Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

RFID Privacy Concerns: A Conceptual Analysis in the Healthcare Sector

Rachida Parks
Pennsylvania State University, rfp127@psu.edu

Wen Yao
Pennsylvania State University, wxy119@psu.edu

Chao-Hsien Chu
Pennsylvania State University, chu@ist.psu.edu

RFID Privacy Concerns: A Conceptual Analysis in the Healthcare Sector

Rachida Parks
Pennsylvania State University, USA
rfp127@psu.edu

Chao-Hsien Chu
Pennsylvania State University, USA
chu@ist.psu.edu

Wen Yao
Pennsylvania State University, USA
wxy119@psu.edu

ABSTRACT

Radio Frequency Identification (RFID) is a wireless technology that utilizes radio waves to automatically capture data for identifying and tracking objects and/or people. As the use of RFID has grown, so has the chorus of privacy invasions against this identity-aware technology. With the planned deployment and use of RFID in healthcare, there are concerns regarding the social, technological and regulatory complexity of the RFID technology vis-à-vis the requirements of the Health Insurance Portability and Accountability Act (HIPAA). In this paper we use the principles of Fair Information Practice (FIP) as a guideline to examine the design of Privacy Enhancing Technologies (PETs). The outcome shows that PETs fail to incorporate the FIP principles and the importance of examining the social aspect of this ubiquitous technology from a socio-technical perspective. The socio-technical perspective, with its emphasis on the examination of complex relations among social and technical interactions of RFID, can provide a useful insight to assess the societal impact and changes to individual behavior that may arise from privacy concerns. We believe that, using the groundwork laid down in this study, future research along these directions could contribute significantly to addressing privacy concerns expressed about RFID in the context of healthcare.

Keywords

RFID, Privacy Enhancing Technologies (PETs), Fair Information Practice (FIP), Healthcare

INTRODUCTION

RFID is a two edged sword technology. On one hand, it introduces new capabilities for reducing labor costs, managing inventory – forecasting and planning, and minimizing theft in real time; On the other hand, there is increased awareness and anxiety over its potential to trigger privacy violations (Juban and Wyld, 2004). The very properties of RFID that make the technology attractive also make it vulnerable to eavesdropping and privacy violations, a condition that has triggered protest from several privacy and civil rights groups (privacyrights.org, 2003) against the adoption and use of RFID by companies like Wal-Mart, Gillette, and Benetton. Weis, Sarma, Rivest, and Engels (2004) warned that unauthorized readers may compromise privacy by accessing tags without adequate access control. The ubiquity and low maintenance costs associated with RFIDs makes it an appealing technology not just to check stock levels or ensure baggage does not get lost in transit – but as an enabling technology in the healthcare industry.

The contactless communication capability is what differentiates RFID from other traceability technologies such as bar coding. The advent of RFID as a healthcare traceability technology results from the industry drive to access medical inventory and the location of patients and healthcare providers in real time to avoid malpractice, such as operating on the wrong person, or leaving equipment inside the patient's body after surgery. Despite the advantages of RFID systems and its successful implementation in several retail and supply chains, several issues yet remain to be resolved, including the security and privacy challenges associated with the widespread adoption of RFID. Although many innovative technologies, like PETs, have been developed to tackle security problems in the hope of addressing the privacy concerns (Juels, 2006), we cannot merely address the problems by introducing more technical solutions. Social aspects need to be examined for this ubiquitous computing technology through a socio-technical perspective, which is the main focus of this paper.

The challenges associated with RFID in healthcare include not only electromagnetic radiation but also privacy compliance issues in regards to the existing regulations. In an effort to improve the efficiency and effectiveness of the U.S. health care

system, the US congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191. Passage of HIPAA with its administrative simplification provisions required the establishment and adoption of national standards for electronic health care transactions and code sets, unique health identifiers, and security. Congress' recognition that advances in electronic technology could erode the privacy and confidentiality of health information led to the adoption of Federal privacy protections for individually identifiable health information. These protections established national standards for the protections of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct standard health care transactions electronically. The privacy protections also permitted the disclosure of personal health information needed for patient care and other important purposes. The privacy rules of HIPAA protect individuals' protected health information (PHI) by dictating how and when a person's PHI may be disclosed and for what reason. It grants individuals more involvement by allowing specific rights to access their medical records and to request amendments, to authorize or restrict the disclosure of their information, to be informed of the way in which their information is shared with others, and to be informed of their rights relating to privacy (Choi, Cptitan, Krause and Streeper, 2005). HIPAA mandates the enforcement of notice, choice, access, and security which are the principles of FIP, and provides penalties for violations and wrongful disclosures of health information.

