Interaction of RFID Technology And Public Policy

Paper presentation at RFID Privacy Workshop @ MIT, Massachusetts.

Author: Rakesh Kumar
rakesh_kumar@iitiim.com

Wipro Technologies
India

Table of Contents

"The right to be left alone -- the most comprehensive of rights, and the right most valued by a free people."
- Justice Louis Brandeis, Olmstead v. U.S. (1928).

1) Science Fiction, No More……..

It is science fiction no more; tiny transponders embedded in everything, starting from innocuous 'cola can' to a package of razor blades to a shirt label can be used to track your shopping habits, your consumption patterns and eventually you.

Recently in news, there had been major controversies regarding usage of RFID (Radio Frequency Identification) by retail giant such as Benetton. Consumers, privacy advocacy groups like CASPIAN (Consumers against Supermarket Privacy Invasion and Numbering) have mounted a media campaign against technology that captures consumer data which includes loyalty cards and RFID.

Lack of privacy, concern for public health (electronic smog), unemployment, 24 hour tracking and ultimately loosing freedom…. are these the only issues playing in mind of consumers, privacy advocacy groups and the Governments all over the world, or is there something more than meets the eye? The paper would address these questions by referring to some of the existing findings and research reports.

The main focus of this paper would look into what goes into developing a comprehensive public policy that balances marketers' information needs and consumers' concerns regarding privacy. The paper **would not** dwell on other issues relating to RFID such as concerns on health and safety, allocation of radio wave spectrum and rise of unemployment.

The paper would also give understanding of the current scenario with respect to personal data security and how current laws may impact the ability of future efforts to frame a comprehensive public policy on usage of RFID internationally.

The paper would try to throw some light on few existing policies which are meant to alleviate privacy concerns and finally, what would be the most probable successes factors which will make a new comprehensive public policy on RFID acceptable by consumers. It will endeavor to provide alternatives to the privacy problem raised by consumers and their counterparts and suggest optimal solution(s) to the imbroglio all the players are caught in.

2) First, getting understanding of RFID

Radio Frequency Identification (RFID) is a type of automatic identification system. The purpose of an RFID system is to enable data to be transmitted by a portable device, called a tag, which is read by an RFID reader and processed according to the needs of a particular

application. The data transmitted by the tag may provide identification or location information or specifics about the product tagged, such as price, color, date of purchase, etc.

The use of RFID in tracking applications first appeared during the 1980s even though RFID was developed by allied forces in WWII so radar operators could distinguish between friendly and enemy aircraft.

For those with technical bent of mind, a basic RFID system consists of three components:

1. An antenna or coil
2. A transceiver (with decoder)
3. A transponder (RF tag) electronically programmed with unique information

The antenna emits radio signals to activate the tag and read and write data to it. Antennas are the conduits between the tag and the transceiver, which controls the system's data acquisition and communication.

When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer for processing. The diagram below depicts basic features of RFID.

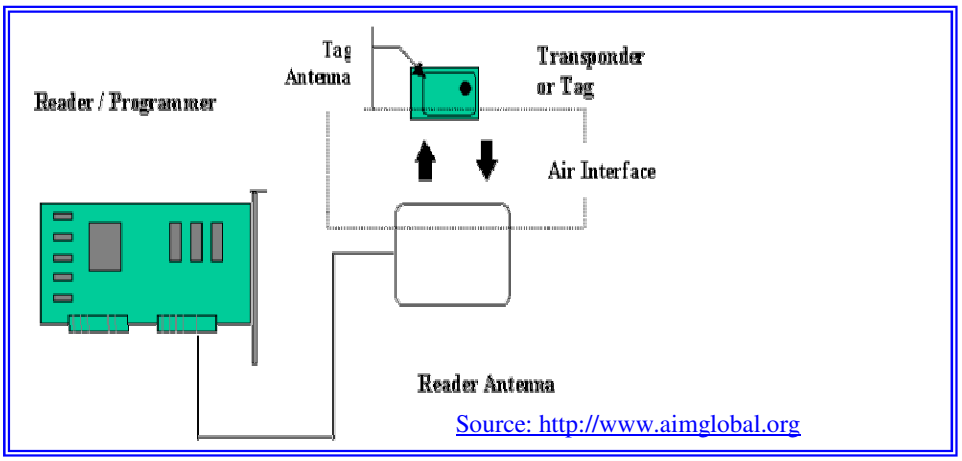

Fig: RFID System Components

2.1) RFID, its application areas

For years, RFID potential for dramatic supply-chain improvements has been clear. The great promise of RFID is to offer more *granular, accurate information* on product availability and to automate processes that are performed manually today.

