

Arbeitskreis Kritischer BibliothekarInnen
(Working Group of Critical Librarians)

RFID

-

Modern Technology with Risks

by

Frauke Mahrt-Thomsen

Translation by Anne Koehler

Lecture at the conference of the Virtuelle Fachbibliothek Recht (Virtual Law Library) / AjBD (Arbeitsgemeinschaft für juristisches Bibliotheks- und Dokumentationswesen = Association of juridical Library and Documentation Work) at the Staatsbibliothek zu Berlin (Berlin State Library)
on 26.2.2010

http://www.vifa-recht.de/fachtagung2010/download/Vortrag_Mahrt-Thomsen_Web.pdf

RFID – modern technology with risks

Frauke Mahrt-Thomsen

First of all I would like to say that I appreciate being invited to be a speaker at this conference. I have been working in public libraries in this city for forty years. Furthermore I have been active in Akribie, the Arbeitskreis Kritischer BibliothekarInnen (Working Group of Critical Librarians). For twenty years Akribie has concerned itself with the relationship of libraries and society. Our main questions are: what kind of libraries do we want? What is the societal responsibility of the librarian? Which library ethic should we follow in everyday work?

As early as 2006 during BibliothekarInnentag (Librarian's Day, traditionally: Bibliothekartag, we always spell it with Innen to show that it is also a day for female librarians) Akribie carried out an event titled "The observed person: RFID in libraries. A discussion about technology, civil rights and the responsibility of librarians". It took place outside the official conference program, with lively participation of citizens who expressed their concern about the minimally controllable implementation of this complex new technology. The next day at the planned event in the conference center concerning RFID our critical inquiries were less welcomed. People were more interested in getting a positive demonstration of the beautiful new radio world at the public library in Munich.

Ulrike Verch who is today professor at the Hochschule fuer Angewandte Wissenschaften Hamburg (University of Applied Sciences Hamburg) gave a lecture in 2007 at the Leipzig Library Congress "Self adhesive, self checkout and also self responsible? Legal frame conditions for the implementation of RFID-Chips in libraries".

<http://www.opus-bayern.de/bib-info/volltexte/2007/305/pdf/verch-leipzig-2007pdf>

Her contribution informed initially about how intensively and critically American colleagues and citizen groups debate about RFID technology.

The view into the United States is also therefore exciting for us, because there are examples of conscious decisions against RFID for social-political reasons. In 2004 citizens demonstrated in San Francisco against implementation of RFID in their libraries and up to this date the San Francisco Public Library has not introduced this technology in spite of existing seed money.

The Electronic Frontier Foundation (EFF) in the USA declares on their website "EFF is strongly opposed to RFID in libraries.....Libraries, schools, the government and the private sector businesses are adopting radio frequency identification tags, or RFIDs – a technology that can be used to pinpoint the physical location of whatever item the

tags are embedded in. While RFIDs are a convenient way to track items, they are also a convenient way to do something far less benign: track people and their activities through their belongings. EFF is working to prevent the embrace of this technology from eroding privacy and freedom.”

See EFF website under:<http://w2.eff.org/Privacy/Surveillance/RFID/libraries/> and:
<http://w2.eff.org/Privacy/Surveillance/RFID>

The protection of privacy and the confidentiality of the reader has always been of high ranking importance to the ALA. As early as 2005 they issued a resolution along with data protection guidelines, supported by many study groups and committees, *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles*:

<http://www.ala.org/Template.cfm?Section=ifresolutions&Templates=/ContentManagement/ContentDisplay.cfm&ContentID=85331>

and in 2006 guidelines for the implementation of RFID: *RFID in Libraries. Privacy and Confidentiality Guidelines*,

<http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/Contentmanagement/ContentDisplay.cfm&ContentID=85331>

in which confidentiality and data protection as guiding principle of library work are anchored. (*Basic Privacy and Confidentiality Principles*). One of the recommendations in these guidelines state, that the colleagues should offer an alternative way for checkout, if requested by the user – an almost revolutionary idea for librarians in the Federal Republic of Germany; an idea which deserves more recognition.

