Preserving Privacy in RFID Deployment

RVS-Occ-04-01

RVS, Faculty of Technology, University of Bielefeld

Jan E. Hennig *

Bielefeld, 2004-03-23

Radio Frequency Identification, RFID, is an item-tagging technology which interests suppliers and retailers. RFID has potential to revolutionise supply chain management but also some potentially distressing social implications. When used inappropriately, RFID is capable of reducing or eliminating customer anonymity, thereby damaging privacy and threatening civil liberties.
I begin with an introduction to the technological background. Second, I explain pros and cons by means of some example scenarios and, third, outline how this technology may be introduced in a way that can preserve privacy.

Background

RFID technology has its roots in early "friend or foe" detection systems helping anti-aircraft gunners discern own from enemy aircraft to prevent "friendly fire" incidents [1]. RFID tags today are tiny computer chips, each connected to a miniature antenna, that can be attached to physical objects. After the technology had been introduced in civil aviation and container logistics it became used in road traffic systems during the 1970s, e.g., in Austria every lorry carries a box in the driving cab that transmits a serial number when a toll bridge is passed along the way [2]. All such transponders are active, i.e. connected to their own power supply.

Passive transponders were developed next. They need no power supply of their own, relying solely on the radio energy transmitted by a reading device for powering. Research began in the 1990s at the Massachusetts Institute of Technology, which called this technology "Auto-ID". Today many companies, especially large

*Thanks to Peter Ladkin and Sebastian Lisken for proof-reading and english language advice

ones such as Philips, Intel, Texas Instruments and many more are pushing forward the development of this technology. They are accompanied by “RFID user” corporations, among them Procter & Gamble, Gillette, Philip Morris, Marks & Spencer, Walmart and Metro, who are marking products from livestock to cream cheese with ID numbers for several reasons [3].

That is one of the key abilities of this technology: The chips are capable of transmitting their identification – an unique serial number. EPCglobal, a consortium consisting of more than 100 of the most influential companies, including government organisations [4], is supervising the electronic product code (EPC) allocation process to ensure that these numbers are globally unique and will remain so for hundreds of years. “Unlike the bar code, however, the EPC goes beyond identifying product categories – It actually assigns a unique number to every single item that rolls off a manufacturing line” [5]. “VeriSign, the company that maintains the Internet’s *.com* and *.net* domain registry, has been hired to run a new directory to be used to keep tabs on consumer goods using a technology known as radio frequency identification” [6]. Apart from this number, many chips are capable of storing, reading and rewriting some number of custom data bytes. But, clearly, there is no need to store voluminous data amounts on the chip itself to make tracking it a possibility. The unique number is enough for a computer linked to a reading device to look up or amend data linked to this particular unique number.

The second key feature of RFID is that no physical contact is required for reading because of the radio transmissions. Dependent on chip and antenna design, reading ranges vary from a few centimetres to a few meters for passive RFID tags. Contrary to claims that these distances are too short to track consumers, this is definitely possible: reader devices do not have to follow the RFID tag for it to be tracked. It is sufficient to install some reader devices at strategic points, e.g. bottlenecks such as doors or on-ramps [7]. Persons must pass those bottlenecks and are, thus, forced into reader range. This tracking is only limited by the number of reader devices installed and by the possible bottlenecks. Internal documents show that developers of RFID technology have a world in mind where RFID reader devices make up an all-embracing global network [8].

Another reason why RFID tags are increasingly favoured by companies is that the chips are becoming tinier and cheaper. The smallest chips cover only 0.2mm^2 and antennas can already be printed directly on the product or the package with an ink jet technology [7]. Prices are predicted to fall below 1¢ each by 2004 [5]. The argument that RFID tags are too expensive for massive introduction is invalid because mass production has just begun: RFID tags are designed to be cheap.

Regarding privacy issues, another technology comes into play: databases and their supersets – archives. In principle, databases are independent of RFID technology. But, as I will show, the main threat to privacy lies in the combination of both technologies.

Of course there are other aspects and risks, e.g. the increased amount of customer-vicinity radio transmissions might lead to health problems, or the increased adoption of RFIDs taking over tasks now performed by humans may lead to more unemployment. These problems go beyond the scope of this paper. I will confine myself to privacy and civil-liberties issues.