RELATED RESEARCH

Current security and privacy research in RFID has predominately focused on different forms of access control (Juels, 2006; Weis, Sarma, Rivest and Engels, 2004). A limited number of research studies have focused on the privacy aspects of RFID (Sharma, Thomas, and Konsynski, 2008) and even less on combining RFID and healthcare (Lee and Shim, 2007). Ultimately, there is very little known about how privacy concerns must be addressed in the healthcare industry with the newest wireless and location-based technologies. While there is an abundance of PETs literature for the Internet and online users (Argyrakis, Gritzalis, and Kioulafas, 2003; Goldberg, 2003; Gritzalis, Moulinos, and Kostis, 2001), only a few studies have emerged for RFID (Spiekermann, 2007; Hennig, Ladkin, and Sieker, 2005, Floerkemeier, Schneider and Langheinrich, 2005, Thiesse, Floerkemeier, Fleisch and Sorensen, 2007), and limited research has focused on the use of RFID in the healthcare domain.

Thiesse (2007) investigated one side of this gap by focusing on the perception of risk and how it impacts RFID adoption. Thiesse et al. (2007) had called for an "open dialogue" with the users to create "technology trust" along with security measures. Langheinch (2001) provided a great foundation for privacy principles guiding system design. We further these non technical perspectives by using FIP as privacy guidelines to examine the design of PETs within the context of healthcare. The outcome of such a process leads us to embrace a socio-technical approach. Despite the abundance of IT research with a socio-technical perspective, a combination of the uniqueness of RFID and its privacy issues within the healthcare domain remain yet untapped. The purpose of our paper is to fill some of these gaps by reviewing PETs that could be applicable for RFID in healthcare and generating a socio-technical trend for this new era of wireless technology and specific domain.

RESEARCH METHODOLOGY

We use a semi-structured research methodology for reference search, data collection, and analysis. The research design for this review and analysis is divided into four parts: literature identification and collection; categorization and comparative review of PETs; collection of protest cases and mapping with FIP to justify the need for a socio-technical approach. We used databases, including ABI/INFORM, ACM Digital library, Elsevier ScienceDirect, IEEE Explore, Springer-Verlag, to search related literature. PET literature was collected and classified into categories based on the RFID tag characteristics and functionalities. We then examine the characteristics of each technology and its application domain. We proceed with mapping PETs to FIP principles, and use protest cases to justify the need for a socio-technical approach.

PETS IN RFID

PETs are technical measures provide satisfactory response to privacy concerns. Several technologies have been developed to overcome security and privacy threats; however, to our knowledge, a limited number of studies have attempted to offer taxonomy for the selection of appropriate PETs. We divide PETs into two categories: physical and logical solutions. The logical solutions can be further divided into three subcategories: destruct, control and encrypt approaches (See Figure 1).

Physical Solutions

Two distinct methods have been used for physical solutions: Faraday cage and jamming. A Faraday cage is an enclosure formed by a conducting material or by a mesh of such material. Such an enclosure blocks out external static electrical fields (Kumar, 2003). The advantage of this approach is that it is impenetrable by radio signals; however some items may not fit within the container due to size constraint. In the active jamming method, the consumer would carry a device that disrupts

and/or blocks the operation of nearby RFID readers by actively broadcasting radio signals. This approach may be illegal and also may cause severe disruptions of all nearby RFID readers (Juels, Rivest and Szydlo, 2003).

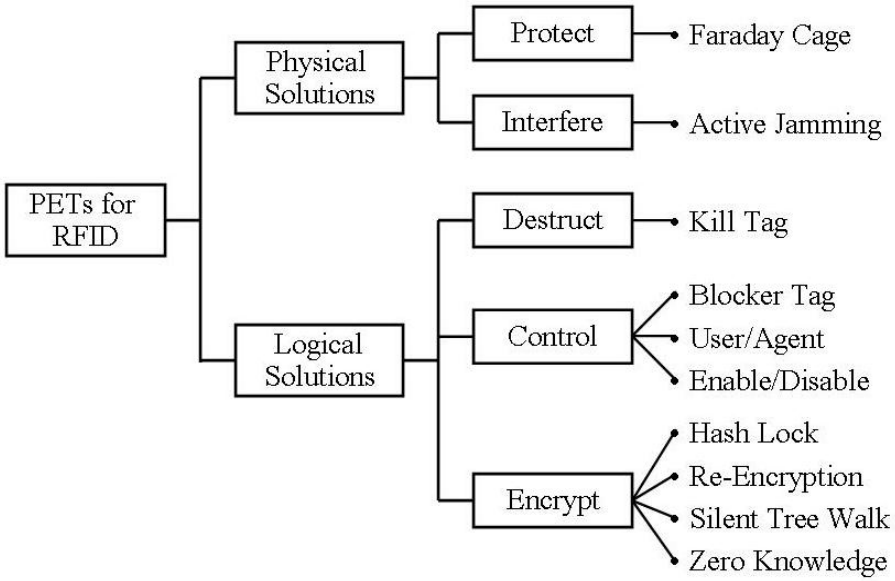

Figure 1. Taxonomy of PETs for RFID

Logical Solutions

Destruct

Juels (2006) suggested that the most straightforward approach to protect consumers' privacy is to "kill" the RFID tag after the sale is completed. This approach received controversial criticism: on one hand, no other readers can track what a particular person buys, their likes or dislikes; on the other hand, many refer to this approach as inadequate as consumers may want to take advantage of the tag's interaction with other products, for example a microwave might read cooking instructions from the tag, washing machines adjusting to their loads or smart refrigerators that automatically check expiration-dates and alert product recalls. Spiekerman (2007) concurred that killing a tag's functionality curtails the future potential use of RFID in consumer services. Clearly, this approach has limitations for use in the retail industry. In the context of healthcare, killing the tag is infeasible as patients need to be tracked at all time during their stay at a healthcare facility.

Control

Spiekermann (2007) proposed an alternative to the kill function by enabling or disabling features in the tag. When a consumer pays for his products, all tags are automatically disabled instead of killed and a 24 bit password is generated on a printed receipt that the consumer can control to enable the tags. Although this model seems beneficial to both users and retailers while protecting privacy, it is still unrealistic in the healthcare applications. Another control approach is the use of RSA blocker (Juels et al., 2003) tag which is an RFID tag that responds positively to all unauthorized requests, thus, blocking some scanners from reading nearby RFID tags. The tags are designed to protect privacy and are supposedly unable to be used for theft, denials of service, and other malicious uses. This tag works by spamming any RFID reader that attempts to scan tags without authorization, thereby, creating a hostile environment for the reader. This technology may add a burden to consumers and will fail to protect when products are separated from the blocker device. A version of the blocker tag can serve as an "Agent PET" or "User PET," where the latter gives users an immediate control over their RFID tags at the client side. Agent PETs are based on the idea that RFID tags are unlocked by default and that the network takes the initiative to communicate with a user's tag. This approach gives users control over the uniqueness of IDs; however, it is application dependent. Since the after-sale area does not apply to the healthcare sector, the method cannot be used in healthcare applications.

Encrypt

The hash-lock (Weis et al., 2004) scheme requires implementing a hash function on the tag and managing keys on the back end. A tag may be locked so that it refuses to reveal its ID until it is "unlocked" by the owner. Tags may still function as object identifiers while in the locked state by using the metaID for database lookups. Unfortunately, since the metaID acts as an identifier, tracking of individuals is possible under this scheme. The re-encryption method has been proposed to reduce the linkability by using multiple public keys where RFID tags embedded in consumer or banknote (Juels et al., 2003) undergo re-encryption. They employ a public-key cryptosystem with a single key pair: a public key and a private key held by an appropriate law enforcement agency. The drawback to this approach is the extensive infrastructure of re-encryption needed. Weis et al. (2004) showed how to encrypt the reader's transmissions so that a passive eavesdropper cannot infer the IDs being read. This approach does not defend against active attacks and it is quite costly. Finally, as to the zero knowledge authentication method (Engberg, Harning and Jensen, 2004), tags are able to verify that an RFID reader has the proper authority to read it but does not require the tag to reveal any identifying information during the authentication process.

FIP COMPLIANCE THROUGH PETs

FIP was initially proposed in 1973 in response to the growing use of automated data systems containing information about individuals. FIPs are a set of principles for addressing the privacy of individual information collected, used and maintained by both public and private sector organizations. These core principles: Notice/Awareness; Choice/Consent; Access/ Participation; and Integrity/Security were intended to safeguard individual privacy and have become the intellectual framework for laws addressing privacy and data protection matters.

Most PETs for RFID have been applied to retail with limited application to healthcare which motivated us to review some relevant PET factors in order to check how applicable they are in healthcare. The observations can be categorized into Table 1:

PETs	Application Domain	FIP	Cost	Tag Type	Apply Time	Major References
Faraday Cage	Retail	Choice, Security	Cheap	Passive	Post-purchase	Eschet, 2005; Juels and Pappu, 2003; Kumar, 2003
Active Jamming	Retail	Choice, Security	Cheap	Passive	Post-purchase	Juels et al., 2003; Kumar, 2003
Tag Killing	Retail	Security	Cheap	Passive/ Active	Post-purchase	Fishkin, Roy and Jiang, 2004; Spiekermann, 2007
Enable/Disable	Retail	Choice, Security	Cheap	Passive	Post-purchase	Hennig et al., 2005; Spiekermann, 2007; Spiekermann and Berthold, 2005
Blocker Tag	Retail	Choice, Security	Cheap	Passive	Post-purchase	Juels et al., 2003; Juels and Brainard, 2004
User/Agent PET	Retail	Choice, Security	Cheap	Passive	Post-purchase	Spiekermann, 2007
Hach-Lock	General	Security	Cheap	Passive	Post-purchase	Weis et al., 2004
Re-encryption	Banking	Security	Expensive	Active	In-store/post-purchase	Juels and Pappu, 2003
Silent-tree Walking	General	Security	Expensive	Active	In-store/post-purchase	Juels et al., 2003; Weis et al., 2004
Zero Knowledge	Retail	Security	Moderate/ Expensive	Active	In-store/post-purchase	Engberg et al., 2004

Table 1. Comparative Analysis of PETs for RFID

- FIP. When mapping PETs to the FIP principles, Table 1 shows that most PETs are centralized around two principles consent/choice and/or integrity/security excluding other principles from their design. With PETs such as Faraday cage, enable/disable (Hennig et. al., 2005), the consumer have the choice to conveniently disable or discard the RFID tag from the product they acquired. PETs with re-encryption or zero knowledge capabilities (Engberg et al., 2004), incorporate

mainly the security principle in their design. While an "Encrypt" logical solutions ensure security and seems more applicable to healthcare; cost and other principles need to be examined.

- PETs and tag type. There is a direct relationship between the type of tags being used and the associated cost. Passive tags are cheap compared to active tags. It is obvious that the cost is a major concern in healthcare and the lower is the better assuming it provides the optimum privacy.
- Apply time. With RFID having been applied mainly in retail, research studies focused on pre/post-purchase timeframes. Most PETs are targeting on post-purchase (Spiekermann, 2007), where consumer privacy could be threaten by unauthorized readers eavesdropping. In the healthcare sector, post-purchase scenario is irrelevant. Patients completely remove their tags when they leave the hospital so the concerns of being tracked outside the healthcare facility are non-existence. The threat comes from the possible eavesdropping while they are at the hospital facility. Security concerns relevant to patients with implantable RFID tags are subject to different issues (Halamka, Juels, Stubblefield and Westthues, 2006). While the physical and some of the logical (destruct and control) may not be optimum, encryption approaches are more appropriate to healthcare though more expensive.

PROTEST AGAINTS RFID

To reinforce the importance of examining the social aspect, we collect several protest cases related to RFID across industries. Table 2 provides an overview of why people are protesting RFID adoption and which principles of FIP could have prevented the protest had it been included. We are considering the user-centered principals of FIP: Notice, Choice and Access. Security principal is not being considered as it was already included within the technical approach of PETs.

Privacy groups continue to portrait RFID as a highly intrusive technology with severe impact on individual's privacy and most of the protests generated enough reactions to cause certain businesses (e.g., Gillette, Tesco, Benetton) to halt or make adjustments to the adoption of RFID. Most of these protests were manifested because of the possible privacy violations and lack of consumers' choice, notification and access to collected information. In Ohio birthing centers (Corsi, 2008), an RFID infant protection system was placed on infants at birth to prevent them from being abducted from the hospital or from being given to the wrong mother. Despite the fact that the system triggers an alarm that can cause hospital entrances and exits to lock shut if a newborn is removed from the ward without authorization or a baby is placed with the wrong mother, critics accuse the system of being an intrusive technology solution to a problem that is rare. Not creating an awareness of the system among employees resulted in no one reporting an abductor dressed in scrubs because "they thought the RFID system would take care of any problem." Not being given a choice "The mothers are not asked." (Corsi, 2008), seems another reason for this protest. Had this facility embraced the notice and choice of FIP when implementing their RFID system, the protest could have been prevented.

Current protest cases appeared predominantly in retail with fewer in healthcare due mainly to the infancy stage of RFID in this domain. With the expansion of RFID technology in healthcare, more protests are to be expected if privacy and security issues are not handled in perspective of HIPAA.

DISCUSSION

Most PETs do not provide adequate protection from RFID technology and this has hampered the widespread adoption of the RFID technology in the healthcare industry due to the privacy related regulations (HIPAA, Children's Online Privacy Protection Act (COPPA)). While technical measures are important, (See Table 1), there is a limited number of a research studies where PETs incorporate more than two principles associated with FIP. Concerns raised in the protests against RFID could have been addressed with measures that incorporate user-centered principles (Garfinkel, 2002). Langheinrich (2002) concurred that technical protection alone cannot protect against privacy threats and brought attention to two principles: awareness and access, to create a sense of awareness and accountability to information privacy. Garfinkel (2002) proposed an RFID bill of rights which is a voluntary framework for commercial deployment of RFID tags. Because it addresses only the user side, and not the technical aspect (security), the five principles within RFID Bill of Rights focus on notice, choice and the access principles of FIP. Healthcare organizations adopting RFID technology can use encrypted PETs solution along with social measures to empower user control - ability to enable or disable the tags, and provide access to the data collected.

When	Industry	Who/Where	Why	Impact	References	FIP
2003	Retail	Benetton, Italy	Clothes embedded with RFID tags	Publicly retreated from plans	Starrett, 2003	Notice, Choice
2003	Retail	Tesco, UK	Use smart tags to track and photograph shoppers	No change	Muncaster, 2005	Notice, Choice, Access
2003	Retail	New Jersey Inst. of Tech., USA	Tag bullets and firearms with RFID	Only allow police officers to tag their guns	Abolins, 2003	Notice, Choice
2003	Retail	Gillette, UK	Hide RFID chips in the packaging	Gillette pulled RFID tags in UK amid protests	Boycott Gillette, 2003	Notice
2004	Retail	Metro AG, Germany	Hide RFID tag in store loyalty cards, shopping carts, and on packages	Stopped to use radio chip card	Black, 2004	Notice, Choice
2005	Public Services	UC. Berkley Library, USA	Personnel layoff and consumers privacy	Forced to organize awareness sessions	Berkeleycitizen. org, 2005	Notice
2005	Public Services	Brittan Elementary School, USA	Violate students' privacy by having them wear tagged IDs	Stop RFID test pilot program	Leff, 2005	Notice, Choice, Access
2007	Healthcare	VeriChip, USA	Implanted microchip-induced tumors in laboratory rodents and dogs	Reverse all animal chipping mandates. Further chipping of humans should be immediately discontinued	Albrecht, 2007	Notice, Choice
2008	Conference	Conference, USA	Protest the use of RFID in individual clothing items	More business were attending each year	Online Security Authority, 2008	Choice
2008	Government	Dept. of Agriculture, USA	Protest against cattle tag with RFID	Lawsuit dismissed by Bush administration	Kravets, 2008	Choice
2008	Government	Government, UK	Inject RFID tags for prisoners released	Denied by the Ministry of Justice	RFIDnews.org, 2008	Choice
2008	Healthcare	Ohio, USA	Birth centers turn to tracking babies with electronic chips	Claimed it has prevented baby abductions	Corsi, 2008	Notice, Choice

Thiesse et al., (2007) had called for an "open dialogue" with the users to create "technology trust" along with security measures. This opportunity can be further examined through more rigorous involvement in the design steps of PETs through a social-technical perspective. The socio-technical approach is based on the concept of interactions and interdependence between machines/tools and people with the goal of achieving a joint optimization of both social and the technical systems (Bostrom and Heinen, 1977). Any organizational system maximizes performance only if the interdependency of the subsystems is explicitly recognized. Hence, any design or redesign must seek out the impact each subsystem has on the other, and planning must aim at achieving superior results by ensuring that all the subsystems are working in harmony.

Within healthcare, HIPAA requirements can be met by incorporating FIP guidelines to RFID technology. Existing PETs for RFID are designed with security in mind but integrating all principles of FIP principles is yet to be achieved. While healthcare facilities can easily implement privacy awareness programs and ask for patients' consent to make the final decision to participate in RFID, the third FIP access, that would enable subject individuals to review their collected data in a timely, accurate and inexpensive manner remains challenging. This FIP standard of access not only improves integrity of collected information but also may prevent unnecessary protests that have been impacting other sectors such as retail.

CONCLUSION AND OUTLOOK

Despite the fact that technical solutions have a great appeal and tamper proof, the deficiencies in PETs of RFID demonstrate that the answer to the privacy concern is not another technology (Langheinrich, 2002). Before it is secured and trusted enough by millions of ordinary consumers to be absorbed into the economic and social infrastructure, the related security threats must be recognized and appropriate countermeasures taken by RFID developers and vendors, as well as by government regulatory agencies (Ohkubo, Suzuki, and Kinoshita, 2005). The opportunities of RFID technology are limitless, as are the possibilities for the technology to be misused. RFID can impact drastically the efficiency, accuracy and availability of information within healthcare, but a socio-technical perspective must be taken into consideration to leverage its full potential. This paper not only provides an integrative overview of PETs for RFID and provides a taxonomy that maps PETs into the framework of FIP, but also exposes the lack of consideration for RFID's impact upon people who will use it, and the associated privacy issues within healthcare.

Due to the special context needs of healthcare and the privacy regulations under HIPAA, adoption of RFID is dependent upon incorporating the user-centered principles of FIP in addition to technical security measures. Since RFID still at its infancy in healthcare, this approach will greatly prevent hostilities that already started on the horizon such as the association of RFID and cancer (Albrecht, 2007), and RFID and electromagnetic interference (Van der Togt and Van Lieshout, 2008). From a practice perspective, we believe that the evidence of protests to RFID adoption underscores the point that the introduction of a social perspective through awareness, choice and access ease the adoption of RFID. Using the groundwork laid down in this study, future research along these directions could contribute significantly to addressing privacy concerns expressed about RFID in the context of healthcare and HIPAA.

ACKNOWLEDGEMENT

We are grateful to Heng Xu (Penn State University) and Lascelles A. Adams (University of Central Florida) for their helpful suggestions and comments.

REFERENCES

Abolins, J. (2003) RFID and firearms. Available at: http://www.jpfo.org/alerts/alert20030907.htm [Accessed January 23, 2009].

Albrecht, K. (2007) Microchip-cancer report. Available at: http://www.antichips.com/cancer/index.html [Accessed January 22, 2009].

Argyrakis, J., Gritzalis, S. and Kioulafas, C. (2003) Privacy enhancing technologies: A review, *Lecture Notes in computer Science, Electronic Government*, 2739, 282-287.

Berkeleycitizen.org (2005) RFID protest rally. Available at: http://www.berkeleycitizen.org/community/rfid1.html [Accessed January 24, 2009].

Black, J. (2004) Shutting shopping bags to prying eyes. Available at: http://www.businessweek.com/technology/content/mar2004/tc2004035_8506_tc073.htm [Accessed January 23, 2009].

Bostrom, R.P. and Heinen, J.S. (1977) MIS problems and failures: A socio-technical perspective, Part I: The causes, *MIS Quarterly*, 1, 3, 17-32.

Boycott Gillette. (2003) CASPIAN launches worldwide Gillette boycott. Available at: http://www.boycottgillette.com/pressrelease8-11.html [Accessed January 22, 2009].

Choi, Y.B., Capitan, K.E., Krause, J.S., and Streeper, M.M. (2006) Challenges associated with privacy in healthcare industry: implementation of HIPAA and security rules, *Journal of Medical Systems*, 30, 1, 57–64.

Corsi, J. (2008) Hospitals tagging babies with electronic chips. Available at: http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=59690 [Accessed January 24, 2009].

Engberg, S.J., Harning, M.B. and Jensen, C.D. (2004) Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience, *The Second Conference on Privacy, Security and Trust, New Brunswick, Canada*, 1-13.

Eschet, G.A.L. (2005) FIPs and PETs for RFID: Protecting privacy in the Web of radio frequency identification, *Jurimetrics*, 45, 301-332.

Federal Trade Commission (FTC), Fair information practice principles. Available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm [Accessed January 22, 2009].

Fishkin, K.P., Roy, S. and Jiang, B. (2004) Some methods for privacy in RFID communication, *1st European Workshop on Security in Ad-Hoc and Sensor Networks*, Springer, 42–53.

Floerkemeier, C, Schneider, R, Langheinrich, M. (2005) Scanning with a purpose-supporting the fair information principles in RFID protocols. *Lecture Notes in Computer Science, Ubiquitous Computing Systems.* 3598, 214.

Garfinkel, S. (2002) Adopting fair information practices to low cost RFID systems. *Ubiquitious Computing*.

Garfinkel, S.L., Juels, A., and Pappu, R. (2005) RFID privacy: An overview of problems and proposed solutions, *IEEE Security & Privacy*, May-June, 34-43.

Goldberg, I. (2003) Privacy-enhancing technologies for the Internet, II: five years later, *Lecture Notes in Computer Science, Public Key Infrastructure*, 2482, 1-12.

Gritzalis, D., Moulinos, K. and Kostis, K. (2001) A privacy-enhancing e-business model based on infomediaries, *Lecture Notes in Computer Science, Information Assurance in Computer Networks*. 2052, 72-83.

Halamka, J. Juels, A. Stubblefield, A. and Westhues, J. (2006) The security implications of VeriChip cloning. *Journal of the American Medical Informatics Association*. 13, 6, 601-607.

Hennig, J.E., Ladkin, P.B. and Sieker, B. (2005) Privacy enhancing technology concepts for RFID technology scrutinised, Available at: http://www.rvs.uni-bielefeld.de/publications/Reports/PETC_RFID_Scrutinised.pdf [Accessed February 19, 2009].

Juban, R.L. and Wyld, D.C., (2004). Would you like chips with that? Consumer perspectives of RFID. *Management Research News* 27, 11/12, 29–44.

Juels, A. (2006) RFID security and privacy: A research survey, *IEEE Journal on Selected Areas in Communication*, 24, 2, 381-394.

Juels, A and Brainard, J. (2004) Soft blocking: Flexible blocker tags on the cheap. In: *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*. ACM New York, NY, USA, 1-7.

Juels, A. and Pappu, R. (2003) Squealing Euros: Privacy protection in RFID-enabled banknotes, *Lecture Notes in Computer Science, Financial Cryptography*. 2742, 103-121.

Juels, A., Rivest, R.L. and Szydlo, M. (2003) The blocker tag: selective blocking of RFID tags for consumer privacy, *Proc. of the 10th ACM conference on Computer and communications security*, ACM New York, NY, USA, 103-111.

Kumar, R. (2003) Interaction of RFID technology and public policy. *Wipro White Paper*.

Kravets, D. (2008) Bush administration: dismiss RFID 'mark of the beast' lawsuit. Available at: http://blog.wired.com/27bstroke6/2008/11/bush-administra.html [Accessed January 24, 2009].

Langheinrich, M. (2001) Privacy by design-principles of privacy-aware ubiquitous systems**.** *Lecture Notes In Computer Science. Proc. of the 3rd International Conference on Ubiquitous Computing*, 2201 273-291.

Langheinrich, M. (2002) A privacy awareness system for ubiquitous computing environments**.** *Lecture Notes in Computer Science. Proc. of the 4th International Conference on Ubiquitous Computing*. 2498, 237-245.

Lee, C-P and Shim, J. (2007) An exploratory study of radio frequency identification (RFID) adoption in the healthcare industry. *European Journal of Information Systems*, 16, 6, 712-724.

Leff, L. (2005) Students ordered to wear tracking tags. Available at: http://www.msnbc.msn.com/id/6942751 [Accessed January 24, 2009].

Muncaster, P. (2005) Tesco sparks RFID protest. *IT week.* Available at: http://www.vnunet.com/itweek/news/2085767/tesco-sparks-rfid-protest [Accessed December 23, 2008].

Ohkubo, M. Suzuki, K. and Kinoshita, S. (2005) RFID privacy issues and technical challenges. *Communications of the ACM*, 48, 9, 66-71.

Online Security Authority (2008) RFID where? You'd better look at your shoes, socks and underwear! Available at: http://www.onlinesecurityauthority.com/thoughts-on-security/rfid-where-youd-shoes-socks/ [Accessed January 24, 2009].

Privacyrights.org (2003). RFID position statement of consumer privacy and civil liberties organizations. Available at: http://www.privacyrights.org/ar/RFIDposition.htm [Accessed January 23, 2009].

RFIDnews.org (2008). Prisoners may be RFID-chipped in the UK. Available at: http://www.rfidnews.org/2008/01/13/prisoners-may-be-rfid-chipped-in-the-uk [Accessed January 14, 2009].

Sharma, A., Thomas, D. and Konsynski, B. (2008) Strategic and institutional perspectives in the evaluation, adoption and early integration of radio frequency identification (RFID). In *Proc. of the 41th Hawaii International Conference on System Sciences*.

Spiekermann, S. (2007) Privacy enhancing technologies for RFID in retail - an empirical investigation, *Lecture Notes in Computer Science, Ubiquitous Computing* , 4717, 56.

Spiekermann, S., and Berthold, O. (2005) Maintaining privacy in RFID enabled environments-Proposal for a disable-model, *Privacy, Security and Trust within the Context of Pervasive Computing* (780).

Starrett, M. (2003) I'd rather go naked. Available at: http://newswithviews.com/Mary/starrett4.htm [Accessed January 23, 2009].

Thiesse, F. (2007) RFID, privacy and the perception of risk: A strategic framework. *Journal of Strategic Information Systems*. 16, 2, 214-232.

Thiesse, F, Floerkemeier, C, Fleisch, E, Sorensen, C. (2007) Assessing the impact of privacy-enhancing technologies for RFID in the retail industry. *AMCIS 2007 Proceedings*.223.

Van der Togt, R. and Van Lieshout, J. (2008) Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment, The *Journal of the American Medical Association*, 299, 24, 2884.

Weis, S.A., Sarma, S.E., Rivest, R.L. and Engels, D.W. (2004) Security and privacy aspects of low-cost radio frequency identification systems, *Lecture Notes in Computer Science*, *Security in Pervasive Computing* , 2802, 201-212.