Journal of Business Ethics (2005) 59: 327–345
DOI 10.1007/s10551-005-2928-8

An Ethical Exploration of Privacy and Radio Frequency Identification

Alan R. Peslak

ABSTRACT. This manuscript reviews the background of Radio Frequency Identification (RFID) as well as the ethical foundations of individual privacy. This includes a historical perspective on personal privacy, a review of the United States Constitutional privacy interpretations, the United Nations Declaration of Human Rights, European Union Regulations, as well as the positions of industry and advocacy groups. A brief review of the information technology ethics literature is also included. The RFID privacy concerns are three-fold: pre-sales activities, sales transaction activities, and post-sales uses. A proposal to address these privacy concerns is detailed, generally based on past philosophical frameworks and specifically on the Fair Information Practices that the Federal Trade Commission has outlined for the electronic marketplace (e-commerce). It is proposed that by application of these Fair Information Practices, the major privacy issues of RFID can be addressed.

KEY WORDS: Agency theory, deontological, electronic commerce, ethical framework, fair information practices, information technology ethics, privacy, radio frequency identification, RFID, teleological

Purpose of the study

Radio frequency identification (RFID) is a technology that allows every manufactured item in the world to be uniquely identified. Essentially, it is an inexpensive passive electronic device that allows for the transmission of a distinctive signal from any product or artifact in which it is embedded or attached. This technology represents unique challenges of privacy as well as monetary and security benefits. This manuscript reviews privacy and the issues associated with RFID including historical perspectives, deontological and teleological issues, and agency theory as it relates to retail privacy. The paper continues with a methodology to address the overall privacy issues of RFID through the application of category and solution frameworks. The category framework is based on privacy classes of DeGeorge (2003). The solution framework proposed is based on philosophical foundations, literature review, and the Fair Information Practices of the Federal Trade Commission (1998, 2000). These practices have previously been recommended for online privacy and electronic commerce. Through this process, a proposal to address RFID issues is recommended.

Alan R. Peslak is an Assistant Professor of Information Sciences and Technology at Penn State University, Worthington Scranton. He received his Ph.D. in Information Systems from Nova Southeastern University, Fort Lauderdale, Florida. He has over 25 years of industry experience. Dr. Peslak's research focuses on the economic, ethical and societal impacts of information technology. He has published in the Information Resources Management Journal, Journal of Computer Information Systems, Information Research, *and* First Monday. *He is a member of ACM, AITP-EDSIG, Financial Executives Institute, IACIS, and ACM-SIGMIS.*

Background of RFID

RFID Technology

RFID has been heralded as a major new technology that will revolutionize supply chain management. According to AIM, The Association for Automatic Identification and Data Capture Technologies, the use of RFID automates the process of collecting product and transaction data (AIM, Inc., 2003c). The actual concept uses three separate components – an antenna, an RFID tag (programmed transponder with unique information), and a transceiver (a reader to receive and decode the signal) (AIM, Inc, 2003b). The

reader or transceiver is usually the source of power and generates a low power radio signal broadcast through an antenna when in use. The RFID tag receives the signal through its own internal antenna and powers a computer chip. The chip will then exchange information with the reader (AIM, Inc., 2003c). These are known as passive tags and are the least expensive and most common. They also only have read capability. In addition, there are active tags which are self-powered, more expensive, and have read/write capability. There are differences in the frequency ranges that RFID tags use. Low frequency tags (30–500 Khz) are used for most inventory type applications whereas high frequency tags (850–950 MHz and 2.4–2.5 GHz) have longer read ranges and higher reading speeds and are used in mobile reading applications such as toll collection (AIM, Inc, 2003d). In all cases, the tag contains specific information that can be used to uniquely identify the item.

The concept of RFID is seen by many to be a step in the direction of ubiquitous computing. Ubiquitous computing presents an environment in which electronic devices are embedded and used in all our manufactured objects and are prevalent in all activities in our lives. It also can usher in an era of proactive computing where systems anticipate and satisfy user needs through ubiquitous devices (Want, 2004). Some of the major characteristics of RFID include

- Tags can take a variety of shapes and sizes.
- Tags can be a fraction of an inch to several inches in length, width and depth.
- Read range can be several inches up to more than 100 feet based on powering of reader and/or chip.
- RFID require no contact or line of sight such as needed with bar codes.
- Active (powered) tags can have a life of up to 10 years.
- Passive (non-powered) tags have a virtually unlimited life.

(AIM, Inc., 2003b)

Uses of RFID

There are also many possible uses of RFID. The initial and still most mentioned use is for inventory management and improved supply chain activities. But many other uses have been both implemented and proposed such as automatic toll collection, ID cards, anti-theft devices (Want, 2004, ''RFID Usage and Trends'', 2003), records management (Faber, 2002), payment systems, counterfeit prevention, product identification for recall purposes (Weiss, 2003), vehicle identification, building security, and library systems (AIM, Inc., 2003b). It has even been suggested that all cattle could be identified and tracked using RFID, thus containing a situation such as the mad cow scare which surfaced in the latter part of 2003 (Sullivan, 2004).

The popular press has noted many cases of privacy concerns related to the use or potential abuse of RFID systems. Wal-Mart and Gillette were planning a test of RFID tags in a Boston location. The test would have involved the use of RFID tags in Gillette products and allowed recording of the tags of the individual razors and other consumer items. The test was called off, however, in July of 2003 prior to its implementation. Spokespersons for Wal-Mart and Gillette denied consumer or privacy activist pressure affected their decision, commenting only that the cancellation reflected a change in strategy to focus on wholesale distribution centers first. Wal-Mart reemphasized its commitment to RFID over the long term by having its top 100 suppliers include tags on pallets and cases by 2005. Gillette, likewise, continues to test RFID in its packing centers. Another retailer who planned to include RFID tags in its clothing was Benetton. This concept inspired an Internet encouraged boycott causing Benetton to retreat from its immediate plans to use the technology. One retailer who is actively using RFID is Prada, which reads tags in their clothes and displays accessories or other information about the clothes when someone tries them on in their display-equipped dressing rooms (Cox, 2003b).

According to Garfinkel (2002), the Massachusetts Turnpike Authority is giving discounts to residents who pay using EZ-Pass, a transponder system relying on radio tags. He suggests this is ''discriminatory and coercive''. It had even been reported that RFID tags are being considered for currency. According to the Economist, the European Central Banks was looking at placing tags into the Euro by 2005, ostensibly to prevent counterfeiting (The Economist, 2002). Although this is no longer being considered in

Europe, the privacy implications would have been significant. In this application, deactivation would not have been possible.

RFID is already being used to track and coordinate movements of people between the U.S. and Canada. A program called NEXUS allows U.S. and Canadian citizens to register their fingerprints, photo, and other personal data and, if approved, receive a card with an RFID tag. When individuals wish to travel between the U.S. and Canada, they display their cards near the inspection booth. An RFID reader identifies the cards and retrieves relevant information about the individuals from their computer. An inspector matches the pictures on their screen to the occupants of the vehicle and if all appears correct, they are cleared though inspection in less than five seconds. This is clearly an example of individuals relinquishing privacy for convenience – in this case, a rapid border crossing (AIM. Inc., 2003a).

The growth of RFID over the next several years is expected to be significant. Some aspects of the technology and the market were noted in ComputerWorld recently (Brandel, 2003). RFID is forecasted to grow to a $3 billion market within 5 years. Wal-Mart estimates savings of 10–20% in labor costs at their distribution centers through RFID. Cost of passive RFID tags is estimated to decrease to five cents by 2006. But even in this report there are hints of privacy concerns.

The current popular press contains many articles noting the rapid rush to implementation of RFID in both wholesale and retail applications. Waters (2004) suggests the use of RFID is the largest change in inventory tracking since the move to bar codes by Wrigley in 1974. She notes the primary usages are suggested to be inventory control, reduction of shrinkage, and elimination of stock-outs. Wal-Mart is noted as the major mover to RFID, but Target and Best Buy also have announced plans to require RFID. In addition, European retailers Metro and Marks and Spencer are moving to RFID. The RFID Gazette (''The Future is Here'', 2004) reports that the U.S. Department of Defense is requiring suppliers to have RFID implemented in 2005. A troubling concern with RFID tags is that the tags are not foolproof. Technical difficulties have been reported with RFID including tag collisions, tag failure, and tag detuning. (Floerkemeier and Lampe, 2004)

Privacy review

Privacy classes

This new technology has raised privacy concerns by many. In examining the privacy impact of RFID tags, it is helpful to review privacy rights origins and history in our society. First, though, in order to address and analyze threats to personal privacy it is desirable to categorize personal privacy. DeGeorge (2003) suggests six different classes of personal privacy which can be categorized as privacy classes.

- Space – physical space such as home, desk, locker etc.
- Body/mental – free speech, no self-incrimination.
- Personal information – information about yourself
- Communication privacy – interchange between individuals such as phone or email.
- Personal privacy – right to be left alone, freedom to do what we want on our own time.
- Cyber privacy – free speech in the electronic world.

US privacy rights

The defined right to privacy in the U.S. traces its roots to Warren and Brandeis in 1890, defining the right to privacy as the ''right to be left alone'' (Warren and Brandeis, 1890). The U.S. constitutional supports for this premise are the first and fourth amendment protecting the right to free speech (and by extension thought) and the right to unreasonable search and seizure. Tort law also supports some aspects of privacy including protection from intrusion on a person's private affairs, disclosure of embarrassing facts, slander, and using an aspect of a person's identity for profit (Schoeman, 1992). Westin (1967) suggests information privacy is a concept that involves ''when, how, and to what extent'' private individual information may be used. Glenn (2003) discusses the three origins that have given rise to the right to privacy: philosophical, constitutional, and common law. These philosophical foundations include Locke who believed

government was necessary to protect natural rights of humans. Those rights were life, liberty, and property. The rights of man were preeminent in this context; government was to serve man. From this privacy has been extended as a natural right.

U.S. Constitutional foundations support four main privacy concepts:

- individualism or the preeminence of the individual versus the state,
- popular consent or power of government comes from the people governed,
- limited government,
- private property.

The first 10 amendments to the U.S. Constitution specifically list rights of U.S. citizens. Amendments suggested to relate to privacy include

First – right to free speech and thought (allows privacy of thought).
Third – right to not have troops quartered in private homes in peacetime, (addresses right of privacy in the home).
Fourth – right to not be subject to unreasonable search and seizure (solidifies rights to privacy in the home).
Ninth – the declaration that there are other possible rights that people retain which certified that rights not specifically enumerated in the amendments did not preclude their existence. (Glenn, 2003)

The ninth amendment allowed for the extension of the first, third, and fourth amendments to be interpreted to be a broader overall right of individual privacy. The final relevant amendment is the fourteenth which requires due process for the deprivation of life, liberty, or property. In these provisions, the U.S. Constitution specifically addresses space and body/mental privacy.

Common law support for privacy includes space and body/mental case law support, but also incorporates communication and personal privacy including

- Inviolability of the home.
- Inviolability of the person.
- Sanctity of Confidential Communications.
- Sacredness of Personal Information.

Glenn notes significant common law case history to support these claims (Glenn, 2003).

U.N. declaration of human rights

The United Nations codified the fundamental human right of privacy in 1948 within their Universal Declaration of Human Rights. Concepts of human privacy are included in several articles of the declaration. A listing of the articles and the related applicable privacy classes is shown in Table I.

Related ethical literature review

The concept of ethics and privacy in an electronic world has been studied by a variety of researchers. One of the early theoretical constructs dealing with ethics in the information age was prepared by Mason (1986). In his discussion piece, he suggests four major ethical issues known by the acronym PAPA, namely privacy, accuracy, property, and accessibility. Privacy concerns, according to Mason, include the large amounts of personal data that businesses and marketers are gathering and storing. Accuracy includes the problem and responsibility of keeping information collected, correct and authentic. He also alludes to the need for remedies if this information integrity is not upheld. Property deals with the concept of ownership of private data and information as well as channels of distribution such as airwaves. Accessibility addresses the issue of individual rights to their own data as well as security for protecting these data.

Stead and Gilbert (2001) discuss ethical issues that are raised by electronic commerce. The primary areas of focus are privacy and security. The privacy concerns of electronic commerce include collection of information without user's knowledge, sales of collected personal information, and receipt of unsolicited information, as in spamming. Security requires the protection of any information collected by organizations in electronic commerce transactions. Many of these same issues apply in relation to the use of RFID.

Technology is evolving rapidly and the ability of ethical theory development to deal with new issues raised by technology has not kept pace (Ogburn's cultural lag theory). Marshall (1999) proposes a general definition of ethics as ''guidelines to influence

TABLE I

U.N. declaration of rights related to privacy

UN article	Privacy Class
Article 12 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks	Space privacy and Communication privacy
Article 3 Everyone has the right to life, liberty and security of person	Personal privacy and Body privacy
Article 9 No one shall be subjected to arbitrary arrest, detention or exile	Body privacy
Article 13 (1) Everyone has the right to freedom of movement and residence within the borders of each state (2) Everyone has the right to leave any country, including his own, and to return to his country	Personal privacy
Article 18 Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance	Body/Mental privacy
Article 19 Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers	Mental privacy, Cyber privacy
Article 20 (1) Everyone has the right to freedom of peaceful assembly and association (2) No one may be compelled to belong to an association	Cyber privacy, personal privacy
Article 29 (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society	General concept of no more laws than necessary for general welfare

(United Nations General Assembly, 1948)

human social behavior in a manner intended to protect and fulfill the rights of individuals in a society''. Technology is defined as an application of science to modify some aspect of the world. There are significant differences between the development of technology and the ethical structure which needs to deal with the effect technology is having on society. Technology develops in a competitive environment. Technology also deals with specific natural laws which can be directly controlled in experiments. The ethics to support these changes do not develop in a controlled environment and need to

deal with secondary impacts on human social structures. Results cannot be directly derived from experiments. In addition, there is little economic incentive to support the ethical study of technological impacts. A cultural lag exists as technology is developed, experimented with, and introduced without study of ethical impacts. Most of these studies occur after the introduction of technologies. In addition, this cultural lag may be widening due to the increasing rate of technological development. Ethical policy related to privacy and electronic commerce is an area that has not been sufficiently developed. (Marshall, 1999)

The U.S., according to Sarathy and Robertson (2003), has maintained a more self-regulatory approach to dealing with technological ethical issues such as electronic commerce and ''digital privacy''. In Europe, stronger legal and regulatory methods have been employed such as Regulation 45/2001. In addition, a model for developing ethical and privacy protection strategies has been proposed. This model starts with a review of precursors, including national culture and global societal trends. Then, external factors including legislation and importance and sensitivity of data are reviewed. This approach has different philosophical backgrounds from which to draw an overall ethical framework, including rule based utilitarianism, act based utilitarianism, egoism, moral relativism, and justice.

The major ethical challenges of electronic commerce, including intellectual property rights, accounting abnormalities, and privacy issues raised by collection of personal information by electronic commerce (EC) firms, are noted by Maury and Kleiner (2002). There are three ways proposed to ''address the concerns'' related to electronic commerce ethics – legislation, litigation, and self-regulation. According to their study, legislation is rigid and ineffective; litigation is expensive and unworkable; but self-regulation is desirable and is recognized by the industry to be necessary.

The concept of self-regulation appears less likely when other research is reviewed. A survey of marketing executives was performed by Bush et al. (2000) to determine their perceptions of ethics related to electronic commerce. The study reviewed perceptions on regulation, ethical Internet marketing issues, ethics and the Internet in their organizations, and the need for codes of Internet ethics. The results were somewhat disturbing. Over 55% of the executives were concerned that the lack of regulation has ''resulted in frequent ethical abuses by organizations''. About 46% of the industry respondents agreed to some degree that the ''Internet be regulated to insure ethical marketing''. This is from individuals within the industry itself, suggesting a strong indictment against current self-regulation. A need for a code of Internet marketing ethics was recommended by 82% of respondents. The major issues facing the marketers were noted to be security, illegal activity, and privacy, all major issues with consumer perceptions of e-commerce as well as RFID. Overall, the marketers recognized significant ethical issues in electronic commerce that were not being addressed.

McArthur (2001) presents a contrary view based on the concept of privacy expectations in electronic and Internet usage. Though privacy is recognized and supported, he suggests two instances where privacy expectations should be reduced. The two situations are the ''Mischance Principle'' and the ''Voluntary Principle''. According to the Mischance Principle we should have low expectations of privacy when we are in public or choose to forego reasonable measures of privacy. In the Voluntary Principle we voluntarily give information, thus we should expect less privacy. He concludes with a discussion of two key Internet examples, surfing and e-mail. He suggests that the Internet has no inherent methodology for hiding identity; therefore privacy expectations should be lowered. Likewise email is suggested to be inherently insecure with many companies and organizations having monitoring in place. Use of the technology represents a negative voluntary principle. We voluntarily choose to use a system that is not inherently private.

Privacy as a deontological versus teleological ethical concept

Much research in recent years has focused on the study of the deontological versus teleological nature of business ethics. General business ethics research has been mixed as to the importance of deontological factors versus teleological factors. Bowen (2004) defines deontology as a ''non-consequentialist paradigm of moral philosophy in which decisions are made based on moral worth as defined by duty.'' Actions

are inherently good or bad; the consequences do not matter. According to Cole et al. (2000) the ''basic difference between deontological and teleological evaluations centers on whether the actor focuses on the action to be taken or the consequences of that action.'' Teleology is grounded in consequences or the results of an action. A general consensus has not been reached as to the relative importance of deontological versus teleological factors with regard to business ethics (Akaah, 1997; Singhapakdi et al., 1996; Vitell and Hunt, 1990). As an example, Vitell and Hunt (1990) analyze both deontological and teleological factors in marketing decision making and find in their study that marketing decision makers are influenced by both deontological and teleological factors when making their marketing decisions. The concept of privacy has come under review as to its position on this ethical continuum. Introna and Pouloudi (1999) note the general acceptance of privacy as an important concern but suggest that there can be many different ''perspectives'' of privacy and ''that privacy is a relational and relative concept.'' Previously, privacy has been regarded from primarily a deontological perspective, viewing privacy as an inherent right and rule-based. But in the era of terrorism, this inherent right has been eroded by the security needs of society. Consequences have projected privacy into the teleological realm. Strict rights of privacy have been abridged to protect the larger goal of public safety.

Even though privacy has been eroded to some extent by security concerns, privacy of information has remained strong and even gained ground in some areas in recent years. One primary example is the enactment of HIPAA regulations. After years of total lack of regulation, Congress enacted comprehensive legislation to assure privacy of medical information in the U.S. In this case, self-regulation was insufficient to protect the privacy rights of individuals and was addressed through legislation. ''The Congress included provisions to address the need for standards for electronic transactions and other administrative simplification issues in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which was enacted on August 21, 1996.'' (Department of Health and Human Services, 2000) The Administrative Simplification Requirements of HIPAA consist of four parts

(1) Electronic transactions and code sets.
(2) Security.
(3) Unique identifiers.
(4) Privacy (Department of Health and Human Services, n.d.).

This issue of the deontological versus teleological implications of privacy was studied by Alder (1998) who examined the issue of electronic performance monitoring in the workplace. After discussing the two conflicting philosophical positions of privacy, he suggests that there is and will be no agreement among philosophers in the near term on the proper position of privacy. As a result, he suggests an approach that does not focus on whether electronic monitoring is inherently ethical but on developing rules that allow for ethical use of the technology. Ultimately, the development of rules and policies to control and enforce privacy rights generally recognized by society is the most practical approach to any privacy issues including RFID.

RFID privacy issues

Limited study has been performed specifically on RFID ethics and privacy issues. Weiss (2003) presents background on RFID technologies and the debate associated with their use. He sees the issue as being a battle between privacy and corporate efficiency. Generally, he notes that the privacy advocates do not object to the concept of using RFID tags to track inventory in warehouses; the most significant concern is when the product reaches the consumer. At present, the tags remain in a working condition after the items to which they are attached are purchased. The tags could subsequently be read when they encounter an RFID transceiver. Thus, if you were to walk into a store with an RFID tagged item, an active transceiver could activate a signal from the tag and through a series of steps identify you, your location, and any other information about you such as criminal history, shopping records, or credit history. Discrimination or unfair treatment as a result of this information is possible. Privacy advocates are advocating either a stop to RFID tags entirely or a deactivation or ''kill'' switch for RFID tags once items enter the retail realm. They recommend that the ''kill'' be automatic rather than

requiring a specific request or opt-out by the consumer. A kill switch would prevent subsequent readings from the tag after sale. RFID advocates counter that these privacy fears are unfounded. The costs of a national or worldwide tracking system to monitor RFID tags to individuals would be cost prohibitive and uneconomic. In either case, the implications of privacy and RFID should be studied prior to its widespread deployment.

Popular reports suggest that RFID concerns range from "big brotherism" to corporate rapacity. There is a major consumer advocacy group named Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) which began as a group opposed to supermarket identification cards. The group has now expanded its concerns into other areas such as RFID. The group exposed a planned public relations campaign by an RFID industry group (Auto-ID) that was planned to "denigrate privacy concerns about RFID tags" (Cox, 2003a).

The position statement of CASPIAN includes the following items:

- Threats to Privacy and Civil Liberties of RFID.
- Framework of RFID rights and responsibilities.
- RFID practices that should be flatly prohibited.
- Acceptable uses of RFID.

Their position statement is supported by other major groups, including the American Civil Liberties Union (ACLU) and is jointly issued by CASPIAN and the organizations such as Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) and Privacy Rights Clearinghouse. The position statement was also endorsed by a long list of information policy bodies and individuals.

There are significant ethical issues included in this position statement including:

- Tags are hidden and unknown to shoppers and purchasers.
- Tags provide an identification of every item purchased, thus allowing a universal product registration system.
- Tags allow the potential for aggregation of massive amounts of personal data based on purchases and ownership, making personal profiling possible.
- Embedded tags (such as in clothing or currency) can be read by active readers and can allow tracking of individuals.

The position statement does address the legitimate cost savings and safety possibilities inherent in RFID tags recommending acceptable uses such as:

- Tracking items with toxic substances (without unique ID).
- Tracking manufactured products through the supply chain (suggested to be part of packaging and disposable or not included in consumer sale).
- Tracking pharmaceuticals to point of sale to ensure proper handling through the supply chain.

(CASPIAN, 2003–2004)

The threat to personal privacy with RFID includes other instances of privacy concerns. Swartz (2003) suggests some of the potential problems with personal information, particularly in the era of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (commonly known as the U.S.A. Patriot Act). Forty-five percent of companies have supplied customer, employee, or supplier data to the government. The use of RFID can potentially provide a plethora of new information about individuals if not properly safeguarded.

An alternative to dealing with RFID could be the blocker tag. Juels et al. (2003) propose a device that can block the active readers of RFID tags from reading tags. A "kill tag" approach which would render RFID tags inoperable prior to consumer purchase is deemed not practical. They report that it disallows many possible positive uses such as suggesting accessories to a dress or allowing automatic cooking instructions for food products purchased. There are also proposed to be benefits to consumers that would be disallowed by deactivation such as physical security control (theft), retail returns, or exceeding of expiration date for foods. Another approach is an on–off switch that could allow benefits if the consumer wishes but could but eliminated for those who do not want to use the benefits. This study proposes there are technical and

cost challenges that cannot be overcome given the low cost that RFID tags need to retain. A low cost alternative called a blocker tag is recommended. When affixed to or wrapped around the item it can disrupt RFID tag readers but when discarded the RFID tag and its benefits can be reactivated. The blockers may not be possible, however, with uses such as RFID currency and airline tickets where continuous activation is integral to its intended purpose. There is also a technical concern with spillover effects on other close proximity tags. Although blockers initially appear to be a viable solution to privacy versus use concerns, ultimately the exceptions noted result in questionable overall viability.

Industry position

According to an industry group, AIM (The Association for Automatic Identification and Data Capture Technologies), RFID tags present no more of a threat to privacy than ''cell phones, toll tags, credit cards, ATM machines, and access control badges'' (AIM, 2003c). They do not describe any personal privacy issues with RFID. The Code of Conduct of AIM is focused only on marketing. The beginning of this Code suggests their objective:

> ''To support the healthy growth and expansion of the RFID industry by creating credibility in the marketplace.'' (AIM. Inc., 2003b)

Toward this objective they pledge:

> ''We, as manufacturers and suppliers of RFID technology, agree that we have a responsibility to our industry to communicate accurate information concerning RFID products and technology including:
>
> - Accurate information concerning the availability of RFID technology and products.
> - Realistic performance and price comparisons with other technologies.
> - Accurate and provable performance information concerning existing RFID products.
> - Advertising and marketing of existing and future products that created realistic customer expectations for such products.'' (AIM. Inc., 2003b)

The Code of Conduct of the AIM industry group does not address privacy. Their code includes only those four tenets.

They conclude with this statement:

> ''We understand the importance of providing accurate and honest information concerning our products and future products and to fulfill the purpose of expanding the RFID industry.'' (AIM. Inc., 2003b)

There is no mention of personal privacy.

RFID privacy category framework

If RFID tags are used in retail environments they allow significant opportunities for obtaining private information. These opportunities can occur prior to, during, and after the sale.

In a retail environment, there are three situations where privacy concerns surface. First, in a pre-sale situation an item is tagged on a shelf and is examined by a customer. The store could, through readers, monitor what items are being examined. An example of a privacy concern could be monitoring of the books that are being examined in a retail book establishment. Profiling and monitoring could be used to track individuals and their choice of reading material. An extreme example could be the monitoring of reading choices among particular ethnic groups during a period of heightened national security alert. Another situation could be the monitoring of clothing items that an individual might model. This could be a considered a violation of personal privacy. Both of these situations could arise as an unintended byproduct of the use of RFID systems to try to increase sales. As noted, Prada already uses RFID systems in dressing rooms to suggest accessories. The information is already collected. More privacy-violating applications are possible. This would be a violation of Body/Mental privacy in the DeGeorge framework.

Though the possibilities for pre-sales privacy violations are a concern, other negative possibilities can occur both during and after the sale. When the sales transaction takes place, the store can permanently store all personal information about you and associate it with the specific item. Personal information would

TABLE II

RFID privacy category framework

Scenario	Privacy Issues	Personal Privacy Class
Pre-sale	Monitoring of items being examined	Body/Mental Privacy
	Tracking of items being modeled	
During sale	Permanent record of item purchased	Personal Information Privacy
	Coordination of current item purchased with other past purchases	Communications Privacy
	Sales and item transaction information shared with internal or external entities	Cyber Privacy
	Sales and item transaction information shared with government or taxing bodies	
Post-sale	Physical tracking of personal items purchased anywhere, anytime	Space Privacy
	Reading of tags in external environments allowing for "custom marketing"	Personal Privacy
	Tracking of personal movement via RFID tag readers	Cyber Privacy

come from credit cards, frequent purchase cards or even telephone numbers, which are often requested and recorded prior to a purchase. This could be combined with information obtained via the RFID tag. Only cash transactions with no other exchange of information can prevent this from happening. Some retail establishments, however, are now requiring some form of personal identification. I was told recently at a large national retail electronics store that I could not make my cash purchase without giving my phone number. Once this information is entered, it can be used for many purposes including sharing with internal departments for marketing activities, sharing with government bodies for security or tax purposes, or selling to third parties for any purpose. There is also the potential for personal profiling based on past purchases. Classes of privacy affected here include Personal Information, Communications, and Cyber privacies.

Perhaps the most insidious of RFID uses is the potential for post-sales monitoring. Technically, all RFID tags can be permanently read through active readers. Items can be tracked and monitored through active readers. Invasive custom marketing activities could be developed in retail establishments through active reading of items possessed with RFID tags; furthermore, personal individual movements could be tracked through their possession of items with RFID tags. These privacy issues fall under the Space, Personal and Cyber privacy categories. All these scenarios and issues are summarized in Table II.

Fair information practices of the US Federal Trade Commission (FTC)

As noted, there has already been significant debate on the merits of RFID. This manuscript proposes that the use of RFID should adhere to the Fair Information Practices that the FTC has proposed for electronic commerce. The detailed approach to the enforcement of privacy for online transactions can be used as a model for RFID tag use, specifically as it applies to consumers.

The U.S. Federal Trade Commission in the late 1990s began a series of steps to address the issue of privacy online particularly with respect to electronic commerce. In 1995, they began with a series of public workshops which reviewed privacy concerns related to Internet firms and electronic commerce. The work continued in 1996 with an initial report; in-depth consumer workshops were held in 1997. The government, up until this time, had primarily relied on industry self-regulation to safeguard electronic customers' privacy information. In 1998, they surveyed 1400 online Internet firms to specifically determine the effectiveness of industry self-regulation. Their initial study suggested that industry self-regulation was not effective and basic concepts of privacy were not being followed in the electronic marketplace. Specifically, 92% of the sample firms were collecting significant amounts of privacy information, with only 14% disclosing anything about their privacy practices (Federal Trade Commission, 1998).

In 1999, after a second survey conducted by Mary Culnan of Georgetown, which confirmed the unfavorable status of Internet privacy (Culnan, 1999), the FTC issued a statement on "Self-Regulation and Privacy Online" that called for continued reliance on industry self-regulation, but asked industry to step up privacy efforts (Federal Trade Commission, 1999). Finally, in 2000, the FTC conducted a second survey of a random sample of web sites, as well as another sample of the Internet's most popular sites. The study confirmed that while most sites continued to collect large amounts of personal information from individuals, there was improvement in the disclosing of privacy practices. Despite the fact that improvements were made, however, the FTC concluded that self-regulation was insufficient and recommended federal legislation to "ensure adequate protection of consumer privacy online". (Federal Trade Commission, 2000).

The FTC in both its 1998 and 2000 reports identified four "widely-accepted" Fair Information Practices with which Internet firms would be required to comply. In addition, the Commission (Federal Trade Commission) added a fifth practice in both the 1998 and 2000 report.

The five Fair Information Practices necessary to protect online privacy were

- Notice – informing the online customer that personal information is collected.
- Choice – allowing consumers option of how personal information is used.
- Access – offering consumers ability to see their collected information.
- Security – protecting the collected information.
- Enforcement – providing penalties for non-compliance with other practices.

According to the Federal Trade Commission, these are the core principles of an online privacy policy. These concepts support and are consistent with European and U.S. privacy protection history. They also support the U.N. Declarations on the right to privacy. Some of the specifics that online companies should include in their practices were also detailed in the May 2000 report. These particulars are shown in Table III. These practices also are supported by researchers such as Mason (1986) whose PAPA principles have been incorporated into the FTC framework (see Table III). Shaw (2003) used the FTC fair information practices as guidelines for privacy protection in his privacy literature review and noted the inclusion of the five principles in OECD guidelines, European Union's Data Protection Directive, and other international guidelines.

RFID solution framework and fair information practices

A proposal for dealing with RFID is to extend the Fair Information Practices promulgated by the FTC for electronic commerce to RFID use, in order to create an RFID solution framework. It has been established that privacy is a fundamental human right. This right has been codified in the United Nations Declaration approved by all UN members. The threats to personal privacy are real and significant. The framework proposed by the FTC to deal with privacy online is a comprehensive, reasonable approach to addressing electronic privacy concerns. There can be a direct mapping of the FTC Fair Information Practices to provide a practical solution to RFID privacy concerns. Table IV presents a summary of the Fair Information Practices (FIP) and a recommendation of how they can be adapted to address personal privacy concerns of RFID creating an RFID privacy solution framework.

Table IV proposes that specific implementation of the FIP can provide adequate protection from RFID abuses. The pre-sales issues of monitoring of items being examined and tracking of items being modeled would be addressed by proper notice in the store. The clear posting of the use and monitoring of RFID tags would at least alert customers to the practice and would allow customers to choose not to patronize the establishment. Preferably, the store could also choose not to monitor via the tags and this could be posted prominently.

The multiple issues that could arise at the time of the sale are addressed by all five fair information practices. The keeping of a permanent record of item purchased, coordination of current item purchased with other past purchases, sales and item transaction information shared with internal or external entities, and sales and item transaction

TABLE III

FTC fair information practices and specific steps

FTC Fair Information Practice	Specific steps to address Fair Information Practice	Mason Framework
Notice	Clear and conspicuous listing of privacy policy	Privacy
	Detail of type of information collected	Property
	Detail of how information collected	
	Specifics of how information used	
	Explanation of how Choice, Access, and Security is provided	
	Whether and what information is disclosed to third parties	
	Whether other organizations are involved in collecting information	
Choice	Selection of how personal information is used beyond original transaction	Privacy
	Choice on how information is used by the original company	Property
	Choice on how information is used by other parties	
Access	Allow consumers to view their personal information	Accessibility
	Allow consumers to correct errors in their personal information	Accuracy
	Allow consumers to delete personal information	
Security	Adopt appropriate security standards for personal information including:	Accessibility
	Conduct risk assessment	
	Establish security system	
	Manage security policies and procedures	
	Conduct security training for employees	
	Conduct security audits	
	Conduct internal reviews	
	Reassess security risks	
Enforcement	Measurement of compliance	Accuracy
	Imposing sanctions for non-compliance	
	Use of third party privacy seals to assure enforcement	
	Or face legislative remedies for enforcement	

(Federal Trade Commission, 2000)

information shared with government or taxing bodies must be addressed first by Notice. Either a printed tag would be provided detailing specifics, or the printed tag would detail that none of these were done. Choice would allow a customer to choose not to participate in the record keeping, and the information would not be retained. If the customer chose to participate, that decision could be changed in the future through Access where mistakes could be corrected or personal information deleted. Security of information would protect against unapproved usage and Enforcement would assure compliance.

All post sales tracking and privacy issues can be directly addressed through the Fair Information Practice of Choice, where a person could choose to deactivate the RFID tag. If the individual were to opt to keep the tag, this decision could be changed at a future date based on the fair information practice of Access.

European Union on data privacy

Europe has long had stringent regulations on data privacy. Data protection was the focus of "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." In its conclusion, The European Union Directive 95/46/EC notes that its reason for implementation is "the achievement of an Internal Market (in this case the

TABLE IV

Solution framework to address RFID privacy issues

Fair Information Practice	Application of Fair Information Practice to RFID Privacy Issue	Sceanrio
Notice	Clear and conspicuous posting of the use of RFID tags in a retail establishment to warn customers of potential monitoring activities	Pre-sale During Sale
	Clear and conspicuous tagging of all RFID items – link to website and/or paper copy listing following items: For each participant in the distribution chain for RFID enabled products: Detail of type of information collected Detail of how information collected Specifics of how information used Explanation of how Choice, Access, and Security is provided Whether and what information is disclosed to third parties Whether others are involved in collecting information and listing of those Or a Notice that no information is collected or used	
Choice	Selection of how RFID related personal information is used beyond original transaction	During sale
	Choice on how RFID related information is used by the original company	Post-sale
	Choice on how RFID related information used by other parties All can and should be possible both during sale – via RFID kill switch at time of sale or post-sale via web or mail	
Access	Allow consumers to view their RFID related personal information	Post-sale
	Allow consumers to correct errors in their personal information Allow consumers to delete personal information All should be able to be done via web or mail including deletion of RFID item from the company database	
Security	Adopt appropriate RFID security standards for personal information including:	Pre-sale
	Conduct risk assessment of use of RFID	During sale
	Establish RFID and related security system	Post-sale
	Manage RFID security policies and procedures Conduct RFID security training for employees Conduct RFID security audits Conduct RFID internal reviews Reassess RFID security risks Security system should be independently reviewed through third party or government.	
Enforcement	Measurement of compliance to RFID privacy and security policies	Pre-sale
	Imposing sanctions for non-compliance	During sale
	Use of third party privacy seals to assure enforcement	Post-sale
	Or face legislative remedies for enforcement Enforcement of RFID practices should be real and practical and involves substantial penalties.	

(Based on Federal Trade Commission, 1998, 2000 Fair Information Practices)

free movement of personal information) and the protection of fundamental rights and freedoms of individuals.'' (Commission of the European Communities, 2003)

Included in the Directive are provisions similar to the U.S. FIP including

- Accuracy,
- Retention,
- Access,
- Right to Object,
- Confidentiality,
- Security,
- Explicit purpose of collection,
- Consent,
- Remedy – ''provide for the right of every person to a judicial remedy for any breach''.

Exemptions are noted in the directive and include:

- National security,
- Defence,
- Public security,
- Crimes or professional ethics breaches,
- Monitoring regulatory functions,
- Subject to rights and freedoms of others.

('Directive 95/46/EC', 1995)

A recent European Union regulation specifically regulates data privacy. The European Union's ''REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data'' provides strong regulations on the collection and use of personal data. The Constitution of the European Union explicitly provides for privacy of personal data. Article 3 section 3 states: ''Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.'' (The Europe, 2002) Within this statement are the five Fair Information Practices of the U.S. FTC. There is implicit and/or explicit Notice, Choice, Access, Security, and Enforcement.

The Treaty of the European Union and the Charter of Fundamental Rights of the European Union contain specific privacy provisions. Article 8 of the Treaty of the European Union states:

''Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'' (European Communities, 2004b). Article 8 of the Charter of Fundamental Rights of the European Union states:

''Protection of personal data:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the

TABLE V
Status of 95/46 Implementation

Country	95/46 directive implementation status
Austria	Entry in force year 2000
Belgium	Entry in force 2001
Denmark	Entry in force 2000
Finland	Entry in force 2000
France	Draft discussed
Germany	Adopted 2001
Greece	Entry in force 1997
Ireland	Enacted April 2003
Italy	Entry in force 2004
Luxembourg	Entry in force 2002
The Netherlands	Entry in force 2001
Portugal	Entry in force 1998
Spain	Entry in force 2000
Sweden	Entry in force 1998
United Kingdom	Entry in force 2000

(European Communities, 2004a)

person concerned or some other legitimate basis lay down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.'' ('Charter of Fundamental Rights', 2000)

The European Commission has taken its privacy position very seriously, to the point of litigation against non-complying members. ''The European Commission has decided to take France, Luxembourg, the Netherlands, Germany and Ireland to court for failure to notify all the measures necessary to implement the directive on the protection of personal data. This step represents the third formal stage of formal infringement proceedings under Article 226 of the EC Treaty.'' (European Communities, 2000) The implementation of the 95/46 European directive has been growing among European Community members. Table V shows each country and their implementation status. Only France has not adopted as of 2004.

Agency theory issues

Agency theory has as its basis a relationship between an actor and agent who has obligations to another actor or principal through an economic relationship. The assumptions related to agency theory include perfect market relationship, voluntary free will among the participants, and equal power among participants (Shankman, 1999).

Through an agency model, the market could possibly determine whether RFID will be accepted by consumers. However, the privacy concerns related to RFID are not being communicated to consumers, and large retail giants are moving forward with RFID without mentioning the privacy implications of the technology. In addition, the current retail marketplace does not reflect a true agency relationship. Consumers are not being informed of all the privacy issues associated with information collected via the Internet and are not being informed of the implications of RFID. With the impending widespread use of RFID for supply chain, consumers will have limited or no information to choose goods without RFID tags. Voluntary choice is negated on the part of the principals. Clearly, individuals have less power than multi-billion retail giants, and thus equal power among agency participants is negated. Finally, with the size and purchasing power of Wal-Mart and others, a perfect market relationship does not exist among retail players. Other retail participants do not have equal access to manufacturer supply and pricing.

The difficulty in monitoring activity in a principal–agent relationship is commonly referred to as the principal–agent problem (Sappington, 1991). Principals and agents tend to act in their own self-interest and consumer principals cannot assure the compliance with the wishes of the corporate agents. Retail stores act as agents for consumers, but retail agents also have economic relationships to their shareholders. The potential for conflicting interests provides a dilemma with agency theory in a non-perfect competitive economic model. The agent–principal relationship has not been honored in electronic commerce activities. RFID usage should result in similar non-compliance with principals' wishes and privacy.

The protection of consumer privacy resulting from the use of RFID tags represents a classic example of the principal–agent problem. The principal–agent problem results when a principal requires an agent to perform work for him, but cannot observe the agent's activity. Consumers buy merchandise from retailers but are not privy to the information collected, what is done with it, or how the information is retained. With an RFID tag, the potential for information collection without the knowledge of the principal starts before the sale, is active through the sale, and potentially can be active after a sale. All of these can take place without the principal/consumer knowledge or acceptance. In a situation such as this, market forces cannot be relied on to assure consumer privacy.

Summary and limitations

Previous research proposes a ''stimulation of an informed debate on the nature and extent of privacy regulation.'' (Cook, 2004). This work has attempted to study the fundamental issue of privacy as well as

the privacy implications of radio frequency identification tags. Although not a complete review, the study does present a detailed background and major research dealing with both privacy and RFID. Four major areas are identified and explored. Further research is clearly encouraged in each area.

First, the foundations and support for privacy rights are reviewed. Privacy as a right traces its roots back to Locke and ''natural rights''. Both the U.S. Constitution and the Bill of Rights contain specific provisions establishing the right to privacy. The U.N. Declaration of Human Rights contains numerous articles recognizing various privacy concepts and classes. But, as noted, debate exists on the interpretation of these rights both from a deontological versus teleological perspective as well as the actual implementation of privacy practices. Although privacy rights are recognized, these rights must be specifically detailed for practical enforcement. Further study is recommended to explore the philosophical roots and justification of privacy rights. This could provide a more comprehensive framework for addressing specific privacy issues and their enforcement through legislative and other means.

The specific issue of Internet and electronic commerce privacy is yet another fertile avenue for research. The ability to collect, store and retrieve vast amount of private data on individuals has surpassed the current self-regulatory capabilities of government, industry, and other organizational participants. Agency theory is not sufficient to control privacy in the electronic world because there is not equal power among the participants. Individuals do not come to these relationships with power equal to large electronic commerce or corporate participants. As a result, various nations have implemented legislation or recommendations to deal with the specific issue of Internet privacy. These acts range from the detailed European Initiatives to the Fair Information Practice guidelines of the FTC. Both the 95/46 European Directive and the U.S. FTC fair information practices have attempted to address the major privacy protection issues associated with electronic commerce, but there has been limited success with these guidelines. Both acts do cover the major ethical issues of electronic commerce but enforcement has been limited. The European Directive has been implemented in many countries but penalties for non-compliance have been lacking. The FTC guidelines remain self-regulating and have not proven to be particularly effective. After over a decade of electronic commerce, only 16% of the U.S. Fortune 50 companies have incorporated all five of the FTC fair information practice principles (Peslak, 2005). More comprehensive legislation appears to be necessary. This issue of enforcement deserves further study.

Third, there are many unique privacy ethics issues which have been specifically identified with relation to RFID. These issues center on three general scenarios of pre-sales, during sales, and post-sales. The monitoring, data collection and retention issues associated with these three areas can potentially violate all the personal privacy classes based on the DeGeorge (2003) framework, namely space, body/mental, personal information, communication, personal privacy and cyber privacy. Further development and empirical study of the ethical conflicts should be pursued.

Finally, there is a detailed proposal to use the Federal Trade Commission Fair Information Practices to deal with each of the RFID privacy scenarios. Notice would require warnings within establishments and on items that RFID tags are in use. Choice would allow deactivation of RFID tags during or after sales take place. Access would require viewing, correcting, or deleting information collected by organizations via RFID tags. Comprehensive Security measures would be taken to safeguard any personal information obtained and/or retained by RFID users. Finally, Enforcement would be external and allow for review of all RFID privacy practices. Through the proper implementation of these provisions, the pre-sales, during sales, and post-sales ethical issues identified with RFID can be managed. Technologists at the first summit on RFID by the U.K. National Consumer Council suggested, ''If you're going to stay within the law, the law needs to change. What needs to underpin the law is fair practice and RFID has got to be guided by privacy, trust and law. Real principles must guide us.'' (Lace, 2004) Hopefully, this article can provide a foundation for the development of ethical and legal frameworks to deal with the challenge of privacy issues resulting from RFID usage.

Acknowledgements

I wish to thank the anonymous reviewers and editor who patiently assisted on this manuscript and helped mold it into a significant research contribution.

References

Alder, G.: 1998, 'Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives', *Journal of Business Ethics* **17**, 729–743.

AIM, Inc.: 2003a, 'NEXUS: Life in the Fast Lane' URL: http://www.aimglobal.org/technologies/rfid/casestudynexus-intermec.htm

AIM, Inc.: 2003b, 'Radio Frequency IDentification Code of Conduct', URL: http://www.aimglobal.org/technologies/rfid/code_of_conduct.htm

AIM, Inc.: 2003c, 'RFID FAQs, not Fiction', URL: http://www.aimglobal.org/technologies/rfid/rfid_faqs.asp

AIM, Inc.: 2003d, 'What is Radio Frequency Identification (RFID)?', URL: http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp

Akaah, I.: 1997, 'Influence of Deontological and Teleological Factors on Research Ethics Evaluations', *Journal of Business Research* **39**, 71–80.

Bowen, S.: 2004, 'Organizational Factors Encouraging Ethical Decision Making: An Exploration into the Case of an Exemplar', *Journal of Business Ethics* **54**(4), 311–324.

Brandel, M.: 2003, 'Smart tags, high costs', *Computerworld* **37**(50), 39.

Bush, V., B. Venable and A. Bush: 2000, 'Ethics and Marketing on the Internet: Practitioners' Perceptions of Societal, Industry and Company Concerns', *Journal of Business Ethics* **23**, 237–248.

CASPIAN: 2003–2004, 'Position Statement on the Use of RFID on Consumer Products', URL: http://www.spychips.com/jointrfid_position_paper.htm

'Charter of Fundamental Rights of the European Union' (2000), *Official Journal of the European Communities*. URL: http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/c_364/c_36420001218en00010022.pdf

Cole, D., M. Sirgy and M. Bird: 2000, 'How Do Managers Make Teleological Evaluations in Ethical Dilemmas? Testing Part of and Extending the Hunt-Vitell Model', *Journal of Business Ethics* **26**(3), 259–269.

Commission of the European Communities: 2003, '265 Final Report From The Commission, First report on the implementation of the Data Protection Directive (95/46/EC)' URL: http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf

Cox, J.: 2003a, 'Battling over RFID ...or is it over spy tags?', *NetworkWorldFusion,* URL: http://www.nwfusion.com/weblogs/wireless/003085.html

Cox, J.: 2003b, 'Wal-Mart shelves RFID test plan', *NetworkWorldFusion,* URL: http://www.nwfusion.com/news/2003/0714walmart.html

Culnan, M.: 1999, 'Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission', URL: http://www.msb.edu/faculty/culnanm/gipps/gipps1.pdf

DeGeorge, R.: 2003, *The Ethics of Information Technology and Business* (Blackwell Publishing, Malden, MA).

Department of Health and Human Services: 2000, 'Health Insurance Reform: Standards for Electronic Transactions', URL: http://aspe.hhs.gov/admnsimp/final/txfin00.htm

Department of Health and Human Services: n.d., 'Provider Hipaa Readiness Checklist – Getting Started' URL: http://cms.hhs.gov/hipaa/hipaa2/readiness-chklst.pdf

'Directive 95/46/EC of the European Parliament and of the Council, Official Journal of the European communities on the protection of individuals with regard to the processing of personal data and on the free movement of such data': 1995*, Official Journal of the European Communities* URL: http://europa.eu.int/comm/internal_market/privacy/docs/95–46-ce/dir1995-46_part1_en.pdf

European Communities: 2000, 'Data protection: Commission takes five Member States to court', URL: http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/00/10&format=HTMLaged=1&language=EN&guiLanguage=en

European Communities: 2004a, 'Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data', URL: http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm

European Communities: 2004b, 'Treaty on the European Union', URL: http://europa.eu.int/comm/internal_market/privacy/law/treaty_en.htm

Faber, M.: 2002, 'RFID: The Next Tool for Managing Records', *The Information Management Journal* **36**(6), 60–63.

Federal Trade Commission: 1998, 'Privacy Online: A Report to Congress', URL: http://www.Federal Trade Commission.gov/reports/privacy3/priv-23a.pdf

Federal Trade Commission: 1999, 'Prepared Statement of the Federal Trade Commission on ''Self-Regulation and Privacy Online', URL: http://www3.Federal

Trade Commission.gov/os/1999/07/privacy onlinetestimony.pdf
Federal Trade Commission: 2000, 'Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress', URL: http://www.Federal Trade Commission.gov/reports/privacy2000/privacy 2000.pdf
Floerkemeier, C. and M. Lampe: 2004, 'Issues with RFID usage in ubiquitous computing applications', URL: http://www.vs.inf.ethz.ch/publ/papers/RFIDIssues.pdf
Garfinkel, S.: 2002, 'An RFID Bill of Rights', *Technology Review* **105**(8), 35.
Glenn, R.: 2003, *The Right to Privacy: Rights and Liberties under the Law* (ABC-CLIO, Santa Barbara, CA).
Introna, L. and A. Pouloudi: 1999, 'Privacy in the Information Age', *Journal of Business Ethics* **22**, 27–38.
Juels, A., R. Rivest and M. Szydlo: 2003, 'The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy', *Proceedings of the 10th ACM Conference on Computer and Communication Security, October 2003, Washington, DC, U.S.A.*, pp. 103–111.
Lace, S.: 2004, 'Calling in the Chips? Findings From The First Summit Exploring The Future Of RFID Technology In Retail Seminar', National Consumer Council, URL: http://www.ncc.org.uk/technology/calling_in_chips.pdf
Langenderfer, J. and D. Cook: 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**, 734–747.
Marshall, K.: 1999, 'Has Technology Introduced New Ethical Problems?' *Journal of Business Ethics* **19**, 81–90.
Mason, R.: 1986, 'Four Ethical Issues of the Information Age', *MIS Quarterly* **10**(1), 5–12.
Maury, M. and D. Kleiner: 2002, 'E-Commerce, Ethical Commerce?' *Journal of Business Ethics* **36**, 21–31.
McArthur, R.: 2001, 'Reasonable Expectations of Privacy', *Ethics and Information Technology* **3**, 123–128.
Peslak, A.: 2005, 'Internet Privacy Policies: A Review and Survey of the Fortune 50', *Information Resources Management Journal* **18**(1), 29–41.
'REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data', : 2000, *Official Journal of the European Communities,* URL: http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_008/l_00820010112en00010022.pdf
'RFID Usage and Trends': 2003, *E-Marketer*, URL: http://www.emarketer.com/Report.aspx?rfid_jul04
Sappington, D.: 1991, 'Incentives in Principal Agent Relationships', *Journal of Economic Perspectives* **3**(2), 45–66.
Sarathy, R. and C. Robertson: 2003, 'Strategic and Ethical Considerations in Managing Digital Privacy', *Journal of Business Ethics* **46**, 111–126.
'SAS Announces RFID Capabilities': 2004, *RFID Gazette*, URL: http://www.rfidgazette.org/2004/07/sas_announces_r.html
Schoeman, F.: 1992, *Privacy and Social Freedom* (Cambridge University Press, Cambridge).
Shankman, N.: 1999, 'Reframing the Debate Between Agency and Stakeholder Theories of the Firm', *Journal of Business Ethics* **19**(4), 319–334.
Shaw, T.: 2003, 'The Moral Intensity of Privacy: An Empirical Study of Webmasters' Attitudes', *Journal of Business Ethics* **46**, 301–318.
Singhapakdi, A., S. Vitell and K. Kraft: 1996, 'Moral Intensity and Ethical Decision-Making of Marketing Professionals', *Journal of Business Research* **38**, 245–255.
Stead, B. and J. Gilbert: 2001, 'Ethical Issues in Electronic Commerce', *Journal of Business Ethics* **34**, 75–85.
Sullivan, L.: 2004, 'RFID Technology Could be Used to Build a National Livestock-tracking System', *Information mWeek*, January 12, 2004. URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=17300330
Swartz, N.: 2003, 'Compromising Customers' Privacy', *Information Management Journal* **37**(4), 17+.
The Economist: 2002, 'Science and Technology: Where's the Smart Money', **362**(8259), 81+.
'The Europe We Need: Constitution of the European Union': 2002, URL: http://www.theepc.be/PDF/Basictreaty.pdf
'The Future Is Here: A Beginner's Guide to RFID': 2004, *RFID Gazette*, URL: http://www.rfidgazette.org/2004/06/rfid_101.html
United Nations General Assembly: 1948, 'Universal Declaration of Human Rights', URL:: http://www.un.org/Overview/rights.html
Vitell, S. and S. Hunt: 1990 'The General Theory of Marketing Ethics: A Partial Test of the Model', *Research in Marketing* **10**, 237–265.
Want, R.: 2004, 'RFID: A Key to Automating Everything', *Scientific American* **290**(1), 56.
Warren S. and L. Brandeis: 1890, 'The Right to Privacy', Originally published in *Harvard Law Review* **4**(5). URL: http://www.louisville.edu/library/law/brandies/privacy.html
Waters, J.: 2004, 'More tech in store: Wal-Mart's muscle is advancing RFID usage', URL: http://cbs.marketwatch.

com/news/story.asp?guid=%7BA9969BF0-C580-4286-A396-B5ADDEA298DA%7D&siteid=google&dist=google

Weiss, A.: 2003, 'Me and My Shadow', *netWorker* **7**(3), 25–30.

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

Information Sciences and Technology,
Penn State University,
120 Ridge View Drive,
Dunmore, PA 18512, U.S.A.
E-mail: arp14@psu.edu