RFID imposes threats to privacy and civil liberties

Civil and consumer rights protection groups have identified five major points concerning privacy and civil liberties issues [8]. These are:

1. Hidden placement of tags
2. Unique identifiers for all objects worldwide
3. Massive data aggregation
4. Hidden readers
5. Individual tracking and profiling

Let's look at these points in detail.

1. Hidden placement of tags.
   RFID tags can be embedded into or onto objects without the knowledge of the individual obtaining or holding these items. This has already been done by Gillette with tags hidden inside the package of Mach3 razor blades, and by Benneton who sewed tags into clothing. As radio waves are able to travel through fabric, plastic, and other materials, it is possible to read those RFID tags without the need for line of sight. Currently liquid and metal still pose problems for tag reading because radio waves are absorbed by liquid or deflected by the metal, so that tags cannot be placed everywhere [7].

   But enough places remain. There is currently no law to notify customers of RFID tags, with two exceptions from 2004: "On Feb. 24, the Utah House of Representatives passed a bill mandating clear labeling of any product in which an RFID chip is embedded. A bill introduced on Feb. 27 in the California Senate goes further, arguing that retailers should need consumers' permission" [9].

2. Unique identifiers for all objects worldwide.
   The Electronic Product Code (EPC) is designed to enable every object on earth to have its own unique identifier (ID). EPCglobal assigns EPC number blocks for all products to all producers in the world and estimates the

number space will not be exhausted for about 1000 years. These numbers are ideally suited for direct and easy use as keys within a database.

The use of these keys could lead to every physical object being identified and linked to its purchaser or owner within a global registration system. For this, there is no need to store more than the ID information on the chip: If all systems are interconnected, an external database will do the trick. Leaked documents [10] show different number blocks to be reserved for different products – one is already reserved for “human”.

3. Massive data aggregation.
RFID deployment requires the creation of huge databases containing the tag IDs. Corporations have learned through grocery “loyalty” cards that collecting data may add new value to the company. Thus, large data collections have been created and tested by individual corporations. The data records could be linked with person data, especially as computer memory and processing capacities expand. Work is now being undertaken to interlink individual data collections to form new, huge, centralised databases, for example by SAP and DARPA [11, 12].

   Once data is in a database, it can be combined or linked with other data to form new data. Those databases are not publicly visible because the collected data is very valuable and companies reserve read and search access for themselves. As a consequence, there is the risk that false or wrongly linked data could persist in those databases. Until now cost-intensive data mining had to be performed to extract useful data from the masses of data. With unique IDs, this data mining can be broken down to a sequence of very much easier operations. This will reduce processing cost and time and can obviously lead to an expansion of data aggregations.

4. Hidden readers.
“Tags can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate. RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being ’scanned”’ [8].

   Accenture and Gillette are talking of and introducing “silent commerce” [13, 14]: The customer does not and will not know that his RFID tags are being read. Cheapest reader devices cost about 20 US-$ today. The smallest ones are as tiny as a 25 US-¢ coin. Portable reading devices are obviously possible to build. But there is the danger of surveillance if reader devices are installed in strategic places: bottleneck locations such as doors or on-ramps to freeways, carpets or the shelving of a store. Here, there is no need for long-range readability because everyone has to walk or drive by, through or over the reader device.

5. Individual tracking and profiling.
   If personal identity were determinable, e.g. linked to unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example, a tag embedded in a shoe can effectively be used as an identifier for the person wearing that particular shoe. The EPC of items people wear or carry around could associate them with events such as political rallies.

   The next step would be to minimise the gap between item and individual by means such as embedding RFID tags into customer or loyalty cards. This is exactly what Metro did in its "extra Future Store" [15] located in Rheinberg, Germany. RFID tags are also used in contactless smart cards which then can be identified before the smart functions are enabled, because the RFID range is larger than that of the smart card functions. There are plans for using RFID tags in (federal) identity cards [16] and passports [17] as well, so that biometric data need not be stored on the identity card itself, but in a central database.

   By minimising the gap, customers may be identified as they enter a store. Habits and preferences could then be recorded and later be used to optimise store layout and seduce or manipulate the customer to buy more or more expensive products in the future. Customer relationship management (CRM) can also benefit from the data collected and from the availability of customers' identities as soon as they enter the store: classification of customers into "good" and "bad" categories [18] may lead to gratification or penalisation of the customer through different prices or different service offers. The customer would not know about this. Such classification is already performed today, but the means to identify a customer before the point of sale were missing until now.