Potential applications for RFID may be identified in virtually every sector of industry, commerce and services where data is to be collected. Principal areas of application for RFID that can be currently identified include:

1. Transportation and logistics
2. Manufacturing and Processing
3. Security

A range of applications may also be distinguished, some of which are steadily growing in terms of application numbers. They include:

1. Animal tagging
2. Waste management
3. Time and attendance
4. Postal tracking
5. Airline baggage reconciliation
6. Road toll management

As standards emerge, technology develops still further, and costs reduce considerable growth in terms of application numbers and new areas of application may be expected.
Some of the more prominent specific applications include:

1. Electronic article surveillance - clothing retail outlets being typical.
2. Protection of valuable equipment against theft, unauthorized removal or asset management.
3. Controlled access to vehicles, parking areas and fuel facilities - depot facilities being typical.
4. Automated toll collection for roads and bridges - since the 1980s, electronic Road-Pricing (ERP) systems have been used in Singapore.
5. Controlled access of personnel to secure or hazardous locations.
6. Time and attendance - to replace conventional "slot card" time keeping systems.
7. Animal husbandry - for identification in support of individualized feeding programmes.
8. Automatic identification of tools in numerically controlled machines - to facilitate condition monitoring of tools, for use in managing tool usage and minimizing waste due to excessive machine tool wear.
9. Identification of product variants and process control in flexible manufacture systems.
10. Electronic monitoring of offenders at home
11. Vehicle anti-theft systems and car immobilizer

2.2) Suitability of RFID

A number of factors influence the suitability of RFID for given applications. The application needs must be carefully determined and examined with respect to the attributes that RFID and other data collection technologies can offer. Where RFID is identified as a contender further considerations have to be made in respect of application environment, from an electromagnetic standpoint, standards, and legislation concerning use of frequencies and power levels.

The most valuable benefits of item-level RFID such as tamper prevention for prescription drugs and the reduction of smuggling rings that distribute stolen goods throughout the developing world are one of the neglected areas which has to be dwelt upon to bring true benefits of RFID technology.

3) Case Studies

CPG manufacturers and retailers, after one of the biggest apparel retailer (Benetton) fiasco, have started addressing privacy concerns by adhering to best practices like outlining uses of RFID data and providing consumers with *opt-in and opt-out* choices.

Benetton put its item-level rollout on hold because it had not adequately addressed consumer privacy concerns. The U.S.-based *'Consumers Against Supermarket Privacy Invasion and Numbering',* **CASPIAN** called for a worldwide boycott of Benetton until the company renounced its involvement with RFID. Benetton later announced it was simply evaluating the use of RFID tags in its inventory management system and was making the announcement because of concern in the financial markets regarding the cost of technology and its benefits.

In another instance under consumer's pressure for privacy intrusion, Tesco had ended a controversial field trial of a merchandizing-tracking system. The Tesco chain stopped using a high tech shelf that it was testing in a Cambridge store. The shelf was designed to monitor stock and detect theft of Gillette razors, which are commonly stolen, by recording images of shoppers who removed razors from the shelf.

Also, Wal-Mart canceled a trial of a so-called smart shelf system. The idea was to test how the chips, embedded in products from Gillette, could monitor inventory levels and deter theft. The company has decided to focus instead on developing RFID systems in its distribution centers and warehouses to cut costs.

4) What privacy exactly means in the context of RFID?

Common fears

The issue of privacy had been in past and faced widespread resistance just as in 1974 with the advent of the barcode. Consumerists got laws passed in eight states that prevented about $85,000 per store in cost savings (due to required unit price tagging) which meant in those states consumers paid more for their groceries. The movement was funded by the labor unions. According to industry experts, barcodes have served their purpose well and also served their time and now its time to take over by RFID.

The common fears which were shared by the consumerists and the employees while deploying barcodes still exist but the priority has changed. Then the paramount concern with barcodes implementation was rise in unemployment but now with RFID it has changed to lack of privacy.

According to privacy advocates, marketers and retailers can develop detailed profiles of their customers, based on their own records of transactions with an individual as well as on that individual's transactions with other institutions with help of RFID. Even when these data bases contain only transactional data, such as name, address, and product or service used or inquired about, they serve as the basic source for development of detailed profiles by interconnecting each other, now very easily with help from ubiquitous RFID.

RFID tags can be attached without knowledge of consumer and this is major concern for privacy advocacy groups. According to them, consumer privacy is enhanced when consumers are aware of information practices and are given a choice over information provision and use. In contrast, consumer privacy is decreased when there is unwanted marketing contact or information gathering without consent

As a result, according to privacy advocates, the potential for widespread dissemination, misuse, unauthorized access, and disclosure of personal information about consumers would increase exponentially and create a new source of privacy concerns for the public.

4.1) Big Brother cometh……

The applicability of RFID in retail sector at item level is slowed not because of lack of technical know-how but because of consumers and their counterparts' backlash concerning prospective misuse of RFID. According to privacy advocates, an unauthorized third party with easy access of RFID scanner could get item level data and information about consumer consumption pattern along with consumer's profile which might help the third party to track down the consumer.