It actually agrees with the core of a decision by the Bundesverfassungsgericht (Federal Constitutional Court of Germany) in 2006, that a voluntary agreement of a citizen – in pursuance of general needs - to a certain procedure only exists, if an alternative is offered, except there are legal regulations. Because Germany has almost no library laws and in the future most assuredly no library law will govern the type of lending organization, libraries move “on thin ice” with the fixing of an exclusive type of circulation, as a collaborator of the public German data protector told me. (Decision of the Bundesverfassungsgericht of October 23, 2006. File number 1BVerfG 2027/02; Amtliche Entscheidungssammlung (Collection of Decisions) of BVerfG, Vol.113, p.273-348, also: §4 and 4a of Bundesdatenschutzgesetz (Federal Data Protection Law)).

Looking back on 20 years of Akribie work on a meeting at the BibliothekarInnenntag in Erfurt in 2006 I gave a small presentation on the topic of “RFID in Libraries”. In view of the continuing risks of the RFID technology and the social and societal consequences, we came to the conclusion: “Akribie thinks, librarian’s ethic demands to do without RFID in public libraries.”

The definition of “responsibility”, as the Gesellschaft für Informatik (Society for Informatics, abbreviated: GI, not to be confused with the Deutsche Gesellschaft für Informationswissenschaft und Informationspraxis = German Society for Information Science and Information Practice, abbreviated: DGI) has found it, shall serve as my motto: “Because human beings cannot always foresee the consequences of their actions, decisions should always be made such, that they can be recalled and remain correctable. Thus the latitude of action of all involved is widened and not from the start limited without alternatives. Communal action requires additionally to individual also communal reflections. Communal responsibility rests on the possibility to carefully contemplate together future actions, which cannot or only partially be developed from experience and their resulting norms.”

(from: Gewissensbisse, p. 122)

It is estimated that more than 2500 libraries worldwide are already using RFID and there are more than 500 million chips in use in libraries. The city libraries in Munich, Vienna, Hamburg, Stuttgart, Halle and Munster have long since been working with RFID, also the university libraries in Karlsruhe, Berlin (Technical University and Humboldt University), many Bavarian college school libraries and the library of the Vatican.

The public libraries of Berlin are introducing the RFID technology area-covering by the end of 2012. The local and regional public data protectors did not feel justified to withhold their support to the introduction of RFID, because there are no real data, only a series of numbers on the library cards, which can only be decoded in the internal computers of the libraries.

As the project manager of the city library of Munich reports meanwhile over 97% of users check out material themselves at their circulation terminals and are happy that they can return books round the clock at the RFID return automat.

There will not be a general agreement or rejection by the public data protector in Berlin concerning the RFID introduction in the local public libraries, instead he goes along with the planned RFID introduction by the VOEBB (Union of Public Libraries in Berlin) in its various phases of development. At present the person in charge is checking the safety concept of the VOEBB, according to § 5 Abs. 3 Satz 1 BlnDSG (Berlin Data Protection Law). Perhaps Dr. Dix (the present Berlin public data protector) can add a few remarks about the state of the proceedings?

A report can be read in our trade journal about the opening of a city public library, which states that the introduction of the RFID self checkout is a must for all patrons (BuB, number 3/2009, p. 194) and at the initial event for the introduction of RFID in Berlin last summer the business manager of the standing conference of directors of the Berlin public libraries proclaimed: “Personally, I find RFID relatively unspectacular, as a matter of fact, as unspectacular as breathing. One can talk a lot about breathing, but one cannot do without it. At least one does not fare well, if one

does without it. You can test it by trying it yourselves.” (from: Technologische Innovation...p.14)

Why then does Akribie have these reservations?

We think that it is not sufficient to rely on the pronouncements of interested propagandists, but instead one needs to take a closer look at how RFID functions technically and socially. There are proven risks even within the sphere of closed systems in libraries with passive, non transmitting chips. The social effects and political connections have to be considered beyond the narrow data protection.

At the outset I would like to quote the activist of the citizens group FoeBuD.e.V., Rena Tangens:

“‘Brave New World’, Aldous Huxleys vision of a state, in which people can consume comfortably, but are living perfectly manipulated in mental slavery, is much more modern than ‘1984’ George Orwell’s description of a totalitarian surveillance state. But let us not assume, that the surveillance state has thereby outlived itself. Civil liberties have been limited extensively in Germany during the last few years. Some keywords: saving of all communication connections, the great listening attack (Großer Lauschangriff), intensification of police laws of the states with computer search (Rasterfahndung), video surveillance in public places (Videoüberwachung), license plate recording on highways, biometric characteristics in passports which are stored on RFID chips, expansion of DNS storage, etc. Hardly a surveillance method, which is not justified with the supposedly threatening ‘international terrorism’.