   More far-reaching issues may arise, as the 2003 Big Brother Awards Germany laudation envisages: "Marion Z. is sent a caution from the Duisburg authorities with a fine. The wrapping paper of a Mars bar she has bought was found in the town park, floating in the duck pond. After some pondering, Marion Z. remembers that she gave the sweet to a young carol singer. Grinding her teeth, she pays the 10 Euro fine" [19].

   At Enterprise Charter School, Buffalo, USA, pupils can already be identified via RFID tags. They are forced to carry around an identification card equipped with such a tag [20]. With these tags, data about course attendance and the pupils' presence and location is to be collected, according to the school's principal. This shows that data greediness is not limited to retailers. Similar to this school, companies might be eager to learn about their workers' presence and location. RFID tags sewn into working clothes would perform this job well.

The next step, implanting the chips directly underneath human skin, is currently pushed by Applied Digital Solutions, who intend to sell their VeriChip, VeriMed, VeriPrime, VeriPay and VeriKid systems, all based on RFID tags. E.g. in Mexico, the VeriKid tags are being implanted "in children as an anti-kidnapping device" [21] albeit the fact that it is unlikely today to fortuitously have a reader device near the hostage's position. Those tags might be used to clearly identify dead bodies, but they cannot prevent kidnapping. With the implantation of RFID tags, Applied Digital Solutions closes the identification gap [22]. Here in Germany, society is very sensitive to the thought of implanted ID numbers in view of the recent, worst part of our history. These concepts are therefore likely to be regarded as wholly unacceptable by a significant part of German society.

Introducing RFID technology adequately

A technology that can be used for such controversial and conflicting interests must be introduced on a basis that balances the concerns of all stakeholders. It must be said that some damage of trust has already occurred as some retail companies deliberately chose to introduce RFID technology without informing their customers. Metro, one of the biggest retailers in Europe, responding to a civil protest organised by the German privacy and data protection group FoeBuD that was supported by more than fourteen German consumer and civil liberties groups, has announced that it will discontinue its trials with embedding RFID tags into customer "payback" cards [23].
Addressing such concerns, RSA Security has announced the availability of a RFID blocker tag [24]. RSA wants to hand them out sewn into shopping-bags at the CeBIT 2004 trade show in Hannover [25]. But as c't, a renowned German computer magazine, figured out, those blocker tags are and will be only partially usable[1]

[1] Blocker tags "jam" readers by sending out unrequested responses to reader signals, "drowning" out data from the RFID chips actually addressed. This works best if one of two main protocols, the Tree Walking Protocol, is being used. The other protocol, the Aloha Protocol (a classic protocol which stimulated the development of Ethernet), is and will be principally immune to passive blocker tags: because this protocol features delayed responses, blocker tags will not be able to gather enough energy to block all consecutive answers following a reading impulse.

[26].
Furthermore, RSA Security announced that its blocker tags will not "drown out" all possible RFID numbers in order not to interfere with planned industry applications. Having to rely on blocker tags is also a disadvantage for customers, because they would *actively* have to protect their privacy. But even if people were to accept the "protection" offered by blocker tags, after technology has been developed and stores have been equipped with RFID installations, blocker tags could just be banned by law or by store owners not allowing entrance to people found to carry blocker tags. Blocker tags can not be the ultimate solution to the perceived evils of RFIDs.
The most radical strategy of a total RFID ban is not feasible either. Once this technology exists it is not possible to uninvent it, especially as there are good reasons for using this technology safely and profitably. Therefore, a line must be drawn between the legitimate interest of tracking products in the supply chain and the damage to individual rights if tracking continues in store rooms and after products are purchased. The public-interest organisation CASPIAN[2], amongst others, proposes a three-part framework: "First, RFID must undergo a formal technology assessment, and RFID tags should not be affixed to individual consumer products until such assessment takes place. Second, RFID implementation must be guided by Principles of Fair Information Practice. Third, certain uses of RFID should be flatly prohibited" [8].
Such a balanced approach respects most valid interests. As efforts to introduce RFID technology secretly have already been made, a moratorium must be set up to cease these tests until a technology assessment has taken place involving civil, industry and commerce stakeholders with the purpose of agreeing on acceptable guidelines for laws and regulations.
At the time of writing, there is not much information available from industry and commerce about what they would regard as acceptable. But it may be assumed that the interest is largely in allowing RFID tags, readers and referencing database technology as far as possible.
On the "civil liberties" side of the debate, demands have already been made: No technology should be introduced secretly. It has to be clearly visible where RFID tags and reading devices are installed or used and for what purpose. Data that is not essential for the given purpose must not be collected. Security and integrity in transmission, databases and system access must be ensured. Installers and users of such technology should be legally responsible for complying with the agreed principles. Auditing by outside third-parties with publicly available results must be actively supported.
The following would not be acceptable [8]:

[2]CASPIAN: Consumers Against Supermarket Privacy Invasion and Numbering

- coercing or forcing customers into accepting RFID tags that are "alive" or only currently inactivated,
- prohibiting detection of RFID tags and readers and prohibiting disabling of tags by customers,
- human tracking, either directly or indirectly through goods and items and
- use of RFID tags to eliminate or reduce anonymity (e.g. embedded into currency).

Acceptable uses of RFID are the tracking of goods in the supply chain up to the point where those goods are brought into contact with customers. That is the point at which those goods are put onto a shelf in the sales area, and not the point of sale, because the sales area is a shared space. Acceptable would also be a use as an additional warning mechanism for products containing toxic substances. The RFID tag could transmit a message relating to recycling or disposal of the product. The information stored would be generic to the product, not specific to the individual item.

These demands could be stated in a more abstract form and then become part of a legal right: the "right for informational self-determination" [27]. In Germany this right has been derived from the Basic Constitutional Law and was first introduced into German legislation by the Federal Constitutional Court[3] in 1983 in a ruling about a population census [28]. The right for informational self-determination includes the individual's control over relinquishment and utilisation of personal data, including withdrawal: the right to know which data is being collected, where it is being collected, stored, connected to other data and processed, and who has access to the data. It also includes the right to designate what may be done with one's data and the right to instruct institutions storing someone's data to delete it or to correct data that is wrong. This right of informational self-determination that is currently threatened by RFID technology introduction must be maintained and strictly adhered to for the foreseeable future. The main objective of the RFID debate must be to ensure exactly this.

References and recommendations

[1] Colin C. Haley: "Are You Ready for RFID?", 2003-11-24, `http://networking.earthweb.com/netsp/article.php/3112801`

[3] The Constitutional Court is Germany's highest judicative body. One of its main functions is to rule on the compatibility of legislation or administrative acts with the constitutional law.

[2] Detlef Borchers, Neue Züricher Zeitung: "Frischkäse bitte bei Kasse 3 melden", 2004-03-05,
http://www.nzz.ch/2004/03/05/em/page-article9G4V4.html

[3] Bob Brewin, Computerworld: "Agriculture head backs national livestock ID system", 2003-12-31,
http://www.computerworld.com/mobiletopics/mobile/technology/story/0,10801,88710,00.html?nas=PM-88710

[4] CASPIAN: List of sponsors of the MIT Auto-ID Center as of 2003-06-25,
http://www.spychips.com/rfid_sponsors.htm

[5] Katherine Albrecht, CASPIAN: "RFID: Tracking everything, everywhere",
http://www.nocards.org/AutoID/overview.shtml

[6] Cybertime: "VeriSign and EPC Global ... tracking consumers through products", 2004-01-13,
http://www.cybertime.net/~ajgood/ecommerce.html

[7] FoeBuD e.V., Public Domain 128: "Spy Chips in the Yoghurt Mug – RFIDs - coming soon!",
http://www.foebud.org/pd/pd128/index-gb.html
with Katherine Albrecht, CASPIAN, lecturing about "Privacy and Societal Implications of RFID" at Bunker Ulmenwall, Bielefeld, Germany, 2004-02-01, presented slides:
http://www.rfidprivacy.org/papers/albrecht.pdf

[8] CASPIAN, ACLU, EFF, EPIC et al: "Position Statement on the Use of RFID on Consumer Products", 2003-11-14,
http://www.spychips.com/jointrfid_position_paper.htm

