RFID Privacy Issues in Healthcare: Exploring the Roles of Technologies and Regulations

Rachida Parks, The Pennsylvania State University, USA
rfp127@ist.psu.edu
Chao-Hsien Chu, The Pennsylvania State University, USA
chu@ist.psu.edu
Heng Xu, The Pennsylvania State University, USA
hxu@ist.psu.edu

ABSTRACT

With the deployment and use of Radio Frequency Identification (RFID) technology in the healthcare domain, there are increasing privacy concerns regarding the technical designs of RFID systems vis-à-vis the requirements of the healthcare regulations. This paper reviews and analyzes the impact of privacy issues in the RFID adoption in the healthcare domain, and presents a conceptual framework for analyzing the relationship between technology and regulations in light of the Fair Information Practice (FIP) principles to ensure patients' privacy. Our conceptual framework uses the FIP principles as a guideline to examine the design of Privacy Enhancing Technologies (PETs) and analyze existing regulations to assess the compliance issues. The conceptual analyses show that current PETs fail to incorporate the FIP principles and thus organizations in the healthcare sector face complex challenges to comply with security and privacy standards and regulations. Using the groundwork laid down in this study, future research along these directions could contribute significantly to address privacy concerns pertaining to RFID for both academia research and industry practice in the context of healthcare.

KEY WORDS

Radio Frequency Identification (RFID), Healthcare, Privacy Enhancing Technologies (PETs), Fair Information Practice (FIP) Principles, Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health (HITECH)

INTRODUCTION

Recently, the growing influence of RFID has attracted significant attention in healthcare. By leveraging heightened patient safety (Neil, 2005), better tracking of drug supplies (Young, 2004), and real time management of hospital assets (Becker, 2004a; Davis, 2004), RFID technologies have enormous potential for reducing operating costs and improving patient safety (Wang et al., 2006). According to the findings of a study assessing the financial benefits of RFID in retail and healthcare, $40 billion have already been reported in benefits with an estimated return on investment of over 900 percent (Barua et al., 2006).

Unsurprisingly, RFID is a double-edged sword technology and its potential benefits have been accompanied by threats of privacy violations (Juban & Wyld, 2004). These threats pertain to the potential risks of unauthorized data access, misuse of patient data, and the capabilities of permanently saving and linking information about individuals through temporal and spatial extension of data collection activities (Thiesse et al., 2007). RFID tags can be read by unauthorized reader without the victim's knowledge since individuals are not sensitive to radio signals (Eschet, 2004).

These threats have led to protests by privacy and civil right groups against RFID adoption (Privacyrights.org, 2003). Boycotts have targeted organizations such as Wal-Mart, Gillette (Boycott-Gillette, 2003), and Benetton (Starrett, 2003). To address these threats, many innovative Privacy Enhancing Technologies (PETs) have been developed with the hope of addressing these privacy concerns (Juels, 2006; Weis et al., 2004). However, RFID privacy threats cannot be merely addressed by the introduction of technical solutions, thus a call for a combination of both technological and regulatory solutions (Eschet, 2004).

In an effort to alleviate privacy concerns and improve the effectiveness of the U.S. health care system, the Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191. Enforcement of HIPAA required the establishment and adoption of national standards for electronic healthcare transactions and code sets, unique health identifiers, and security compliance. Congress' recognition that advances in IT could erode the privacy and confidentiality of health information led to the adoption of privacy regulations for protecting individual identifiable health information.

Currently, the bulk of research on RFID security and privacy has purely focused on technical solutions (e.g., Juels, 2006; Weis et al., 2004). In the healthcare domain, the focus has mostly been on the analyses of potential benefits and cost of RFID implementation (Wicks, 2006). Little is known about how privacy concerns could be addressed in the healthcare industry with the implementation of wireless and location-based technologies such as RFID.

The objectives of this research are two-fold. First, the study aims to use the principles of fair information practices (FIP), a global standard for protecting consumers' privacy, to assess how well current technological solutions and regulations comply with FIP principles. Second, the study generates a conceptual framework for understanding RFID privacy issues and the interaction between its key elements in the healthcare domain. A conceptual framework allows the conceptual analyses of the relationships among PETs, government regulations, and the FIP principles.

This paper offers a research agenda for studying privacy issues pertaining to the use of RFID in healthcare to address a series of broad research questions related to:

- What kind of existing PETs could be applicable to RFID in healthcare?

- How well do existing PETs comply with the FIP principles?
- How well does HIPAA/HITECH comply with the FIP principles?
- How are the RFID privacy issues in the healthcare domain different from other application domains?

The organization of the paper is as follows: Section 2 is the literature review for this study. The research methodology and conceptual framework are then described in section 3. Analysis and discussion and future directions are presented in section 4. Finally, section 5 concludes by offering managerial and academic implications, examining limitations and providing recommendations for future research.

LITERATURE REVIEW

Privacy has become one of the most important ethical issues of the information age (Mason, 1986). It has been defined as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p.7). Culnan and Armstrong (1999) concurs that privacy is the ability of an individual to control the conditions under which personal information is collected and how it is used. The scope of this research pertains specifically to *information* privacy which is defined as the ability to control over how personal information is acquired and used (Culnan & Bies, 2003). It is differentiated from data privacy that is more focused on disguising data identity such as anonymity, unlinkability, unobservability, or pseudonymity.

RFID systems are composed of three key elements (Weis et al., 2004): the RFID tag, the RFID reader, and the back-end database that associates records with tag data collected by readers. The RFID readers interrogate tags for their contents by broadcasting a radio signal. Tags respond by transmitting back resident data, typically including a unique serial number (Weis et al., 2004). The way such communication occurs differs based on the tag type: passive, semi-passive, and active. Active tags initiate and respond with a stronger signal while passive tag can only respond to the RFID reader's interrogation. The backend IT system is responsible for cross-referencing the RFID tag's ID number with a database record that describes the object to which the tag housed within is attached.

The adoption of RFID in the healthcare domain is still in its infancy but is rapidly becoming the standard for hospitals to track inventory and identify patients (Fisher & Monahan, 2008). Few hospitals have emerged as leaders such as Bon Secours Health System in Richmond (Becker, 2004a), St. Luke Health System in Kansas City (Becker, 2004a), and Beth Israel Medical Center in New York City. However, little research in hospital-specific RFID applications exists (Wicks et al., 2006) and most current applications in hospital settings are small-scale trials (Mowry, 2008).

Embracing RFID systems in healthcare offers great potentials for: 1) improving traceability of medical equipments (Fisher & Monahan, 2008); 2) enhancing patient

safety (Jossi, 2004; Neil, 2005) by electronically identifying patients; 3) better tracking of drug supplies (Young, 2004); and 4) improving efficiency for managing hospital assets in a real time fashion (Davis, 2004).

While RFID technology can improve the overall quality of healthcare delivery, the benefits must be balanced with the privacy and security concerns. The use of RFID introduces a new set of risks: Security risks are associated with the possible failure of the RFID system under various security attacks, i.e. injections, eavesdropping, and denial of service, while the threat to privacy reside in the capabilities to permanently save and link information about individuals through temporal and spatial extension of data collection activities (Thiesse et al., 2007). Although concerns about information privacy are not unique to the healthcare domain, health related information can be perceived as more personal and more sensitive. A recent report by the California HealthCare Foundation found that 67% of the national respondents worry about the privacy of their personal medical records (Bishop et al., 2005). Due to the highly personal and sensitive nature of healthcare data (Westin, 2003), both healthcare providers and patients can be expected to resist further digitalization and data source sharing of personal health data until security and privacy protections are in place.

Current security and privacy research in the context of RFID has predominately focused on using different forms of access control mechanisms for prevention and protection (Juels, 2006; Weis et al., 2004). For instance, Juels (2006) provided a technical solution on the problems of privacy and security for RFID systems through the cryptographic mechanisms and symmetric-key tags approaches. An RFID bibliography compiled by Avoine (2006) with over 360 articles demonstrated that a large number of RFID literature focuses predominately on technical elements of RFID. In the context of healthcare and RFID, Wicks et al. (2006) stated that current literature only focuses on potential benefits and costs related implementation issues, and there is a limited number of academic research on hospital specific applications of RFID. Thus very little is known about how privacy concerns could be addressed in the healthcare industry with the newest wireless and location-based technologies.

Thiesse et al. (2007) investigated one side of this gap by examining individual perception of risk and how it impacted RFID adoption. Thiesse had called for an "open dialogue" with the users to create "technology trust" along with security measures. Langheinrich (2001) provided a theoretical foundation for privacy principles guiding system design. This paper further extends these non-technical perspectives by using FIP principles as the privacy guidelines to examine the design of PETs within the context of healthcare. The outcome of such process leads us to embrace a Technical-Regulatory approach. A combination of the uniqueness of RFID and its privacy issues within the healthcare domain remains yet untapped. The purpose of our paper is to fill some of these gaps by reviewing the literature on PETs that could be applicable for RFID in the healthcare domain and generating a Technical-Regulatory framework for this new era of wireless technology in the specific domain of healthcare.

RESEARCH METHODOLOGY

In this research, relevant publications were acquired via different search engines, databases and libraries. Abstracts of these publications were analyzed to assess the relevance to ensure that they covered the appropriate topics for our review. The process of this review and analysis is divided into four stages: literature identification and collection; categorization and comparative review of technical and legislative measures; mapping of PETs and regulations to the FIP principles; and finally development of a conceptual framework. In addition, publicized protest cases were collected and analyzed, to justify the need for a proactive Technical-Regulatory approach.

The principles of FIP were used as a guideline to examine the design of PETs and existing regulations to assess their compliance. The uniqueness of FIP principles resides in providing a set of guidelines that represent widely-accepted concepts concerning fair information practices in an electronic transaction. A conceptual framework (see Figure 1) was proposed to understand the extent to which current regulations and technologies comply with the principles of FIP. As shown in Figure 1, HIPAA regulations govern the technology design which in return triggered additional privacy and security regulations. A continuous assessment of HIPAA and its shortcomings triggered the recent adoption of HITECH. Figure 1 summarizes the Technical-Regulatory approach used in this research: how the RFID technologies and applications may be better compliant with principles of FIP, and how a technology design or regulation may fail to be compliant with FIP.

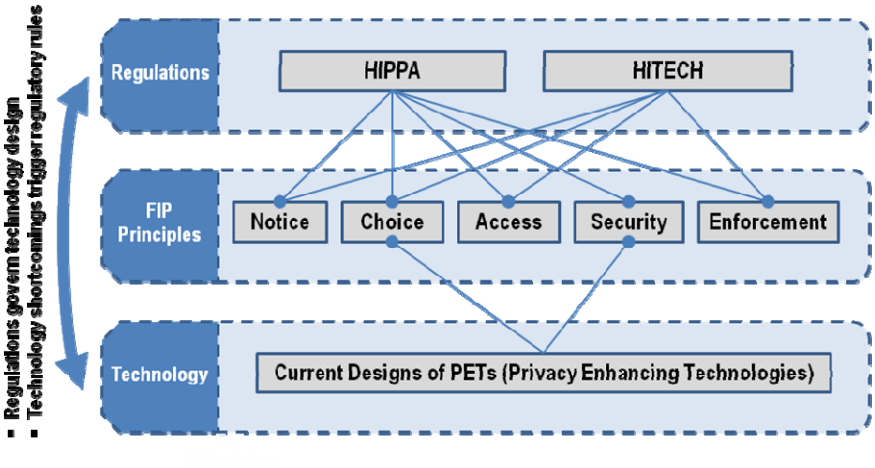

Figure 1. Conceptual Framework

Principles of Fair Information Practice (FIP)

Most of industry self-regulations of privacy and government privacy regulations are based on the principles of FIP, which was originally developed by the US department of Health, Education and Welfare (HEW, 1973). FIP principles are considered one of the most widely-used guidelines for both industry self-regulation and government regulations (Milne & Culnan, 2002; Xu et al., 2010) and include a set of principles for addressing the privacy of personal information collected, used and maintained by both public and private sectors. FIP principles are procedures that provide individuals with control over the disclosure and subsequent use of their personal information (Culnan & Armstrong, 1999).

The FIP principles have been adopted by US agencies, such as the Federal Trade Commission (FTC), to assess how well private sectors regulate themselves. The five core principles are: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress. These principles were intended to safeguard individual privacy and have become the intellectual framework for laws addressing privacy and data protection matters. This study extended the use of FIP principles to RFID use in the Healthcare environment (Table 1) based on Peslak's work (2005) developed in the retail environment. Due to HIPAA and HITECH security and privacy rules, the adoption of RFID in the healthcare domain is subject to more specific privacy requirements that are not relevant in the retail industry.

Table 1. FIP Principles Applied to Address RFID Privacy Issues in Healthcare

FIP Principles	Application of FIP to Address RFID Privacy Issues
Notice	Patients' warnings of RFID technology use for a healthcare facility Patients' awareness of information collection and use
Choice	Patients' choices whether or not information collected for one purpose will be used for other purposes Patients' choices whether or not information will be shared with third parties unless it is required by law (i.e. claims billing)
Access	Patients' rights to access collected information Patients' rights to correct errors
Security	Protection of patients' collected information from unauthorized access during transmission and storage by: – Appropriate RFID security standards – Conducting security training for employees – Conducting RFID security audits and reviews
Enforcement	Measurement of RFID compliance to FIP principles Compliance to healthcare regulations (HIPAA/HITECH) Imposing sanctions and penalties for non-compliance

1) **Notice/Awareness.** This fundamental FIP principle would notify patients of the potential capture, use, and disclosure of their private health information. In the context of RFID technology, notifying patients of the existence of the

technology in a hospital environment is very important. Patients ought to be aware of areas and products where RFID tags are being used or under surveillance by RFID readers. Xu et al. (2009) emphasized that the notice principle prevents data collection from uninformed individuals and allows individuals to undertake necessary counter-measures for their data protection. Patients should be educated about the essence of RFID technology, its benefits, and threats to privacy in order to make an informed choice.

2) **Choice/Consent.** When applied to RFID technology in healthcare, this principle of choice/consent requires entities to receive explicit consent from the patients (Langheinrich, 2001) related to how any personal information collected may be used beyond original transaction and whether or not information collected for one purpose will be used for other purposes. The most widely used method of consent is through the mechanism of either opt-in or opt-out. With a clear notification, an opt-out regime allows patients to make appropriate choice of keeping the tag or getting rid of it.

3) **Access/Participation.** This principle provides an effective means to challenge the accuracy and quality of collected protected health information (PHI). In fact, patients should be informed of the use and disclosure of their PHI collected by RFID technology and shall be given access to that information and be able to contest the data's accuracy and completeness.

4) **Integrity/Security.** This principle dictates that covered entities and business associates should protect patients' collected information from unauthorized access. Robust security mechanisms and protocols are essential to ensure data integrity during transmission between RFID tags, readers, middleware, databases and system access to authorized entities. Eschet (2004) recommended that these measures should be audited and verified by an outside entity and the assessment becomes publicly disclosed.

5) **Enforcement/Redress**. This principle requires a set of rules along with mechanisms for detecting violations. In the US, the FTC has the authority to regulate information practices of organizations to ensure that: (a) their information policies are in line with federal regulations, and (b) their information practices are consistent with these policies (Schwaig et al., 2006). In the healthcare context, the use of RFID technology should be compliant with healthcare regulations (e.g., HIPAA and HITECH) as well as defining sanctions and penalties for non-compliance.

Technical Approaches to RFID Privacy

Many technologies were conceived expressly to be privacy-invasive technologies leaving data-trail generation and lacking anonymity. Due to increasing concerns about privacy, there has been an emergence of technologies that are expressly designed as PETs. PETs are designed to guard or promote the privacy interests of individuals (Xu, 2009). Based on existing literature, PETs for RFID applications can be divided into two categories: physical and logical solutions. The logical solutions can be further

divided into three subcategories: destruct, control and encryption approaches (See Figure 2).

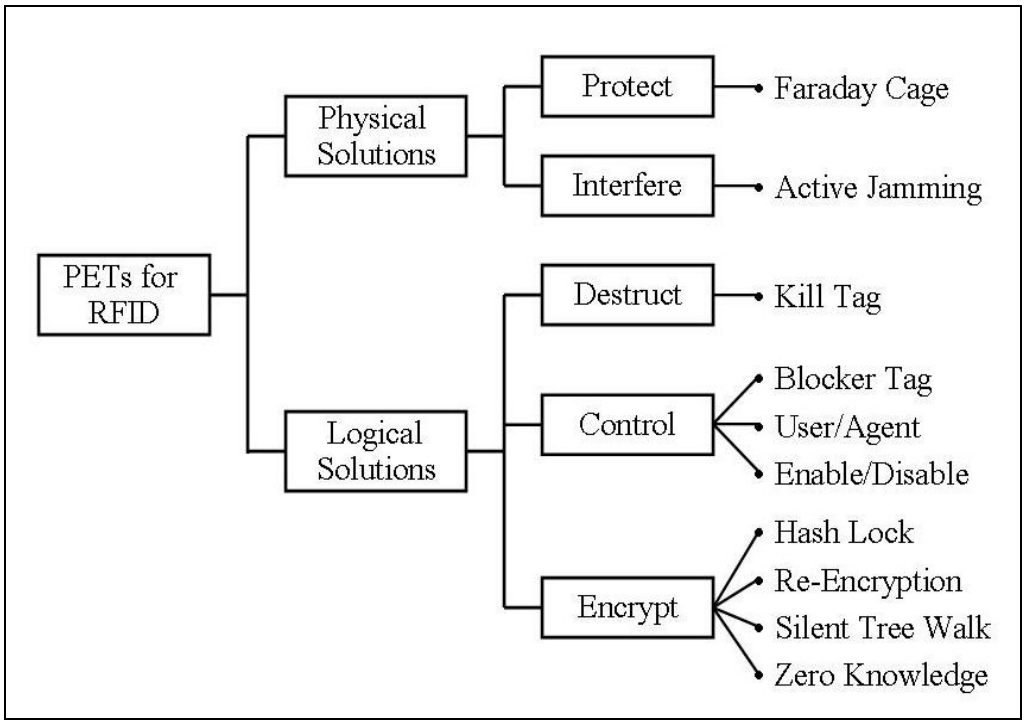

Figure 2. Taxonomy of PETs for RFID

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. 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 et al., 2003).

Logical Solutions

1) **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 is controversial since no other readers can access data from the tag. Spiekerman (2007) concurred that killing a tag's functionality curtails the future potential use of that RFID tag. In the context

of healthcare, killing the tag is infeasible as patients need to be tracked at all time during their stays at a healthcare facility.

2) **Control.** Spiekermann (2007) proposed an alternative to the kill function by enabling or disabling features in the tag. Although this model seems beneficial to both users and retailers while protecting privacy, it is unrealistic in the healthcare applications. Another control approach is the use of RSA blocker tag which is an RFID tag that responds positively to all unauthorized requests (Juels et al., 2003). This approach gives users control over the uniqueness of their IDs and associated information; however, it is application dependent and as such. Since the after-sale area does not apply to the healthcare sector, the method cannot be used in healthcare applications.

3) **Encrypt.** Encryption is the transformation of data into some unreadable form with a purpose of ensuring information privacy. A tag may be locked so that it refuses to reveal its ID until it is "unlocked" by the owner. 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., 2003a) undergo re-encryption. The drawback of this approach is the extensive infrastructure needed for re-encryption. 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.

Adherence to the Principles of FIP

Most of the PETs for RFID have been applied to the retail industry with limited application to the healthcare domain, which motivated us to review how applicable they are in the healthcare domain. The observations can be categorized into Table 2.

1) **FIP principles.** When mapping PETs to the FIP principles, Table 2 shows that most PETs are centralized around the two principles (i.e., consent and security) excluding other principles from their design. With PETs such as Faraday cage, and enable/disable (Hennig et al., 2004), consumers have the choices to conveniently disable or discard the RFID tag from the products they acquired. PETs with re-encryption or zero knowledge capabilities (Engberg et al., 2004), incorporate mainly the security principle in their design. Physical solutions as well as "destruct" and "control" approaches do not seem applicable to patients' use in healthcare because the physical shield or killing the tags defeats the purpose of tracking the patients' locations at the hospital. Allowing patients to enable/disable devices may create more reporting confusions (e.g., patient may be reported as not in facility while she had only disabled the RFID tag). Thus encrypting logical solutions for ensuring security seems more applicable to the healthcare domain.

2) **PETs and tag type.** There is a direct relationship between the types 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 the healthcare domain but so is the need for privacy. Thus the tag chosen must satisfy the demands of these positions.

3) **Apply time.** With RFID having been applied mainly in the retail industry, 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 eavesdropping. In the healthcare sector, post-purchase scenario is irrelevant. The threat comes from the possible eavesdropping while they are at the hospital facility, which makes the encryption solution more appropriate to the healthcare domain.

Table 2. Mapping of major PETs to FIP principles

		Application Domain	Notice/ Awareness	Choice / Consent	Access / Participation	Integrity / Security	Enforcement/ Redress
Faraday Cage	(Eschet, 2004; Juels et al., 2003; Kumar, 2003)	Retail				X	
Active Jamming	(Juels et al., 2003; Kumar, 2003)	Retail		X		X	
Tag Killing	(Fishkin et al., 2005; Spiekermann, 2007)	Retail				X	
Enable /Disable	(Hennig et al., 2004; Spiekermann, 2007; Spiekermann & Berthold)	Retail		X		X	
Blocker Tag	(Juels & Brainard, 2004; Juels et al., 2003)	Retail		X		X	
User/Agent PET	(Spiekermann, 2007)	Retail		X		X	
Hach-Lock	(Weis et al., 2004)	General				X	
Re-Encryption	(Juels & Pappu, 2003)	Banking				X	
Silent-Tree Walking	(Juels et al., 2003; Weis et al., 2004)	General				X	
Zero Knowledge	(Engberg et al., 2004)	Retail				X	

Regulatory Approaches

There are many different regulations and rules surrounding healthcare. HIPAA and HITECH define the federal regulatory requirements for handling patients' privacy but the state-level regulations can override these requirements (Appari et al., 2009; Meingast et al., 2006). In this section, a review of HIPAA and HITECH federal regulations is provided, followed by a discussion of their current state. Finally an FIP-Regulation table (see Table 3) is presented to map healthcare regulations to FIP principles.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPPA is an act that establishes the privacy, security and electronic transaction standards with regard to patient health information for all covered entities (HIPAA, 1996; Volonino & Robinson, 2003). HIPAA was enacted by the U.S. Congress in 1996, and became effective on July 1, 1997 with a purpose to combat waste, fraud, and abuse in health care delivery and health insurance. The intention of the HIPAA is also to improve the effectiveness and efficiency of the healthcare system, portability and continuity of health insurance coverage in the group and individual markets. HIPAA standards encompass several elements: standards code sets (for diagnoses and procedures), privacy standards (protection of individuals' health information), security standards (physical, technical, policies and procedures), unique identifiers (national provider Identification and tax ID number), insurance portability (move from one healthcare plan to another with no disruption of coverage), and fraud enforcement (HIPAA, 1996).

Table 3. FIP Principles Mapped to HIPAA and HITECH

Framework	FIP Principles				
	Notice/ Awareness	**Choice/ Consent**	**Access/ Participation**	**Integrity/ Security**	**Enforcement/ Redress**
HIPAA **Guidelines for PHI**	Individual right to be informed of the way in which their information will be shared with others, and to be informed of their right relating to privacy.	Ability to authorize or restrict disclosure of their information in certain circumstances	Individuals have right to access their medical records and to request amendments, and authorize or restrict.	Physical, technical and administrative - security rules to secure PHI.	Compliance failure results in punitive actions (fines and prison). Only a covered entity could be criminally liable.
HITECH **Expansion of the HIPAA Privacy Rule and Security Standards**	Security breach notification requirements.	Implementation of adequate consent mechanisms (Online Privacy Alliance guideline).	Access rights to electronic format Accounting of disclosures with EHRs.		Civil monetary penalties and enforcement expanded. Expanded applicability to business associates.

					Criminal penalties apply to individuals whether they are employees of the covered entity or not. Periodic audits to ensure compliance with the privacy rule and security standards.

HIPAA privacy rules pertain to health plans (e.g., insurers, managed care organizations, and federal health programs) and clearinghouses that handle data in standardized formats, as well as healthcare providers who handle claims billing, payments and remittance and eligibility information. Regardless of the transmission format, electronic or paper, covered entities have to handle PHI according to HIPAA rules. Further, HIPAA privacy rules emphasize the importance of patient privacy rights to include patient education on privacy protections, patient access to their medical records, patient consent before information disclosure, and providing recourse if privacy protections are violated. People will have the right to file a formal complaint with a covered provider or health plan, or with the United States Department of Health & Human Services (HHS), about violations of the provisions of this rule or the policies and procedures of the covered entity.

HIPAA regulations pose major challenges for the complex and evolving e-health environment (McGraw et al., 2009). The Institute of Medicine concluded that HIPAA privacy rules did not adequately safeguard the privacy and security of health records. The privacy rules rely heavily on informed consent to protect privacy. Multiple studies have demonstrated that patients do not read or understand complex privacy notices and consent forms, which are often designed to shield the institution from liability (Breese et al., 2007). McGraw et al. (2009) suggested that congress should task HHS and the FTC with jointly developing privacy and security requirements for personal health records (PHRs). Gostin and Sharyl (2009) concurred that focusing on FIP principles, patients would gain strong privacy protection.

Despite its mapping to FIP principles (See Table 3), several complaints have been filed by consumers since the enactment of HIPAA. However, very few punitive actions have been taken against covered entities. Among the criticisms of HIPAA were that the privacy and security rules did not apply to many organizations that routinely handled large amounts of health information, the potential sanctions were not sufficiently severe, and the HHS's Office of Civil Rights had never imposed a single civil penalty (Belfort, 2009).

HIPAA regulation lays out a broad set of specifications for privacy at the federal level and defines the regulatory requirements for PHI with override capabilities at the state level (Appari et al., 2009). This creates variability in state-level and federal regulations that some scholars are considering a major impediment to healthcare organizations to comply with regulations (Hodge Jr, 1999; Langenderfer & Cook, 2004).

Health Information Technology for Economic and Clinical Health Act (HITECH)

The HITECH Act, which was part of the $787 billion federal stimulus bill signed into effect by President Obama on February 17, 2009, addresses various aspects relating to the use of health information technology including providing federal funding by way of grants and incentive payments to promote health information technology implementation.

HITECH strengthens and expands HIPAA's privacy and security requirements in five key areas (HITECH, 2009):

1) **Expansion of Covered Entities**: Under HIPAA, covered entities are responsible for the actions of their third party business partners and must address situations when business associates fail to comply with their privacy obligations. The HITECH Act now directly obligates business associates to comply with the HIPAA Security Rule's administrative, physical and technical safeguard requirements, including developing and implementing comprehensive written security policies and procedures with respect to the protected PHI that they handle.
2) **Security Breach Notification Requirements**: The HITECH Act include security breach notification requirement that requires, in the event of a breach of unsecured PHI, that the covered entities to notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of such breach.
3) **New Restrictions on the Use and Disclosure of PHI**: HITECH restricts permissible uses and disclosures of PHI to include only the minimum necessary disclosures and prohibit receiving any remuneration in exchange of any PHI unless a valid authorization is obtained.
4) **New Patients Rights**: HITECH grants individuals several new rights regarding their PHI consisting of complying with patient's requested restrictions on how covered entities use and discloses his/her PHI. The HITECH Act amends HIPAA to give individuals the rights to receive an accounting of PHI disclosures made by covered entities or their business associates for treatment, payment, and healthcare operations during the previous three years to and to give individuals the rights to obtain access to their PHI in electronic format, if they request.

5) **Heightened HIPAA Enforcement**: HITECH establishes civil monetary penalty for HIPAA violations to include tiered increases based on the nature of the improper conduct and also requires formal investigation of complaints and the imposition of civil monetary penalties for violations due to willful neglect.

In relation to FIP principles (Table 3), HITECH focuses more on the enforcement/redress principle by setting higher civil and criminal penalties, which directly affects more entities, businesses and individuals in more diverse ways than ever before. While this new act is not explicit about additional security aspects, it allows patients to have access in different formats to their medical records and to have more control over who has access to their PHI as well as notifying patients of any security breaches.

ANALYSIS AND DISCUSSION

Widespread adoption of RFID technology in the healthcare industry has been hampered by the lack of adequate privacy protection from RFID technology vis-à-vis the privacy provisions and relevant healthcare regulations. According to Langheinrich (2002), technical protection alone cannot protect against privacy threats and he has suggested that the problem should be more effectively addressed with awareness and accountability.

Within the healthcare industry, HIPAA regulations can be satisfied by applying FIP principles to RFID development and deployment. Presently, RFID applications have incorporated PETs in their design and manufacture; however they have failed to adequately address all five FIP principles. While healthcare facilities can easily implement privacy awareness programs and secure patients' consents to participate in RFID usage, satisfying the dictates related to access - which would enable individuals to review their collected data in a timely, accurate, and inexpensive manner, remains a challenge.

To reinforce the importance of our study and its impact on the healthcare sector, several cases related to RFID protests in various industries were examined. Table 4 provides a summary of the reasons why people were protesting against the adoption of RFID and which FIP principles these cases failed to address. As shown in Table 4, it is evident that adopting notice, choice and access principles could have prevented most of protests.

Privacy groups continue to portrait RFID as a highly intrusive technology with adverse impact on individual privacy. The manifest causes of these protests were possible privacy violations and lack of consumers' choices, lack of notifications, and lack of access to the collected information. For example, in Ohio birthing centers, an RFID infant protection system was placed on infants at birth to prevent them from being abducted from the hospital or from being placed with the wrong mother (Corsi, 2008). Despite the fact that the system triggered an alarm and secured the hospital

entrances and exits if a newborn was removed from the ward without authorization or a baby was placed with the wrong mother, the system faced protests. The failure to create employee awareness about the system resulted in an abductor dressed in scrubs making off with an infant because "they (employees) thought the RFID system would take care of any problem". According to Corsi (2008), the failure to provide mothers with the choice of participating in the program was another reason that contributed to protestations. In Corsi's opinion, if the facility had embraced the notice and choice provisions of FIP in their implementation of the RFID system, these protests could have been prevented.

Table 4. Summary of RFID Protest Cases

When	Industry	Who/ Where	Why	Impact	References	FIP
2003	Retail	Benetton, Italy	Protest against Benetton clothing embedded with RFID chips and "Individual's behavior could be monitored to the n^{th} degree".	Publicly retreated from plans.	(Starrett, 2003)	Notice, Choice
2003	Retail	Tesco, UK	Boycott because of customers' concerns about the potential of item-level RFID tags to track consumers outside stores.	No change.	(Muncaster, 2005)	Notice, Choice, Access
2003	Retail	New Jersey Inst. of Tech., USA	Protest against RFID Tagging bullets and firearms and concern over traceability especially when bullets are maliciously swapped.	Only allow police officers to tag their guns.	(Abolins, 2003)	Notice, Choice
2003	Retail	Gillette, UK	Protests due to Gillette 'smart shelf' fitted with RFID "Tracking and photographing consumers without their knowledge and consent".	Gillette pulled RFID tags in UK amid protests.	(Boycott-Gillette, 2003)	Notice
2004	Retail	Metro AG, Germany	Stop RFID protest due to customers' concerns over	Stopped to use radio chip card.	(Black, 2004)	Notice, Choice

			hidden RFID tags in loyalty cards, shopping carts, and some other products.			
2005	Public Services	UC. Berkley Library, USA	Protests by library employees over RFID implementation taking over their jobs, and jeopardizing kids' safety with fewer staff.	Forced to organize awareness sessions.	(Berkeleyciti zen.org, 2005)	Notice
2005	Public Services	Brittan Elementar y School, USA	Parents protested their school children wearing RFID badges, for privacy concerns, as well as possible health risks.	Stop RFID test pilot program.	(Leff, 2005)	Notice, Choice, Access
2007	Healthcare	VeriChip, USA	A strong concern of the connection between implanted microchip and cancer 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	Conferenc e, USA	Protest by RFID advocates against an annual event that promotes the use of RFID in clothing and footwear.	More businesses were attending each year.	(Online Security Authority, 2008)	Choice
2008	Governme nt	Dept. of Agricultur e, USA	The Amish farmers protested the use of RFID devices on their cattle, arguing that it constitutes some form of a "mark of the beast" which is in violation of their fundamental religious beliefs.	Lawsuit dismissed by Bush administratio n as RFID are optional not mandatory.	(Kravets, 2008)	Choice
2008	Governme nt	Governm ent, UK	Protest against injection of prisoners with RFID	Denied by the Ministry of Justice.	(RFIDnews.o rg, 2008)	Choice

			tags to help "enforce home curfews".			
2008	Healthcare	Ohio, USA	Protests against Birth centers for tracking babies with electronic chips. Concern is over "an intrusive technology solution to a problem that is rare".	Claimed it has prevented baby abductions.	(Corsi, 2008)	Notice, Choice

Current protest cases appeared predominantly in the retail industry with fewer in healthcare, mainly due 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 carefully. Our conceptual framework depicts the relationships between privacy enhancing technologies and healthcare federal regulations. By strengthening the enforcement power, HITECH seems to be taking care of HIPAA's limitations. Due to the recent enactment of HITECH, its actual efficacy remains to be seen.

A summary of our proposed future directions is as follow:

Research Direction 1: *Adopt an interdisciplinary research approach.* There should be collaboration between design scientists (who develop RFID artifacts) and privacy researchers who help to improve the effectiveness and efficacy of these technologies in light of privacy principles. Doing so may require a paradigm shift incorporating FIP principles into the design, operations and management of information processing technologies and systems (Cavoukian, 2009).

Research Direction 2: *Explore a cost-benefit proposition associated with RFID PETs in healthcare.* Only a full analysis of technical functionalities (see Figure 2), costs of each option as well as operational benefits can provide healthcare administrators a complete picture of RFID effectiveness and motivate their adoption. Such cost-benefit analysis will also help to identify the high cost components, where further cost reduction or technological advances are needed.

Research Direction 3: *Explore the impact of existing regulations on the compliance of PETs.* Future research should explore how regulations are shaping the design and compliance of PETs. This leads to unavoidable examination of how the new challenges emerging with the newest technologies are impacting regulations.

Research Direction 4: *Explore the barriers to the adoption of RFID in healthcare.* Different adoption drivers determine the intentions of technology users and organizations (Huyskens & Loebbecke, 2007; Karahanna et al., 1999). Since limited RFID adoption research has been undertaken (Chen et al., 2007; Lee & Shim, 2007),

more questions remain to be answered concerning the particularity of the healthcare domain that embraces and adopts technology differently from other domains.

CONCLUSION AND OUTLOOK

The benefits of RFID technology adoption within the healthcare industry have the potential to deliver great values (Fisher & Monahan, 2008). RFID can positively impact the efficiency, accuracy and availability of information within that domain. While technical solutions have great appeal, technology is not tamper proof (Eschet, 2004; Langheinrich, 2001). The deficiencies of PETs demonstrate that the answer to the privacy concerns is not merely on technology, but acceptance and integration of a technical-regulatory perspective into the design and deployment of RFID technology must be undertaken to leverage its full potentials. Technological innovations and adoptions cannot be separated from legal realities (Langheinrich, 2001).

The contributions of this research are multifold: First, the study expanded the privacy research in the context of healthcare with regards to the newest wireless and location-based technologies (Wicks et al., 2006). RFID privacy threats resides into its capability of permanently saving and linking information about individuals through temporal and spatial extension of data collection activities (Thiesse et al., 2007), which increases vis-à-vis the complex regulation requirements of the healthcare domain. Second, the study develops a conceptual framework that considers FIP principles as a measurement for compliance to respond to the call by Thiesse et al. (2007) for an "open dialogue" with the users. The developed framework also supports Langheinrich's (2002) claim that technical protection alone cannot protect against privacy threats. Our proposed technology-regulatory framework maps technology and regulations to the five principles of FIP: notice, choice, access, security, and enforcement. This mapping exposes the failure of technological designs to integrate all FIP principles and the complexity of healthcare regulations, stressing the need for a technology-regulation interaction and collaboration. Our third contribution is on investigating RFID protest cases from other industries and revealing the shortcomings that would prevent similar protests in the healthcare domain. Finally, we believe that the development of taxonomy of PETs based on interdisciplinary literature review and analysis improves our current understanding of the functionality of PETs and their proper selection and usage.

This study has important implications for IT developers and hospital administrators who worry about privacy with the implementation of wireless and location based technologies. The taxonomy developed in this study provides IT developers with various options, which go beyond a catalog of existing PETs, to choose the most appropriate PETs and to develop awareness and training programs. For example, while "killing" or deactivating the tag is an appropriate solution in retail; such method is not viable in healthcare environment where patients need to be tracked during their hospital visits. Given the significance of consequences of non-compliance to healthcare regulations, it is recommended that IT developers and hospital administrators proceed with a mapping of their selected PETs to FIPs principle to

avoid protests and boycotts as in other industries. Table 2 cross references PETs and FIPs.

This study opens up several avenues for further research but also presents limitations that deserve consideration. Although our conceptual model is logically built upon existing literature and practical feedback from industry protest cases, the model needs further validation. Future research on validating this framework using quantitative or qualitative methods might be considered. In summary, it is our opinion that successful adoption of RFID technology in the healthcare industry is dependent upon incorporating a technical-regulatory approach centered on FIP principles. While RFID technology usage in the healthcare industry is still at its infancy, such an approach will greatly reduce the public resistance, especially with the introduction and integration of awareness, choice and access into the adoption and deployment decisions. Using the groundwork laid down in this study, future research in this field should be geared towards addressing privacy concerns expressed about RFID in the context of healthcare. It is our hope that this paper will lead to a better understanding of the underlying issues by informing both academia researchers and practitioners in the healthcare industry.

ACKNOWLEDGMENT

The authors thank Prof. Chuleeporn Changchit (Editor-in-Chief: JIPS), the associate editor and three anonymous reviewers for their constructive comments on improving this paper. Rachida Parks and Heng Xu are partially supported by the National Science Foundation for this work under Grant NSF-CNS 0716646. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

Abolins, J. (2003). RFID and firearms. Available online at: http://www.jpfo.org/alerts/alert20030907.htm.

Albrecht, K. (2007). Microchip-cancer report. Available online at: http://www.antichips.com/cancer/index.html

Appari, A., Anthony, D. L., & Johnson, M. E. (2009). HIPAA Compliance: An examination of Institutional and Market Forces. *The 8th Workshop on Economics of Information Systems (WEIS 2009).*

Avoine, G. (2006). Bibliography on security and privacy in RFID systems. Available online at http://www.avoine.net/rfid/download/bib/bibliography-rfid.pdf.

Barua, A., Mani, D., & Whinston, A. B. (2006). Assessing the Financial Impacts of RFID Technologies on the Retail and Healthcare Sectors. *Center for Research in Electronic Commerce, Department of IROM, McComb School of Business, The University of Texas at Austin.*

Becker, C. (2004a). A new game of leapfrog? RFID is rapidly changing the product-tracking process. Some say the technology--once costs drop--could displace bar-coding. *Modern healthcare, 34*(28), 38-40.

Belfort, R. (2009). HITECH raises the stakes on HIPAA compliance [Electronic Version]. Available online at: http://www.manatthealthsolutions.com/publications/articles/HITECH%20%20HIPAA%20Implications.pdf

Berkeleycitizen.org. (2005). RFID protest rally [Electronic Version]. Available online at: http://www.berkeleycitizen.org/community/rfid1.html

Bishop, L. S., Holmes, B. J., & Kelley, C. M. (2005). National consumer health privacy survey 2005. *California HealthCare Foundation*. Available online at: http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005

Black, J. (2004). Shutting shopping bags to prying eyes. Available online at: http://www.businessweek.com/technology/content/mar2004/tc2004035_8506_tc073.htm

Boycott-Gillette. (2003). CASPIAN launches worldwide Gillette boycott. Available online at: http://www.boycottgillette.com/pressrelease8-11.html

Breese, P., Rietmeijer, C., & Burman, W. (2007). Content among locally approved HIPAA authorization forms for research. *Journal of Empirical Research on Human Research Ethics*, *2*(1), 43-46.

Cavoukian, A. (2009). Privacy by design... take the challenge. *Information and Privacy Commissioner of Ontario (Canada).* http://www.ipc.on.ca/images/Resources/PrivacybyDesignBook.pdf

Chen, C. C., Wu, J., & Crandall, R. E. (2007). Obstacles to the adoption of radio frequency identification technology in the emergency rooms of hospitals. *International Journal of Electronic Healthcare, 3*(2), 193-207.

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

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

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Contemporary Perspectives on Privacy: Social, Psychological, Political, 59*(2), 323-342.

Davis, S. (2004). Tagging along. RFID helps hospitals track assets and people. *Health facilities management, 17*(12), 20-24.

Engberg, S. J., Harning, M. B., & Jensen, C. D. (2004). Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience. Paper presented at the *Second Annual Conference on Privacy, Security, and Trust.*

Eschet, G. (2004). FIPs and PETs for RFID: Protecting privacy in the web of radio frequency identification. *Jurimetrics,* 45, 301- 323

Fisher, J. A., & Monahan, T. (2008). Tracking the social dimensions of RFID systems in hospitals. *International journal of medical informatics*, *77*(3), 176-183.

Fishkin, K. P., Roy, S., & Jiang, B. (2005). Some methods for privacy in RFID communication. *Proceedings of 1st European Workshop on Security in Ad-Hoc and Sensor Networks, Springer*, 42-53.

Gostin, L. O., & Sharyl, N. (2009). Reforming the HIPAA privacy rule: Safeguarding privacy and promoting research. *Journal of the American Medical Association (JAMA), 301*(13),1373-1375.

Hennig, J. E., Ladkin, P. B., & Sieker, B. (2004). Privacy enhancing technology concepts for RFID technology scrutinised. *Research Report, RVS-RR-04-02, University of Bielefeld, Germany*.

HEW. (1973). Fair Information Practices. U.S. Dept. of Health, Education and Welfare. http://www.privacyrights.org/ar/fairinfo.htm

HIPAA. (1996). Health Insurance Portability Accountability Act (HIPAA). Available online at: *http://www.hipaa.org/*.

HITECH. (2009). Health Information Technology for Economic and Clinical Health Act (HITECH). Available online at: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf*.

Hodge Jr, J. G. (1999). Intersection of federal health information privacy and state administrative law: The protection of individual health data and workers' compensation, The. *Administrative Law Review, 51(1)*, 117-144.

Huyskens, C., & Loebbecke, C. (2007). RFID adoption: theoretical concepts and their practical application in fashion. *International Federation For Information Processing-Publications-IFIP, 235*, 345- 361.

Jossi, F. (2004). Electronic follow-up: bar coding and RFID both lead to significant goals--efficiency and safety. *Healthcare informatics: the business magazine for information and communication systems, 21*(11), 31-33.

Juban, R. L., & 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 Communications, 24*(2), 381-394.

Juels, A., & Brainard, J. (2004). Soft blocking: Flexible blocker tags on the cheap. Paper presented at the *Proceedings of the 2004 ACM workshop on Privacy in the Electronic Society*, Washington DC, USA.

Juels, A., & Pappu, R. (2003). Squealing Euros: privacy protection in RFID-enabled banknotes. *Financial Cryptography, Springer Berlin / Heidelberg, 2742*, 103-121.

Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. Paper presented at the *Proceedings of the 10th ACM conference on Computer and Communications Security*, Washington D.C., USA.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 23(2), 183-213.

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

Kumar, R. (2003). Interaction of RFID technology and public policy. *Wipro White Paper*. Available online at: http://www.rfidconsultation.eu/docs/ficheiros/Wipro_Interaction_RFID_Technology_Public_Policy.pdf

Langenderfer, J., & Cook, D. L. (2004). Oh, what a tangled web we weave the state of privacy protection in the information economy and recommendations for governance. *Journal of Business Research, 57*(7), 734-747.

Langheinrich, M. (2001). Privacy by design-principles of privacy-aware ubiquitous systems. *Ubicomp 2001: Ubiquitous Computing,* Lecture notes in computer science *2201*, 273-291.

Langheinrich, M. (2002). A privacy awareness system for ubiquitous computing environments. *UbiComp 2002: Ubiquitous Computing,* Lecture notes in computer science *2498*, 315-320.

Lee, C. P., & Shim, J. P. (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. [Electronic Version]. Available online at: from http://www.msnbc.msn.com/id/6942751

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 5-12.

McGraw, D., Dempsey, J. X., Harris, L., & Goldman, J. (2009). Privacy as an enabler, not an impediment: building trust into health information exchange. *Health Affairs, 28*(2), 416-427.

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with health care information technology. *Proceedings of 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, NY, 5453–5458.

Milne, G. R., & Culnan, M. J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US Web surveys. *The Information Society, 18*(5), 345-359.

Mowry, M. (2008). A survey of RFID in the medical industry. Available online at: http://www.winmec.ucla.edu/rfid/course/2008s/Final_project_Mike_Mowry.pdf.

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

Neil, R. (2005). On a roll. RFID moves toward patient safety. *Materials Management in Health Care, 14*(3), 20-23.

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

Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics, 59*(4), 327-345.

Privacyrights.org. (2003). RFID position statement of consumer privacy and civil liberties organizations. Available online at: http://www.privacyrights.org/ar/RFIDposition.htm

RFIDnews.org. (2008). Prisoners may be RFID-chipped in the UK. Available online at: http://www.rfidnews.org/2008/01/13/prisoners-may-be-rfid-chipped-in-the-uk

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management, 43*(7), 805-820.

Spiekermann, S. (2007). Privacy enhancing technologies for RFID in retail-an empirical investigation. *UbiComp 2007: Ubiquitous Computing, Springer Berlin / Heidelberg, 4717*, 56-72.

Spiekermann, S., & 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*, 137–146.

Starrett, M. (2003). I'd rather go naked [Electronic Version]. Available online at: http://newswithviews.com/Mary/starrett4.htm

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*, Keystone, Colorado, Paper 223.

Volonino, L., & Robinson, S. R. (2003). *Principles and practice of information security*: Prentice.

Wang, S. W., Chen, W. H., Ong, C. S., Liu, L., & Chuang, Y. W. (2006). RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, Kauai, Hawaii, vol 8, 184a.

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. *Security in Pervasive Computing 2802*, 50-59.

Westin, A. F. (1967). *Privacy and Freedom*, Atheneum: New York.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453.

Wicks, A. M., Visich, J. K., & Li, S. (2006). Radio frequency identification applications in hospital environments. *Hospital topics, 84*(3), 3-9.

Xu, H. (2009). Consumer responses to the introduction of privacy protection measures: an exploratory research framework. *International Journal of E-Business Research, 5*(2), 21-47.

Xu, H., Bagby, W. J., & Melonas, R. T. (2009). Regulating privacy in wireless advertising messaging: FIPP compliance by policy vs. by design. *Proceedings of 9th Privacy Enhancing Technologies Symposium* (PETS 2009), Seattle, Washington, 19-36.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems, 26*(3), 137-176.

Young, D. (2004). FDA embraces RFID to protect drug supply. *American journal of health-system pharmacy, 61*(24), 2612-2612.