To be sure, almost all these measures are not aimed at criminals or immediate suspects, but instead concern millions of completely uninvolved citizens. The presumption of innocence is actually being ignored. Most people realize, that their private sphere is being attacked, when they become the object of surveillance (for example video surveillance or phone tapping) or when their personal secrets are being dragged into public view. The fact that their privacy also can be assaulted by collection, analysis and use of a variety of data, which accumulate through daily actions - this realization is coming about only gradually.”
(<http://foebud.org/datenschutz-buergerrechte/linsengericht>)

The FOEBuD member *padeluun* (pen name) told me in a telephone conversation: the placing of such data “is always evil, is wrong, each central data collection can be abused.”

What is new with RFID technology, as compared with the barcode, which also works with a sequence of numbers? RFID stands for radio frequency identification. Data are being transmitted via radio waves, without touch and visual contact. An RFID system encompasses a transponder, a minute computer chip with an antenna, which can be integrated in a stick-on label or plastic card, as well as a send/receive equipment and an IT system which operates in the background. Each chip contains a unique serial

number, each objects which carries this chip, for example a fruit crate or a cup of yoghurt, is thereby identifiable worldwide and potentially also the buyer, when he purchases the cup with a debit or credit card. The radio transmission happens soundless and almost invisible, because the reading equipment in many instances are difficult to recognize. Even a hidden installation into a door frame, floor or shoes is no problem.

FoeBuD e.V. writes, “the chips are so tiny and cheap, that they can be implanted into each jacket collar, and into each shoe sole. Once there they cannot be removed without destroying the product (for example the shoe). This means: each reader antenna, which you happen to pass, catches your chip once again (perhaps on the bus, at the gas station, in the nearby supermarket). The ‘deactivators’ familiar to us, have not prevented that. Our consumption habits are being found out without our knowledge. For example: who stands how long in front of which shelf? Which ads can be sent to this customer specifically?”

[\(http://www.foebod.org/rfid/das-problem/\)](http://www.foebod.org/rfid/das-problem/)

Meanwhile reading equipment has become so inexpensive (20 Euros) that each technology fan can buy and experiment with them. For example if he stands with his reading equipment next to a library user who carries the books which he just checked out in his bag, he can read the chip numbers and can discern with the aid of application family identifiers (AFI) that the person has library media.

With the help of ISIL (International Standard Identifier for libraries and Related Organizations) –numbers which have been integrated into the serial numbers of the RFID chip following the Danish data mode - he can ascertain exactly, from which individual library or library system the items came. Should one of these libraries be in the vicinity, he can eventually even find out with aid of the multiply repeated numbers to which subject area the borrowed books belong – if the library has carelessly issued the numbers in sequence, instead of scattering them according to the chance principle (hint by collaborators of the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent State Center for Data Protection of Schleswig-Holstein, the most northern state of Germany).

Completely realistic and several times mentioned is the misuse scenario which Ulrike Verch describes: “If, for example, I am in a department store which has implemented customer cards and want to pay at the cash register and happen to hold my bag, including my purse in front of the reading equipment, it can discern with the aid of the unique application family identifier that I am also carrying library books. The department store thereby has the opportunity to enter into my customer card file the remark: ‘library user’. As soon as items containing RFID chips are linked with personal databases, the possibility of establishing personal profiles increases, enabled by radio frequency technology and the many data tracks, which we leave behind.”

The fact that reading equipment in department and other stores react to RFID chips from libraries, was recently confirmed to me by an user of the Technical University Library in Berlin.

A much wider security gap with certain RFID applications, which could have serious effects on libraries, has already been discovered 2-3 years ago by members of the Chaos Computer Club and researchers of American and Dutch universities. It concerns the most used chip system Mifare (producer NXP and Infineon Technologies) of which a thousand million cards and more than five million reading equipments have already been sold worldwide. The Mifare system is mostly used in libraries, like in Munich and in future times also in the Berlin public libraries, version Mifare Mini.