[9] Jane Black, Business Week: "Shutting Shopping Bags to Prying Eyes", 2004-03-05,
http://www.businessweek.com/technology/content/mar2004/tc2004035_8506_tc073.htm

[10] Cryptome and Quintessenz Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter: 68 confidential documents from Auto-ID found by CASPIAN, 2003-07-06,
http://cryptome.org/rfid-docs.htm and
http://quintessenz.org/rfid-docs/cryptome.org/rfid-docs.htm

[11] Jürgen Kuri, Heise Newsticker: “SAP verstärkt mit RFID-Unterstützung Engagement im Einzelhandel”, 2004-01-13,
http://www.heise.de/newsticker/meldung/43560

[12] Bill Fetech, Systems and Processes Engineering Corp.: “RFID Technology Tests Successful”, July 1999,
http://www.spec.com/PipelineJuly99.pdf

[13] Accenture Technology Labs: “Silent Commerce”,
http://www.accenture.com/xd/xd.asp?it=enweb&xd=services%5Ctechnology%5Cvision%5Csilent_commerce.xml

[14] Michael Fitzgerald, Small Times: “Alien lands big Gillette deal, but privacy is not on razor’s edge”, 2003-01-24,
http://www.smalltimes.com/document_display.cfm?document_id=5363

[15] Metro AG, Future Store Initiative Website: “STORE OF THE FUTURE”
http://www.future-store.org/servlet/PB/menu/1000373_l2/1079032461800.html

[16] JurText online: “Sklaven der RFID (Radio Frequency Identification)”,
http://www.jurtext.de/modules.php?name=News&file=article&sid=889

[17] Andreas Wilkens, Heise Newsticker: “Reisepass mit RFID-Chip”, 2004-03-19,
http://www.heise.de/newsticker/meldung/45780

[18] Dionco Inc. presentation: “The Future of Commerce”, 2003,
http://www.dionco.com/downloads/NRF2003final.ppt

[19] Rena Tangens, FoeBuD e.V., and Frank Rosengart, Chaos Computer Club (English translation: Sebastian Lisken): Big Brother Awards Germany 2003 laudatio for the Metro Group: “Consumer Protection”, 2003-10-24,
http://www.bigbrotherawards.de/en/2003/.cop/

[20] Florian Rötzer, Telepolis: “Sicher und überwacht”, 2003-10-24,
http://www.heise.de/tp/deutsch/inhalt/te/15936/1.html

[21] Julia Scheeres, Wired: “Tracking Junior With a Microchip”, 2003-10-10,
http://www.wired.com/news/technology/0,1282,60771,00.html

[22] Charles J. Murray, EETimes: “Injectable chip opens door to ’human bar code”’, 2002-01-07,
http://www.eetimes.com/story/OEG20020104S0044

[23] Metro AG, Future Store Initiative Website: “Position paper Subject: The use of RFID in the Future Store in Rheinberg”, 2004-02-28,
http://www.future-store.org/servlet/PB/menu/1002376_l2/index.html

[24] RSA Security: “RSA Security Demonstrates New RFID Privacy Technology: The RSA® Blocker Tag”, 2004-02-24,
http://www.rsasecurity.com/company/news/releases/pr.asp?doc_id=3376

[25] Dr. Hans-Peter Schüler, Heise Newsticker, “RFID-Störsender für Hacker und Verbraucher”, 2004-02-25,
http://www.heise.de/newsticker/meldung/45009

[26] Peter Schüler, c’t magazin für computer technik issue 6/2004, page 40: “Schnüffeltechnik ausgetrickst – Ein Störsender verwirrt RFID-Lesegeräte”, ISSN 0724-8679

[27] Jürgen Kuri, Angela Meyer, Peter Schüler, c’t magazin für computer technik issue 6/2004, pages 138ff: “Im Fadenkreuz - Verbindungsdatenspeicherung, Biometrie, DRM, RFID: Die Aushöhlung des Datenschutzes”, ISSN 0724-8679

[28] Dr. Benda, Dr. Simon, Dr.Hesse, Dr. Katzenstein, Dr. Niemeyer, Dr. Heußner, Niedermaier, Dr. Henschel: “BVerfGE 65, 1 - Volkszählung: Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden”,
http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm