] VeriChip makes subdermal

---

[83] Mocking the privacy concern of some activists, one author noted the following: "In this report [submitted by privacy groups], RFID readers on freeways read tags embedded in shoes and transmit the information to satellites. Yes, shoe-tracking satellites circling the globe." Jim Harper, *Privacilla Criticizes Anti-Commercial Screed Against RFID Tags*, Privacilla Organization (Nov. 14, 2003), *at* http://www.privacilla.org/releases/press027.html.

[84] News, *Singapore Fights SARS with RFID*, RFID Journal, *available at* http://www.rfidjournal.com/article/articleview/446/1/1/

[85] Demir Barlas, *Let's Get Chipped*, Line 56 (Apr. 25, 2003), *at* http://www.line56.com/articles/default.asp?NewsID=4609

tags that are usually implanted in the tricep. One VeriChip spokesman praised the potential benefits of the technology, revealing that he himself had been "chipped"—"It's a simple, painless procedure, like getting a shot."[86] Moreover, the spokesman noted that RFID technology is "not like a GPS device, you need close proximity to a scanner to read the chip."[87] This, however, is exactly the point of contention between privacy activists and the RFID technologists. It is the potential fear that RFID tags could function like GPS devices, either by having multiple readers track them as they move about—as in the hospital example discussed above—or by the tags themselves having the potential to relay their position from anywhere. Thus, this kind of RFID use becomes especially worrisome since subdermal tags are difficult, if not impossible, for tagged individuals to remove in order to prevent tracking.

Another related example is tracking people at work, specifically, at law firms. In order to increase efficiency, one New York law firm, Akin & Smith, LLC, installed an RFID analogous finger sensing device that is kept at a secretary's desk to track attorney and staff comings and goings. One managing partner at the firm concluded that "It keeps everyone honest," and that it has been "very successful" in increasing productivity.[88] Perhaps betraying a voyeuristic aspect to the system, the partner admitted that he "like[s] to see how long they [lawyers and staff] take for lunch."[89] This system's tracking ability is analogous to RFID technology and raises the same concerns regarding privacy, namely, being monitored constantly, even if it is during working hours. A boss might want to know why an employee spends so much time in a restroom, or

---

86 *Id.*
87 *Id.*
88 Kris Maher, *Companies Monitor Workers With New Tracking Systems*, RFID Privacy Organization, *at* http://www.rfidprivacy.org/papers/smith/index.htm
89 *Id.*

why that employee is not in his office working? Or, it might interest the boss to know the individuals with whom the employee is associating or possibly organizing.

B. Tracking by the Private Sector: Economic Streamlining

From the private sector point of view, the purpose of tracking is to increase economic efficiency. Wal-Mart, a retailing giant, is pushing its top 100 suppliers to adopt RFID technology by the end of 2004 and the rest of its suppliers to do so by 2005.[90] This is part of Wal-Mart's drive to have every carton and palette it receives carry an RFID tag. The savings to Wal-Mart could be huge, given its economies of scale. Precise tracking of supplies could cut down on the needed inventory storage by 5%, and reduce the corresponding labor costs anywhere from 7.5% to 20%, which translates to millions of dollars in savings.[91] With these economic potentials in sight, some maintain that the private sector has maintained a rather casual attitude towards privacy risks.[92] Yet, recently, recognizing consumer concern about privacy, Linda Dillman, Wal-Mart's chief information officer, said in a statement that "we want our customers to know that RFID tags will not contain nor collect any additional data about consumers. In fact, in the foreseeable future, there won't even by any RFID readers on our stores' main sale

---

[90] Barnaby J. Feder, *Wal-Mart Plan Cost Suppliers Millions*, The New York Times Online (Nov. 10, 2003), *available at* http://www.nytimes.com/2003/11/10/technology/10radio.html (Although the plan will cost millions, Wal-Mart said it would confine the initial rollout of the technology to three distribution centers and 150 stores in Texas). Moreover, Wal-Mart has suffered some setbacks regarding this ambitious plan. Ron Coates, *Setback for Wal-Mart's RFID project*, Silicon.com (Mar. 29, 2004), *at* http://zdnet.com.com/2100-1103_2-5181244.html.

[91] Feder, *at* http://www.nytimes.com/2003/11/10/technology/10radio.html. Such efficiency will also probably result in a loss of jobs, but that is another issue.

[92] Andy McCue, *U.K. retailer tests radio ID tags*, CNET News.com (Oct. 16, 2003), *at* http://news.com.com/2100-1039-5092460.html. A rather passionate privacy advocate, Katharine Albrecht, has stated that: "retailers have simply chosen to ignore the serious privacy and health concerns of their customers." *Marks & Spencer Moves Forward with RFID Trials CASPIAN says, "M & S responsible, but setting a dangerous precedent"*, CASPIAN web site (Oct. 15, 2003), *at* http://www.spychips.com/marks_and_spencer.htm.

floors."[93] Thus, RFID proponents have responded to pressures from consumer advocacy groups.

In the United Kingdom, the retailer Marks & Spencer conducted a four week trial run of RFID tags contained within throwaway paper labels, but not embedded in, a selection of men's suits, shirts, and ties.[94] The RFID tags hold only the number unique to each garment and respond only to a Marks & Spencer secure reader. A Marks & Spencer spokeswoman commented that "[w]ith the ability to read product details on the RFID tags at different points in the supply chain, the information can be used to ensure that the right goods are delivered to the right store at the right time," whereby customers can benefit from better availability of the goods they want when they shop.[95] Perhaps the most significant point regarding privacy is that "[i]rrespective of the method of payment, no association is made between the information on the [tags] ... and the purchaser."[96] Thus, Marks & Spencer has found a way to balance economic efficiency and privacy concerns.

As mentioned above in Part I, the private sector has also enlisted the help of academia to develop RFID technology. The Auto-ID Center at MIT embarked on a four year collaboration with dozens of blue-chip companies to develop and field test a new breed of computer networks that can track the location of everyday objects, such as razors and shoes.[97] Thus, in addition to expanding across borders, RFID technology has extended across disciplines to make the technology more standardized and efficient

---

[93] Matt Hines, *Wal-Mart Turns On Radio Tags*, CNET News.com (April 30, 2004), *at* http://news.com.com/Wal-Mart+turns+on+radio+tags/2100-1012_3-5202240.html.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] Alorie Gilbert, *MIT winds down radio tag activity*, CNET News.com (Oct. 23, 2003), *at* http://news.com.com/2100-1008-5095957.html.

in tracking objects. Now that RFID technology is garnering more attention for its economic potential, the private sector is beginning to cope with privacy issues that are being constantly raised. Certain retailers and manufacturers like Tesco and Gillette have attracted criticism regarding tracking, while others like Wal-Mart have somewhat backed-off from their initial ambitious projects to push RFID technology to the forefront of implementation.[98] Although the private sector has responded to privacy advocate pressures, it appears that an increase in RFID technology use will be proportional to the number of privacy concerns that surface.

C. Tracking by Government: Big Brother

Tracking by the private sector is scary enough for some, but even more troubling is the potential tracking by the government. The U.S. Department of Defense recently announced a new policy of requiring its suppliers to use RFID tags.[99] The new policy requires that by January of 2005, all suppliers embed passive RFID chips in each individual product, or at least at the level of cases or pallets.[100] This policy applies to everything except bulk commodities like sand, gravel, or liquids.[101] The purpose behind the policy is supply-chain and business process streamlining. Specifically, the goal is to stop critical shortages of ammunition, fuel, and water, which plagued American

---

[98] *Id.*

[99] Matthew Broersma, *Defense Department drafts RFID policy*, CNET News.com (Oct. 24, 2003), *at* http://news.com.com/2100-1008-5097050.html. According to Alan Estevez, interviewed by Alorie Gilbert, *RFID goes to war*, CNET News.com (Mar. 22, 2004), *at* http://news.com.com/2008-1006_3-5176246.html, the Department of Defense has 46,000 suppliers, and this RFID policy touches all of them.

[100] According to Alan Estevez, the Department of Defense has probably spent $100 million over the last 10 years on active RFID implementation. Gilbert, *RFID goes to war*, CNET News.com (Mar. 22, 2004), *at* http://news.com.com/2008-1006_3-5176246.html.

[101] The FDA is also becoming involved with RFID technology: "The Food and Drug Administration recently encouraged the pharmaceutical industry to use the technology to help curb the counterfeit drug trade," Alorie Gilbert, *Tracking Tags May Get Congressional Scrutiny*, CNET News.com (Mar. 24, 2004), *at* http://news.com.com/2100-1008_3-5178859.html; Alorie Gilbert, *FDA endorses ID tags for drugmakers*, CNET News.com (Feb. 18, 2004), *at* http://att.com.com/2100-1008-5161220.html.

troops during and after the current Iraqi war.[102] While the DOD's policy will affect soldiers and not non-military personnel, the government is giving RFID technology a big push.

The approach taken by the DOD differs from the private sector in that it requires suppliers to embed tags in each product as opposed to merely attaching a tag to a product, in which case, the tag can be easily removed. Embedding leads to mandatory tracking since a lot of the time a person cannot remove a tag from an embedded product, either because its not physically possible to do so without destroying the product itself or because the tags are so small and so prevalent that they cannot, practically speaking, be removed. Thus, the DOD's policy might give rise to more troubling privacy issues than it otherwise would have, had it allowed for RFID tags to be removable.[103]

Some state legislatures have preemptively joined the RFID/privacy debate. For example, California's Senate Subcommittee on New Technology has held hearings[104] to inquire whether embedding RFID tags could invade a consumer's privacy.[105] According to an industry study conducted by A.T. Kearney, an estimated $40 billion, or 3.5 percent of total sales, are lost each year due to supply chain information

---

[102] Alorie Gilbert, *RFID goes to war*, CNET News.com (Mar. 22, 2004), *at* http://news.com.com/2008-1006_3-5176246.html.

[103] But then again, there's no real reason why soldiers would need to remove RFID tags, since privacy in the context of the military is not as troubling as it is in the private sector.

[104] On April 29, 2004, the California state Senate voted to approve a measure (SB 1834) that sets privacy standards for use of RFID technology in stores and libraries. It passed the measure by a vote of 22 to 8. The bill now goes on to the Assembly where it will be head in June. Richard Shim, *Calif. Senate passes RFID measure*, CNET News.com (April 30, 2004), *at* http://news.com.com/2110-1008_3-5203428.html.

[105] Susan Kuchinskas, *California Scrutinizes RFID Privacy*, siliconvalley.internet.com (Aug. 15, 2003), *at* http://siliconvalley.internet.com/news/article.php/3064511; Alorie Gilbert, *Privacy Advocates Call For RFID Regulation* (Aug. 18, 2003), *at* http://zdnet.com.com/2100-1105_2-5065388.html.

inefficiencies.[106] Among the parties testifying at the hearing were representatives from the Association for Automatic Identification and Data Capture Technologies (AIM). In contrast to such privacy groups as Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), which stress the tracking ability and hence invasion of privacy by RFID technology, AIM has pointed out that the infrastructure costs for a government entity to track all its citizens would be astronomical and technologically infeasible.[107]

The government's involvement is not just limited to the United States. In the United Kingdom, the Parliament is expected to debate the use of RFID technology in the upcoming Parliamentary session.[108] One Labour MP, Tom Watson, posed the following question: "How can we regulate the information collected? For example, do I pick up product 'A' and 'B' before choosing 'C'? Why should they know all our musings?"[109] Moreover, Watson stated that "[t]hey [the 'unscrupulous retailers'] push our current data protection laws to the limit and therefore require a review by government."[110] Moreover, at least in Europe, RFID technology is also in tension with Section 8 of the Human Rights Act, which states that every individual has a right to privacy.

The problems associated with governmental invasion of privacy are poignantly addressed in such literature as George Orwell's *1984*, where the government controls individual thought by "tracking" every aspect of its citizens' lives. Although *1984* issues

---

106 *Id.*

107 *Id.*

108 Munir Kotadia, *Government may regulate RFID use*, ZD Net News, *at* http://news.zdnet.co.uk/business/legal/0,39020651,39115376,00.htm

109 *Id.*

110 *Id.* Watson noted that RFID tags "offer profound challenges to the civil liberties of people… [that's why] I'm going to try and secure a debate in parliament about them."

are far away from today's concerns regarding RFID technology in 2004, governmental abuse of information about its citizens in not that incredible. For example, unless sectoral privacy legislation prohibits it, a business owner can voluntarily provide customers' personal information to police, whether or not a crime has occurred.[111] Yet, such scenarios remain today largely unaddressed, but they are coming to the forefront of the RFID/privacy debate.[112] Perhaps more importantly, governments on both sides of the Atlantic are taking preemptive measures to address privacy issues before they become intractable.

The Complexity of RFID Tracking in Different Contexts

One conclusion that can be drawn from the above examples is that the idea of "tracking" is a complex one and that it is context dependent. For example, focusing just on tracking within one context, a retail store (and putting aside the more exotic[113] examples of tracking through tires, currency, clothes,[114] or embedding chips in people), numerous issues arise. Ari Schwarz, the associate director of the Center for Democracy and Technology, points out that "[t]he question is really what's it's [RFID technology] used for and how it's done, rather than the technology itself."[115] Schwarz adds that "[m]ost of the benefits out there comes on the back end, in the stock room, and most of the privacy concerns come when it [RFID] leaves the stock room." Thus, one must ask

---

111 *Id.*

112 Although, the FTC is currently seeking comments and requests to join a June 21 workshop looking at consumer uses and impacts of RFID technology. Richard Shim, *FTC to explore RFID consumer implications*, CNET News.com (Apr. 12, 2004), *at* http://news.com.com/2110-7343_3-5190155.html?part=rss&tag=feed&subj=news

113 For some more "exotic" examples of RFID use, *see* Ephraim Schwartz, *Reality Check*, InfoWorld (Feb. 13, 2004), http://home.netcom.com/~hal55/id55.html.

114 Matthew Broersma, *RFID Chips Sent to the Dry Cleaners*, ZD Net News (UK) (Aug. 12, 2003), *at* http://zdnet.com.com/2100-1103_2-5062542.html (reporting that chipmaker Texas Instruments announced a wireless identity chip for clothing which can survive the dry cleaning process).

115 Grant Gross, *RFID And Privacy: Debate Heating Up in Washington*, InfoWorld (May 28, 2004), http://www.infoworld.com/article/04/05/28/HNrfidprivacy_1.html.

whether privacy concerns should pertain to stock rooms to a lesser extent than the store premises where consumers are shopping, or if they should pertain at all to areas where consumers are not present?

In the same vein, tagging individual items cannot be conflated with tagging crates or palettes. As Simon Garfinkel, author of *Database Nation* and a former[116] member of Auto-ID Center's privacy advisory council points out, "RFID tags are currently being used in the supply chain for asset management and warehouse automation, not to track individual items."[117] And yet, Garfinkel observes that as "the price of the tags drops to five cents or less, companies will use them on consumer items."[118] This raises the issue to what extent is consumer privacy at risk today versus what it could be in the future? And is it fair to treat those companies that only use such tags in the supply chain in the same manner as those that tag individual items or use smart-shelves?[119]

Furthermore, aside from *where* tracking is done, there's the question of *what* type of tracking is being done. For example, are RFID tags used as a barcode substitute or do they go further and act as loyalty cards? In the former case, RFID should not raise substantially new privacy concerns, since some barcode proprietors can already[120] associate item purchase with a particular consumer if the consumer is not paying in

---

[116] As mentioned, the Auto-ID Center disbanded in late 2003, having fulfilled its mission. Alorie Gilbert, *MIT winds down radio tag activity*, CNET News.com (Oct. 23, 2003), *at* http://news.com.com/2100-1008-5095957.html.

[117] Jennifer Maselli, *Privacy Group Focuses on RFID*, RFID Journal (Aug. 26, 2003), *available at* http://www.rfidjournal.com/article/articleview/547/1/1/. *See Also* Alorie Gilbert, *Tracking Tags May Get Congressional Scrutiny*, CNET News.com (Mar. 24, 2004), *at* http://news.com.com/2100-1008_3-5178859.html

[118] Jennifer Maselli, *at* http://www.rfidjournal.com/article/articleview/547/1/1/.

[119] Alorie Gilbert, *'Smart shelf' test triggers fresh criticism*, CNET News.com (Nov. 14, 2003), *at* http://news.com.com/2100-1017-5107918.html.

[120] John Carroll, *The wonders of RFID*, ZD Net News (Jan. 12, 2004), *at* http://zdnet.com.com/2100-1107_2-5139151.html

cash.[121] In the latter case, RFID technology could be subject to the same restrictions a loyalty cards. There are already protections in place set out to guard data collected via loyalty cards.[122] However, some legislators believe that RFID technology is different in kind from anything that has come before, and thus the states of California, Missouri, and Utah have introduced legislation that deals with RFID technology specifically.[123] Similar legislation may also appear on the federal level.[124]

These are just some of the issues that come up in a single context of RFID tracking, namely, retail tracking. Similar and distinct issues will come up in different contexts, like tracking books, money, tires, medical patients, and employees. Unfortunately, many of these latter tracking scenarios that impinge on privacy are speculative, because they are either (as of today) technologically very difficult to realize or economically infeasible. Retail tracking provides perhaps the most concrete scenario, and yet even retail tracking is in its infancy. The most sound approach to addressing privacy concerns will have to examine each kind of tracking within a specific context, and a context that is developed enough to provide concrete, substantive solutions to burgeoning privacy risks.

For now, general guidelines, like the ones enumerated at the end of this paper, provide an approach that is at the same time not over-inclusive, because it does not

---

[121] Although RFID tags can act as barcodes, they can be read by readers, intended or not, from a distance, thus their use does not exactly raise the same privacy concerns.

[122] Mary Deibel, *Some Shoppers Just Aren't Buying Grocery Discount Cards*, SimplyFamily, *at* http://www.simplyfamily.com/display.cfm?articleID=grocery_discount.cfm

[123] Alorie Gilbert, *Tracking Tags May Get Congressional Scrutiny*, CNET News.com (Mar. 24, 2004), *at* http://news.com.com/2100-1008_3-5178859.html. *See Also* Jaikumar Vijayan, *Use of RFID Raises Privacy Concerns*, Computerworld (Sept. 1, 2003), *available at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,84515,00.html.

[124] *Id.* (noting that "A Democratic senator [Sen. Patrick Leahy, D-Vt] has called for a congressional hearing on [RFID] ... tracking technology that has alarmed consumer privacy advocates." And yet, a "hearing at the federal level is not likely before the end of the year, a Leahy representative said.").

brush over the unique issues within each context, and not under-inclusive, because it deals, on a general level, with issues that come up (to some extent) within each context. As RFID technology becomes more prevalent in use, more specific guidelines, and perhaps even rules, will have to be developed to cope, on a context-by-context basis, with privacy risks. The guidelines presented at the end of this paper, attempt to address legitimate risks raised by privacy advocates, but in such a way as to allow a potentially beneficial technology to develop while respecting the right to privacy that every one of us shares.

Conclusion

In some respects, the potential abuses of RFID's technology and the accompanying threats to privacy have become overstated. The most heated issues raised presently have to do with the *potential* abuse of RFID technology.[125] On the one hand this is beneficial because the debate anticipates potential issues that will have to be addressed eventually. On the other hand, some of the risks raised about continuous consumer or citizen tracking may have a deleterious effect on the further development of this nascent technology. The danger is that *potential* fears might negatively impact *actual* developments of this technology.

---

[125] *See* e.g. Scott McNealy, *Scott McNealy on RFID and Privacy, at* http://www.sun.com/aboutsun/media/presskits/nrf2004/BMscottmcnealyrfid.pdf (arguing that privacy concern is no greater than conventional mail, where "[w]e write our innermost thoughts, unencrypted, on a piece of paper, which we seal inside a thin paper envelope … [t]hen we write our name and address, and those of the recipient … [t]hen we put the whole thing in a tin box … [t]hen we trust a government worker to take that letter and somehow get it to another tin box somewhere else in the world … and you don't hear folks complaining about it [the potential privacy invasion]." *Cf.* Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 Stan. Tech. L. Rev. 2 (2004) (pointing out that "critics fear RFID system would expose consumers to needless risk by allowing tech-savvy burglars to inventory a victim's house from a distance. In some instances, RFID systems could also pose a fatal threat, if stalkers manage to adapt the technology to monitor a victim's belongings, embedded with RFID microchips, and track their whereabouts."), Helen Nissenbaum, *Symposium: Technology, Values, and The Justice System: Privacy As Contextual Integrity*, 79 Wash. L. Rev. 119 (2004) (noting that "[u]less RFID tags are designed specifically to allow for easy detection and disabling, discretion is removed from the customer and placed into the hand of information gatherers.").

In other respects, privacy advocates have so far made headway in dispelling private sector complacency about the inevitability of troublesome (mis)uses of RFID technology. Perhaps the most fundamental progress made by such advocates is the acknowledgement by RFID users that privacy is a legitimate concern.[126] However, further advocate success will have to take a more nuanced approach to addressing privacy concerns. For example, is the RFID technology used on individual items or is it used on crates or palettes? Is RFID technology used in places where customers have substantial contact with RFID tags, such as a store, or in places where no contact is made, such a warehouse? Are RFID tags used merely as barcode substitutes, or is data collected a la a loyalty card? And so on. The danger is in demanding too much of RFID users, such as when tags are only used in warehouses, or not enough, such as when tags are used for post-sale purposes.[127] Employment of RFID technology is complex and varied, and the response to protecting expectations of privacy shouldn't be any less so.

General Recommendations

There are several general guidelines that balance the economic potentials of RFID tags against the accompanying privacy concerns discussed in the examples above. One writer, Declan McCullagh, has made four such suggestions: (1) Consumers should be notified when RFID tags are present in what they're buying; (2) RFID tags should be disabled by default at the checkout counter; (3) RFID tags should be placed

---

[126] Matt Hines, *Wal-Mart Turns On Radio Tags*, CNET News.com (April 30, 2004), *at* http://news.com.com/Wal-Mart+turns+on+radio+tags/2100-1012_3-5202240.html ("'We can certainly understand and appreciate consumer concern about privacy,' Linda Dillman, Wal-Mart's chief information officer, said in a statement."); *See Also* News, *EPC Privacy Principles to Evolve*, RFID Journal (Dec. 8, 2003), *at* http://www.rfidjournal.com/article/articleview/678/1/1/.

[127] The use of RFID tags in post-sale use may be done for warranty purposes.

on the product's packaging instead of on the product when possible; and (4) RFID tags should be readily visible and easily removable.[128] The first and third suggestions serve to give a consumer notice of potential RFID tracking. As such, these suggestions are not inconsistent with what RFID technology users are trying to accomplish, namely, tracking objects as they move through the supply chain. Moreover, they provide a way for consumers to become aware of potential privacy risks and provide a means to protect their privacy. The second and fourth suggestions give the consumer the ability to prevent tracking outside of its intended area, namely, beyond the point of purchase. Again, this is not inconsistent with the intended RFID use; furthermore it provides a way for consumers to make sure that any purchased items will not be subject to misuse by RFID users or other parties.

Another suggestion is that RFID technology users respect the confidentiality of consumers.[129] For example, a store should notify a consumer if it wants to share consumer data with another vendor or possibly the government, whether for profit or for non-profit reasons. On a related note, data collectors should tell consumers when, where and how and for what purpose data was collected.[130] And finally, the ability of data collectors to manipulate such collected information should be limited if not outright prohibited.

---

[128] Declan McCullagh, *RFID tags: Big Brother in small packages*, CNET News.com (Jan. 13, 2003), *at* http://news.com.com/2010-1069-980325.html.

[129] Rakesh Kumar, *Interaction of RFID Technology and Public Policy*, RFID Privacy Workshop @ MIT: November 15, 2003 (Nov. 15, 2003), *at* http://www.rfidprivacy.org/papers/kumar-interaction.pdf.

[130] Simon Garfinkel, *An RFID Bill of Rights*, Technology Review, Oct. 2002, *at* http://www.simson.net/clips/2002.TR.10.RFID_Bill_Of_Rights.htm. *See Also* Catherine Albrecht, *RFID Right to Know Act of 2003*, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) web site, *at* http://www.nocards.org/rfid/rfidbill.shtml; Beth Givens, Testimony to Joint Committee on Preparing California for the 21st Century, California Legislature, Privacy Rights Clearinghouse (Aug. 18, 2003), *at* http://www.privacyrights.org/ar/RFIDHearing.htm.

These are but preliminary suggestions to take into consideration. The key is to balance the enormous economic ability of RFID technology to streamline the supply-chain side of business against the potential abuses of data tracking of consumers. This balance must be measured against the broader issue of regulation. As of now, the industry is fairly self-regulated,[131] but it does appear that the government is starting to get more involved.[132] Again, here a balance must be struck between a laissez-faire approach that might let tracking information abuse run amuck and a governmental regulation approach that might stifle this economically and technologically beneficial technology. Guidelines that attempt to strike this balance are provided below.

---

131 *See* Mark Roberti, *New Rules of the Game*, RFID Journal, *available at* http://www.rfidjournal.com/article/articleview/820/1/2/ arguing for self-regulation since "[i]n the end, no businessperson wants to lose a customer [and] ... [n]o CEO wants to see the company's brand tarnished or its stock price take a hit over bad publicity ... companies are not going to go around surreptitiously spying on their customers because if they do, the only revenue they will increase will be that of their competitors." *Cf.* John Wehr of RFIDnews.org, commenting that "corporations regularly commit appalling abuses of consumer privacy to little or no resistence"; and Peter Winer commenting that Mark Roberti's "argument works well for companies, but not for governments who can deploy RFID at will without fear of alienating the public," on RFIDbuzz.com (Mar. 12, 2004), *at* http://www.rfidbuzz.com/news/2004/rfid_and_privacy_market_or_legal_regulation.html

132 Claire Swedberg, *Sen. Leahy Voices RFID Concerns*, RFID Journal (Mar. 24, 2004), *at* http://www.rfidjournal.com/article/articleview/843/1/1/.

Proposed Guidelines For Use of RFID Technology: Enumerating the Rights and Duties of Consumers and Private Enterprises

Introduction

These Guidelines were prepared for EPIC (Electronic Privacy Information Center). Thus, they strive to coincide with EPIC's mission statement, which is "to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values."[133]

The guidelines are proposed to guide the use of RFID (Radio Frequency Identification) technology in order to balance private enterprise interests against consumer privacy interests. This means that these guidelines do not address protection of consumer privacy from any governmental action. Rather these guidelines seek to protect consumer privacy from private, namely, business enterprises. Protection against government invasion of privacy is assumed to be protected by the 4th Amendment and other Constitutional and statutory provisions, such as The Privacy Act of 1974, The Electronic Communications Privacy Act of 1986 (ECPA), The Foreign Intelligence Surveillance Act of 1978 (FISA), and the like.

In the balancing of consumer privacy interests and private enterprise interests, the latter are assumed to include but are not limited to efficiency gains in supply-chain improvements, transportation and logistics, manufacturing and processing, and security. Specifically, the following are examples where RFID technology may be employed:

Electronic article surveillance in clothing retail outlets
Protection of valuable equipment against theft
Controlled access to vehicles, parking areas and fuel facilities
Automated toll collection for roads and bridges
Controlled access of personnel to secure or hazardous locations

[133] EPIC mission statement: http://www.epic.org/epic/about.html.

> Time and attendance to replace conventional "slot card" time keeping systems
> Animal husbandry in supporting individualized feeding programs
> Automatic identification of tools in numerically controlled machines in order to facilitate condition monitoring of tools, for use in managing tool usage and minimizing waste due to excessive machine tool wear
> Identification of product variants and process control in flexible manufacture systems
> Electronic monitoring of offenders at home Vehicle and anti-theft systems and car immobilizer[134]

Consumer interests in protecting privacy vary widely. Generally speaking, they include but are not limited to such practices as tracking of consumers through RFID tags, using information gathered by RFID systems without the knowledge and choice of consumers, and sharing of that information with third parties. Specifically, the following are examples, from a privacy perspective, when RFID technology may be misused:

> Tracking individuals via the tagged items they carry, posses, own, etc.
> Profiling individuals by associating personal information with tag data
> Reading of individual's tags by third parties
> Hidden use of RFID technology, whether tags or readers, without the knowledge or consent of individuals
> Unique Identifiers for just about any object that can allow tracking, profiling, and other privacy invasive practices
> Massive data aggregation allowing profiling

These guidelines are divided into three parts. Part I addresses the duties of private enterprises that use RFID technology in an analogous way to barcodes. Hence, it imposes the minimum and least burdensome requirements on such RFID users, recognizing the above listed advantages that RFID technology can provide while at the same time addressing privacy concerns. Part II, addresses the duties of private enterprises who go a step further and use RFID technology in an analogous way to loyalty cards, where personal information is associated with data stored on RFID tags to

---

[134] Kumar, Rakesh, *Interaction of RFID Technology And Public Policy,* Paper presentation at RFID Privacy Workshop @ MIT, Massachusetts (Nov. 15, 2003), *available at* www.rfidprivacy.org/papers/kumar-interaction.pdf.

potentially obtain a profile of a consumer. For example, in this part written consent is required from a consumer—unlike when a private enterprise in Part I is merely collecting information that is aggregate in nature and does not personally identify an individual. Finally, Part III states the rights of consumers who are exposed to RFID technology and incorporates the duties stated in Parts I and II.

One important observation must be made regarding the use of the words "right" and "duty" throughout these guidelines. These are words with legal overtones, meant to define the relationship of private enterprises to consumers, but they are also used in such a way as to most clearly convey their ordinary plain English usage. The word "right" is correlative of the word "duty." That is, both words exist together as a pair. Thus, if one person has a "right," another person necessarily has a "duty," otherwise a "right" without a "duty" is meaningless—and vice versa. One word expresses the relationship of person A to person B, while the other word expresses the relationship of person B to person A. The guidelines are structured in such a way as to highlight such relationships.

For example, the guidelines impose a "duty" on private enterprises to give consumers notice of RFID tag presence. With this "duty" comes the correlative "right" of consumers to have notice of RFID tag presence. The guidelines express notice as a "duty" to emphasize the obligation a private enterprise has towards a consumer. Thus, the focus here is on the private enterprise and what it must do for the consumer. Conversely, the "right" of a consumer to access information gathered by an RFID system is expressed as such to emphasize what a consumer can do given the correlative "duty" of a private enterprise. Thus, the focus here is on the consumer.

Definitions

"RFID" means Radio Frequency Identification.

"Tag" means a portable device, capable of receiving data from or transmitting data to a Reader.

"Reader" means a device, capable of reading data from a tag or transmitting data to a RFID tag.

"Individual" means any human that comes in contact with a product that has attached to it or contains an RFID tag.

"User" means an RFID operator, such as a store, warehouse, hospital, and the like, who employs RFID technology, including RFID readers and tags.

"Premises" means a store, a warehouse, a hospital, or any other such equivalent space that encompass RFID tags and the readers that communicate with them.

Guidelines

I. Duties of A User Employing RFID Systems That Do Not Gather Data About Individuals

A. A user employing an RFID system shall:

1. Give notice to an individual of tag presence, whether through labels, logos, or equivalent means, or through display, either at the place where a tagged item is stored, such as a shelf or counter, or at point of sale, such as a cash register. The notice shall be reasonably conspicuous to the individual.

2. Turn off tags before the completion of sale of a tagged item, where turning off a tag means disabling it permanently, unless an individual chooses to leave it active for such benefits as warranty tracking, loss recovery, or compliance with smart appliances. If the choice of an individual is not known, by default, a tag shall be turned off. Once a tag is turned off it cannot be turned on again without the consent of an individual.

3. Attach tags to items in such a way as to allow for the easiest possible removal of tags.

4. Designate at least one person who is accountable for the user's compliance with these guidelines.

B. A user employing an RFID system shall not:

1. Track the movement of individuals via tagged items on the premises or outside the premises where an RFID system is employed to obtain individual shopping habits or any other such information obtainable through tracking, even upon suspicion of such activities as fraud or shoplifting.

2. Record or store tag data from tags that do not belong to the user, or from tags that have been already purchased.

3. Coerce individuals to keep tags turned on after purchase for such benefits as warranty tracking, loss recovery, or compliance with smart appliances.

II. Duties of A User Employing RFID Systems That Can Gather Personal Data About Individuals

A. A user employing RFID tags in such a way as to gather data about individuals, in addition to the duties listed above in section I, shall:

1. Obtain written consent from an individual before any personally identifiable information of the individual, including name, address, telephone number, credit number, and the like, is attached to, stored with, or otherwise associated with data collected via the RFID System and at least:

   a. Inform individuals about the purpose of associating gathered data with personal information and specify that purpose before such attaching, storing, or association.

   b. Inform individuals about the scope of use of gathered data, whether the use is limited to the user's own interests or whether it extends to third parties.

2. Obtain separate written consent from an individual before any personally identifiable information about the individual collected by an RFID system is shared with a third party.

3. At least not require individuals to provide unnecessary personal information as a precondition of a transaction and allow individuals who so desire to enroll anonymously in any RFID data gathering project.

4. Take reasonable measures to ensure that any individual data collected via an RFID system is transmitted and stored in a secure manner, and that access to the data is limited to those individuals needed to operate and maintain the RFID system

5. Keep gathered data accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

6. Keep data only as long as it is necessary for the purpose for which the data was associated with personal information

7. Make readily available to individuals, through the internet or other equivalent means, specific information about its policies and practices relating to its handling of personal information. Any personally identifiable information itself shall be provided to an individual upon written request of the individual in a secure manner.

III. Rights of An Individual When RFID Systems Are Used

A. An individual shall have the following rights in addition to duties of the user listed above in sections I and II:

1. To access data containing personally identifiable information collected through an RFID system and the opportunity to make corrections to that information

2. To have tags removed from tagged items when it is reasonably practical to do so without compromising or destroying the item itself.

3. To challenge the compliance of users employing RFID systems with the person who is accountable under Section I when any of the above listed duties are not fulfilled or rights are violated.

Web Sites

The following are some useful web sites to further refine RFID and privacy guidelines.

Electronic Privacy Information Center (EPIC)

Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)

Privacy Rights Clearinghouse (containing links to numerous privacy organizations)

Canadian Standards Association (CSA). 1995. "Model Code for the Protection of Personal Information". CAN/CSA-Q830-1995 Rexdale: CSA.

Organization of Economic Cooperation and Development, 1980

RFID Privacy Workshop @ MIT: November 15, 2003 (containing numerous RFID/privacy sources)

Association for Automatic Identification and Mobility (AIM) (industry trade group)

EPC Global (standards setting organization)

Electronic Frontier Foundation

Lexis.com (containing CA, MO, and UT RFID bills introduced in the 2004 session)

FTC (upcoming RFID workshop)