It was demonstrated at the Hacker Congress in December 2007 as well as in an article in number 8/2008 of the journal c/t how the algorithm of Mifare was broken, which means analyzed, and a system fault was found, which makes the coding practically useless. "The security of the Algorithm", the conclusion of the researchers, is "close to zero...The weaknesses of Mifare are contained not only in the capturing of the keys of reading equipment. The cards could likewise simply be 'cloned' or copied. If no other security mechanisms are applied, people can with a duplicate of an RFID card gain access to buildings or other secure areas."

The researcher Bart Jacobs from the Radboud University in Nijmegen, Netherlands, shows in a YouTube Video at the website ([http://golem.de/087/\(60973.html\)](http://golem.de/087/(60973.html))) in front of a running camera how he duplicates a Mifare card and uses with this the London subway for free. According to statements of researcher Karsten Nohl who participated in the decoding, this attack functions also with the improved successor Mifare Plus, as long as the reading equipment was not changed to the 'Plus' standard. Mifare Plus uses another way of coding, but older reading equipment defaults to the unsafe algorithm of the earlier version.

With Mifare Mini we are dealing with a slim version of Mifare for application with reduced storage need. When I asked the technical expert of the Independent State Center for Data Protection Schleswig-Holstein, whether this version of Mifare is still safe, I got the answer "The cryptography of these chips is also broken, according to our information." The process length for an attack "on a standard PC without special hardware and without prefigured tables lies around 200 seconds." He could teach this any student in about 20 minutes.

If it is not a problem for any student to decode the Mifare card, he can, according to the example by Bart Jacobs, capture unnoticed another library card number just by walking by and check out books with the duplicate card. The real reader will be held responsible for this and he might decide never to use his library again when he experiences this gap of security. The misuse/abuse will be much easier in the future, since the reader does not have to confront a library employee, who would recognize

immediately the false library card or use of name, because he might know the real owner of the card.

Just a few days ago I heard from a colleague who is responsible for RFID planning in the Berlin public libraries the justification for the wish for Mifare cards: "they are much more falsification proof than barcode cards, because one can copy the barcodes any time and can unwatched check out things at the self checkout automat." I believe he vastly underestimates the potential of the many computer freaks in this city.

The transponders used in libraries are until now passive as a rule and can only be moved to send their number code because of the magnetic field of the reading instruments. The IT system deciphers the code and links it with information, which is deposited in the database. The knowledge or the intelligence of the system does not lie in the transponder, but rather in the database. But long since there are 'intelligent' transponders or 'smart' chips, which have their own battery, store a great deal of information and send signals across a considerable distance, are able to receive and process. Passive, but increasingly also 'smart' chips are already being utilized in vast parts of the work and everyday world.

Here are a few examples:

- logistics (goods, transport containers, packages worldwide, f.i. DHL)
- transport system (electronic toll systems)
- package directing at airports
- production and finishing planning: Computer Integrated Manufacturing (CIM) mainly in the automobile industry (BMW, Volkswagen)
- local transportation systems (London, Netherlands, Rhein-Ruhr area)
- key systems, drive-off barriers
- electricity use metering
- dangerous goods storage
- health systems, pharmaceutical industry, sick and aged care: Ambient Assisted Living (AAL)
- trade and business (WalMart, Metro-Group: FutureStore), warehouse administration, debit and credit cards
- Maintenance and repair management (Airbus A380)
- forestry (Cambium Forestry, Odenwald), tree care
- leisure (ticket systems, traffic tickets, ski passes)
- sports (Marathon runners: chip in the shoe)
- employee IDs
- work clothes
- administration (U.S. social security files)
- system of registration (BRD passports, German personal IDs from fall 2010)
- animals (dogs, cats, cows: clips in the ear, capsules in the stomach)

- people (identification of criminals or members of beach clubs and security firms by implants under the skin, preventive tooth implants for identification in case of catastrophe).

The RFID chips act in part as spy chips, because often and unintentionally they tell something about us, our buying habits, our location and communication, our preferences and dislikes, possibly even the color and size of our underwear – the attempt of a worldwide clothes manufacturer, to put RFID chips in lady's underwear, was only prevented due to the FoeBuD campaign: "I'd rather go naked".

Everyday objects become 'intelligent' via the 'smart chips', the universal availability of information for us on the internet shifts to movable objects and things in the real world. The RFID technology is the deciding prerequisite for the 'Internet of Things' (abbreviated IoT), in which things exchange themselves and possibly find their way independently, because they and their surrounding net structures 'know', where they have to go. Goods and objects of all sorts are being interlinked worldwide, identifiable and capable of action.

The effects upon vast areas of commerce, administration, science and especially upon the world of labor are enormous. More often in the production process the worker does not decide, what the machine has to do, but the worker gets instructions via the 'intelligent' equipment from the system, which is steered by RFID. Human beings become receivers of commands, to perform process optimized movements which up to now are too complicated for automatization, say Alfons Botthof and Marc Bovenschulte in their study "Das 'Internet der Dinge'. Die Informatisierung der Arbeitswelt und des Alltags." (The 'Internet of Things'. The Informatization of the Work World and the Weekday).

The study comes to the conclusion that RFID is a rationalization technology, which is being mostly introduced by employers insidiously, without timely information and inclusion of the workers, and that this causes a massive change and the elimination of many jobs.

The logic behind the introduction of RFID is not only the rationalization and elimination of work places, but the control of logistic and work processes. People in the work process can be temporally and spatially located, networked and controlled with the aid of RFID, down to exact timing for certain work steps and breaks. These data collections are an excellent foundation for personnel decisions at the next wave of rationalization. Data protection like anonymization are often not planned in these proceedings.

On the other hand an enormous growth of RFID technology applications is being predicted and therewith the increase of work places in this area. The responsible division head at the Berlin Senate for Economy reports: "The analyzer...for example prognosticate a development of the world market for RFID application from

approximately 5 billion (in Germany: Milliarden) Euro in 2007 to more than 16 billion (Milliarden) Euro in the year 2016. In this same time the RFID market in Germany will also grow, whereby annual growth rates of an average of 19% are expected.” She adds that these numbers were “of course” gathered before the economic crisis, and it would be doubtful, whether they can be reached, but “the tendency is surely correct”. (from: Technologische Innovation...p.9)

The RFID lobby publishes numbers about the “RFID-influenced value creation in Germany”, they say it amounted to 3,4 billion.(Milliarden) Euro in 2004 and will increase to 62,14 billion (Milliarden) Euro until 2010. (from: Basiswissen RFID, p.11). What do these numbers mean? Does it mean the value of all products, which have been manufactured with RFID transponders and distributed? Was the value of saved work places included, and if so, at which level?

This technology is also being supported in a sustained effort on the European plain. The EU-Commission published on June 19, 2009 their statement “Internet of Things – An Action Plan for Europe”, in which they developed a whole scenario of measures, to insure the spread of the new technology.

Applications at the level of millions to promotional funds of the EU, which are usually difficult to access (for example to EFRE, the European Fond for Regional Development) stand a good chance of being approved within a few months, if it deals with the implementation of RFID. This can be shown by several examples in Berlin. So in 2009 besides the introduction of RFID in public libraries, carrying the name TENIVER (Technological Innovation in the Information Supply); there was also approved EFRE-money for RFID application in the university library of the Humboldt University and for the project “POSEIDON” (information systems for museums to demonstrate the potential of RFID technology).

I noticed that in the project name TENIVER the mentioning of the citizens was omitted, while at the starting event in May 2009 the value of RFID for the citizens was so much emphasized. The motto then was “Technological Innovation for Strengthening the Citizens Community.”

The German RFID lobby is well established. In 2005 the *Informationsforum RFID e.V.* (Information Forum RFID) was founded, with the aim to “move the future and innovative potential of RFID stronger into the consciousness of the public and to further the implementation of this forward looking technology through dialog” (from: Basiswissen Internet der Dinge, p. 19). The *Informationsforum* has found its seat in the very representative house Dorotheenstrasse 37, on the highest level, in direct sightline contact with the government quarter. Among the members of the *Informationsforum* are the crème of the producers, implementers and service managers of RFID: IBM, Siemens, Hewlett-Packard, Intermec (system developer), Bitkomm (trade association of information, telecommunication and media), Volkswagen, Metro Group, Henkel, Proctor & Gamble, DHL, ORACLE, BVL (federal

union of logistics), IT-Systems (RFID solutions for big users), GS1 Germany (rationalization and standardization organization) and the Fraunhofer-Society (a research society, application oriented and close to industry).

One problem is nevertheless being categorized from the *Informationsforum* as “not yet finally clarified”, namely the question of waste disposal. The chips are special waste, because they contain several metals, and this is not a simple matter in view of the desired exponential increase of application of RFID chips in consumer goods of all kind. It is hoped that progress in material research of polymer technology will bring relief, because polymers contain neither metal nor silicium.

A possible further threat with constant and area covering use of RFID is radiation damage. At constant exposure to RFID radiation similar risks are valid as with use of WLAN. Supposedly they turned off WLAN in Paris libraries because of health problems of several librarians. At least the *Informationsforum* admits “radiation is the great unknown”.

However, these are questions which do not move the representative of the Berlin economic senate, who at the starting event for the introduction of RFID describes in euphoric terms the spreading of the market for wireless application, especially in the area of RFID and NFC (Near Field Communication) technologies in recent years in Europe, Germany and the region Berlin-Brandenburg. She continues: “We know, that RFID develops faster, when successful pilot projects show the advantages for all involved, and show solutions for questions like data protection, data security, acceptance. That is why the library project is very important as well from a technological political view.” (from: *Technologische Innovation*....p. 9/10)

A starting point of the Berlin senate’s strategy is therefore not the interest in furthering the public library system in those areas which most urgently need support, like the acquisition budget. The subsidy of the regional acquisition budget of 1,7 Mill Euro annually has just recently been brusquely rejected by the mayor and cultural senator with these words: “I do not have that kind of money, it does not interest me.” Now he is not hesitating at all to invest 10 million Euros in the RFID technology, even though half of it comes from the funds of the EU, the senate still has to pay 2,5 million Euros, the rest by the ZLB (Central and State Library Berlin) and the districts which are partially under compulsory rule (due to their debts). Even the collaborator in the *Informationsforum* says: “It is not cheap, the introduction of RFID.”

The most important motive for the introduction of RFID in public libraries therefore is the furthering of technology and economy, the search for a possibly large and effective area of application with a big public, where solely through a massive operation acceptance of RFID is produced and data protection and legal considerations can be leveled. After RFID use and self scanning in many areas of commerce (for example Future-Store of the Metro-Group, IKEA and Real) were confronted with rejection or restrained resonance (80% do not use the self scanner

checkout of IKEA, as reported by TAZ of 24/25.10.2009), the use of RFID in large public establishments, which are supported by the trust of their users, delivers a much better push of acceptance.

Librarians need to check, whether they are not abusing the trust their users are giving them, when they are too much willing, directed by a strategy from above, to switch to this “technology with risks”.

Finally, in keyword form I would like to come back to arguments of supporters of RFID in libraries in Berlin and comment on them critically:

1. limited reach of the RFID chips (~12-20” (30-50 cm) / Milfare Mini only 2” (5 cm)
2. only numbers stored on the RFID chip
3. RFID simultaneously takes care of security and simplified inventory
4. with RFID the possibility of 24 hour return is created
5. RFID in libraries deals only with closed systems
6. public data protectors were involved and gave their o.k. to the introduction of RFID in various regions without bigger problems.

To the individual points:

1. As already mentioned above, the reach of 20” of the media chips is sufficient for multiple reading (and misuse) possibilities. The algorithm of the mostly used RFID system Mifare is ‘broken’ and the cards can be duplicated by somewhat clever persons at any time.
2. An unauthorized person can only read numbers, but they are constructed according to a certain structure and give certain hints as to the type of object (library media) and origin of the media (library seal and country), occasionally also the subject area. At RFID customer checkouts it is possible when paying with debit cards to store personal customer data with the notation ‘library user’ and exploit it for advertising purposes.
3. It has been said that with RFID you get complete security, but as soon as RFID technology is implemented, a need is created for more perfect security technology. Libraries which work with RFID as in Singapore, installed videocameras in each row of stacks, which have every user in view. There is no 100% security and should not be desired by libraries. The trouble-free inventory control with RFID equipment promised above, does not work in a lot of cases, simply because many shelves, support posts etc, are made out of metal. That influences the send signal negatively.
4. The return ability of library media round the clock is an old hat. For example in American libraries. There almost every public library has a return drop box, which is accessible from the outside – it has functioned for decades even without RFID.

5. FoeBuD notices to the topic of closed systems with direct reference to libraries: “Although RFID applications are limited today to closed systems, there is going to be a huge demand for standardized labeling. For example, publishers could one day deliver books to libraries and bookstores with labels, which can be written on. Each copy of ‘Grapes of Wrath’ would carry a part of its standard product code, which is identical with every other copy. The library is capable to adjust the rest of the code, to comply with the demands of inventory control....Even if closed systems remain closed, the lack of transparency causes uneasiness from the point of view of privacy. Because many details about closed systems are possibly not easily available, consumers would have great difficulty with the acquisition of information they need, to assess endangerment of their privacy and to be able to protect it.” (<http://www.foebud.org/rfid/unsere-positionen>)

This scenario is very realistic because libraries have for a long time been using the standing order delivery models with the EKZ (Purchasing Central for Public Libraries in Germany) and also with book dealers, and the taking over of further services by the supplier is desired by libraries, because it speeds up the readiness of material/media. Technically it should not pose a problem that for example, the EKZ delivers the material with already inserted RFID chips, the question remains, how far they need the local database for the issuing of numbers.

The colleagues at the ALA early on included a wide circle of people into the data protection consideration. Ulrike Verch writes: “Finally the master guidelines refer to the heretofore barely considered aspect of the contractual relationships to the suppliers of RFID checkout systems (*Talking to vendors about RFID*), by requesting for example, that data control lies solely with the library, that the business conditions of the system supplier do justice to all data protection requirements and that security aspects are to be considered at contract negotiations.”

6. It is my impression that several public data protectors (in Germany) have not taken much pain in signing off on the application of RFID in libraries. In spite of the fact that it was emphatically reported at the librarian’s day in Dresden 2006 that on request of the Bavarian public data protector the old barcode library cards should be kept, the city library of Munich in 2009 introduced new ID cards with RFID. A simple letter to the public data protector and the soothing declaration of the city library, that the new ID cards carry only numbers was sufficient to allow the Mifare cards.

This points to the desire for upgrading, as soon as the first steps for the introduction of RFID technology were taken. In Berlin I was informed in a telephone conversation by a collaborator of the public data protector, that the VOEBB according to

application is going to retain the barcode ID's. Merely an hour later the person in charge of the RFID introduction at the VOEBB told me : "We also want to have library cards with RFID, a letter to this effect has just been sent to the public data protector."

The Berlin public data protector is probably going to check carefully whether to allow this, but for the time being his hands are tied, because he cannot prove, that the RFID cards at present time are "mobile, person specific storage and processing media" according to paragraph 6c of the Bundesdatenschutzgesetz (federal data protection law) or corresponding state laws in Germany. Furthermore the public data protectors, under pressure to being "carriers of concern", could be threatened with hostility or reduced in their competence if they oppose technological modernization.

When reading the brochure "RFID-Einführung in die Öffentlichen Bibliotheken Berlins" (RFID Introduction in Public Libraries of Berlin) it becomes apparent that all participants often talk about what will be possible in the future thanks to RFID: more counseling, furthering of reading, more continued education and qualification; the culture state secretary even dreams from opening the Berlin libraries on sundays and the central project director develops imaginations, how with RFID "spaces and regions can be re-conquered" in the city for public libraries.

Nobody talks about what the introduction of RFID really means for the employees: loss of workplaces. The main council for civil servants (Hauptpersonalrat=HPR) was until now not given a share to participate in the introduction of RFID, but for a member of the HPR who hails from the library system it's clear: "That is a rationalization measure of the finest." The senate does not like to talk about job loss, but they push it off to the districts. Especially hit by the upcoming cutting of jobs are going to be the FAMIs (Fachangestellte für Medien- und Informationsdienste), the clerical employees, because 50% of their tasks are eliminated though self checkout automats.

"At any rate, the library system occupies a leading role in the spread of RFID technology in Germany and should take account for this special responsibility, by aligning itself closely with data protection legal guidelines and ethical principles", says Ulrike Verch.

She recommends that the local libraries should develop their own data protection concepts, by leaning on American recommendations and declaring them binding in the framework of public self commitment. In first place stands the commitment to transparency and openness, to extensive information of citizens about use, contents and purpose of the use of RFID. This includes unconditionally the clear marking of all checkout and reading instruments with an easily recognizable logo and cleartext information on the gadgets and to take along. Neither in Munich nor at the Technical University or Humboldt University library in Berlin there are easily visible directions for the use of RFID technology, if at all then in the small print user information the reader can discover information about this.

That is decidedly too little!.

The library should pledge to uphold the principles of data sparsity, data protection and transparency and that it will do everything to protect the right of each individual library user to confidentiality and privacy. It should develop its own concept of data protection and pledge itself to the principle of data avoidance and to further measures which create transparency. At the transmitting of data, the databases and in relation to system access, security standards have to be followed and have to be checked by a neutral authority. Libraries should nominate RFID representatives, routinely educate personnel on RFID and collaborate closely with personnel council and the public data protector.

In particular libraries should be accountable – this is one main demand of Akribie – to the principle of free choice and should offer for all who reject RFID the possibility for an alternative way of checkout!

Jenny Oltersdorf writes in her master's thesis of 2007 about "RFID in Bibliotheken" (RFID in libraries) at the Institut fuer Bibliotheks- und Informationswissenschaft (Institute for Library and Information Science) of the Humboldt University in Berlin: "In spite of this the implementation of RFID in the public sphere has a dimension which threatens privacy....People of the present time are uneasy, because the real and potential possibilities of RFID are not within reach for them and the effects of technology in the long run appear barely controllable." A feeling of uneasiness seems to spread, which in the long run could lead to behavioral changes. She continues: "The efforts of public libraries for social justice and equal opportunity are being carried ad absurdum, when unsure patrons consider, which item not to borrow, because they cannot calculate, which potential reach into their privacy is possible with the borrowing of a library item with RFID label."

In the name of Akribie I would like to emphasize again at the conclusion: with the use of RFID technology in libraries an abuse at the cost of readers is principally not impossible.

We therefore say: Librarian's ethic demands to do without RFID in libraries.

I thank you for your attention.

Bibliography:

Basiswissen RFID. 2nd ed. Berlin: Informationsforum RFID, 2007.
Basiswissen Internet der Dinge. Berlin: Informationsforum RFID. 2009

Gewissensbisse. Ethische Probleme der Informatik. Biometrie – Datenschutz – geistiges Eigentum. Ed. by Debora Weber-Wulff a.o. Bielefeld 2009.

Das „Internet der Dinge“. Die Informatisierung der Arbeitswelt und des Alltags. Erläuterungen einer neuen Basistechnologie. Ed. by Alfons Botthof / Marc Bovenschulte. Düsseldorf: Hans-Böckler-Stiftung, 2009.
http://www.boeckler.de/show_product_hbs.html?productfile=HBS-004457.xml

Oltersdorf, Jenny: RFID in Bibliotheken – Ökonomische, juristische und informationsethische Aspekte des Einsatzes von Radio Frequency Identification in Öffentlichen Bibliotheken. Magisterarbeit. Humboldt-Universität zu Berlin, 2008.
<http://edoc.hu-berlin.de/master/oltersdorf-jenny-2008-02-14/HTML/>

Technologische Innovation als Stärkung der Bürgerkommune: RFID-Einführung in die Öffentlichen Bibliotheken Berlins. Auftaktveranstaltung am 29.Mai 2009 im Ernst-Reuter-Haus. Ed.: ZLB-Zentral- und Landesbibliothek Berlin, VOEBB, 2009.
Current information about the project:
<http://www.bibliotheksportal.de/hauptmenue/Themen/rfid/praxis/voebb>

Verch, Ulrike: Selbstklebend, selbstverbuchend und auch selbstverpflichtend? Rechtliche Rahmenbedingungen für den Einsatz von RFID-Chips in Bibliotheken.
<http://www.opus-bayern.de/bib-info/volltexte/2007/305/pdf/verch-leipzig-2007.pdf>

About the work of Akribie (Working Group of Critical Librarians):
www.akribie.org