The detailed data about the consumer and his/her purchasing habits, compiled by marketer, may fall in unwanted elements if they decide to sell them for a profit say to interested parties, from insurance providers, and mortgage lenders, to government agencies

and anyone with a credit card. Also there are chances that the data collected by authorized parties (data vendors, data exchanges etc.) may fall in hands of rogue elements if the security and access system, for such a database and data exchange, is not up to the standards.

According to privacy advocates, the information-rich governments would have perfect hegemony over the citizen's actions and thoughts once RFID systems are set in without proper care taken for public privacy. They cite *'The Patriot Act II'* the law in which authorities would have power and provisions for profiling based on the tracking of purchases. RFID just makes it easier to invade consumer's privacy that way.

Comment: The legislation, would broadly expand the government's surveillance and detention powers. Among other measures, it calls for Extend authorization periods for secret wiretaps and Internet surveillance

4.2) Cradle-to-Grave Surveillance

One of the common fears faced by shoppers and consumers is what happens when they leave the retail store? In a world of always-on marketing, some fear that these tags will become ubiquitous. If the tiny chips keep active -- and they can do that because they carry no on-board power, but simply react to queries from in-store systems -- then more and more of customer's products will identify them as they go about their business. Sooner, stores would have capability to recognize the customer as soon as they enter, and that's what customers are worried about.

The privacy advocates take the cue from the movie Minority Report, when Tom Cruise walks through the shopping mall and all the signs recognize him? The scene takes place in the year 2054 in Washington, D.C. It portrays a society nearly devoid of privacy. According to privacy advocates RFID would be a great way for the government to keep tabs on all its citizens. To alleviate such fears, Dan Mullen, interim CEO of the U.S. branch of the Association for Automatic Identification and Data Capture Technologies (AIM) says that it would be really, really hard.

Comment: When Steven Spielberg was developing the 2002 movie *Minority Report,* he consulted a group of Massachusetts Institute of Technology (MIT) scientists, urban planners, inventors, and futurists to construct a society 50 years from now, based on the technology trends of today.

According to one of the industry reports, gadgets from Alien Technology of Morgan Hill, Calif., can read chips from about 90 feet away, but in principle such tags could be picked up by more powerful receivers in the service of marketers, government agencies and snoops of all kinds. According to the privacy advocates, given the Homeland Security Department's appetite for high-tech tools and the headlong pace of tech innovation, the nightmare scenario could become a reality. They fear that Police would gain a trendy method of constant, cradle-to-grave surveillance.

According proponents of RFID, the consumerists are people who are afraid and who believe that they will be tracked around their homes. For them, the consumerists don't understand that the technology is only good for a few feet.

5) Various alternatives available in present context

To avoid and mitigate public backlash, sponsors/supporters of RFID tags are coming up with innovative solutions. The alternatives are four pronged viz. technologically; regulatory framework, ethically and marketing/branding the RFID right.

The following are some of the alternatives generated technologically by sponsors and manufacturers of RFID.

5.1) Alternatives on the Technological Front

Retailers in conjunction with Auto-ID Center, to ally fears of shoppers have framed guidelines that clearly label all RFID-carrying products at the checkout counter. Chips with "kill switches" are being developed by Philips Semiconductor and Alien Technology. In this way the customers have option to disable as they leave the store. This is needed as RFID moves from warehouse to retail. The kill tag approach is described in detail below:

5.1.1. A) The "Kill Tag" approach

The most straightforward approach for the protection of consumer privacy is to kill" RFID tags before they are placed in the hands of consumers. A killed tag is truly dead, and can never be re-activated.

The standard mode of operation proposed by the Auto-ID Center is indeed for tags to be killed upon purchase of the tagged product. When this design is incorporated a tag can be killed by sending a special kill command (including a short 8-bit password).

For example, a supermarket might use RFID tags to facilitate inventory management and monitoring of shelf stocks. To protect consumer privacy, checkout clerks would kill the tags of purchased goods; no purchased goods would contain active RFID tags.

From the privacy advocates perspective the 'kill' approach is inadequate. According to them, there are many situations and many environments in which simple measures like kill commands are unworkable or undesirable for privacy enforcement as there are many times customer him/herself would not want to kill for specific products. Below is a case presented against killing tags at point of sale.

5.1.1. B) A case against killing active tags

Consumers may wish RFID tags to remain operative while in their post purchase session. Certain examples include a home use set e.g., microwave oven that reads cooking instructions from food packages which rely on actively operational tags. What now know as 'Smarter Homes' can become reality once 'smart appliances' that can use the EPC™ would start interacting with each other when they are connected to Internet. This interaction would

be possible by RFID which will monitor the products inside them and thus helping the customer to alert if any discrepancy arises.

Similarly, new and smart consumer-specific applications for RFID-tags are already beginning to emerge. For example, a Prada store in New York City tracks the RFID tags of items held by customers in order to display related accessories on nearby screens.

Other examples of RFID-tag applications for ordinary consumers include effortless physical access control, theft-protection of belongings, and wireless cash cards.

Individuals may wish to have RFID tags embedded in their business cards, to facilitate scanning by recipients. Here the tag ID may be used to create a URL referring to the actual card data. Also a store may wish to embed RFID tags in store-issued coupons, for ease of scanning at the checkout counter. A user may wish to scan his possessions when a recall for a specific set of products is issued. Collectibles such as baseball cards or CDs may have RFID tags, to enable owners to manage their inventory better.

An airline ticket may contain an embedded RFID tag to allow simpler tracking of passengers within an airport.

Businesses may include RFID tags on the invoices, coupons, and return envelopes they mail to consumers, for ease of sorting upon return.
Such function creep promises to result in many more uses unimagined or unimaginable today in which active tags will be valuable to consumers or businesses.

Pros and Cons:
Thus, while the kill-tag on purchase approach may handle many or even most instances of potential concern for privacy, it is unlikely to be a fully satisfactory solution because of many issues as mentioned above or in general, lethargy of the consumer to kill the tag. It thus seems imperative to explore alternative approaches.

5.1.2) The Faraday Cage approach

An RFID tag may be shielded from scrutiny using what is known as a Faraday Cage, a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies).
If high-value currency notes do indeed come supplied with active RFID tags, then it is likely that foil-lined wallets will become big sellers.

However, a vast range of objects using RFID tags cannot be placed conveniently in containers, such as clothing, wrist-watches, and cell phones.

Pros and Cons:
Faraday cages thus represent at best a very partial solution to consumer privacy. Petty thieves are known to use foil-lined bags in retail shops to circumvent shoplifting-detection mechanisms.

5.1.3) The Active Jamming Approach

Active jamming of RF signals is another, related physical means of shielding tags from view. The consumer could carry a device that actively broadcasts radio signals so as to block and/or disrupt the operation of any nearby RFID readers.

Pros and Cons:
This approach may be illegal. It could cause severe disruption of all nearby RFID systems, even those in legitimate applications where privacy is not a concern.
The approach is akin to jamming, but is much more subtle in its operation, interacting cleverly with the RFID singulation protocol to disrupt only certain operations.

Comment: RFID readers can't talk to more than one tag at a time, so when multiple tags reply to a query, the readers detect a collision and revert to what's known as a singulation protocol to communicate with each tag individually

5.1.4) The Smart RFID Tag Approach

Another general approach is to make the RFID tags smarter, so that they interact in a way that protects privacy better, while providing the desired active functionality would typically involve the use of cryptographic methods.

In smart RFID approach, consumers can selectively block readers from reading any chip on the consumer's person. Such blocker chips can be built cheaply. They only need to interfere with the "singulation" protocol that readers use to address each RFID chip individually in turn.

Pros and Cons:
Thus selective blocking approach is compatible with this method of protecting reader transmissions from eavesdroppers.
By giving consumers the ability to block unwanted readers from reading their RFID tags, as well as allowing consumers to "kill" their RFID tags, one may be able to provide consumers with sufficient control over how their RFID tags are used to allow implementation of acceptable privacy policies.

5.1.5) Selective disclosure of information

RFID sponsors and manufacturers must look into technological solutions that protect consumer personal identity while enabling consumers to provide accurate information to retailers to which the consumer is interacting. RFID sponsors can take cue from 'The Platform for Privacy Preferences Project' (P3P) applications which helps consumers control the type of information they provide to Web sites (Reagle and Cranor 1999). P3P allows

Web sites to offer explicit agreements based on specific privacy disclosures. On similar lines, RFID users can be given power to selectively give information depending on agreements with the retailer.

Pros and Cons
The complexity involved in providing customized RFID to each customer may be a logistical nightmare. Technologically also, it may take time to develop such applications incorporating selective dissemination of information.

5.2) The Regulation Approach

Privacy and confidentiality issues have existed since the earliest days of modern computers. The Census Bureau used Hollerath machines, the first electronic calculators in the 1880 census. Census marshals in that same census signed oaths agreeing not to divulge information they collected about census subjects.

At one time, US Congress operated an organization that engaged in technology assessment. It established the nonpartisan Office of Technology Assessment (OTA) in 1972 to provide Congressional committees with objective analysis of public policy issues related to scientific and technological change. This agency survived for two decades.

The OTA was dissolved in September 1995, tragically just at a time of dramatic advances in many technologies – the Internet, genetics, biometrics, wireless communications, technologies of surveillance, and the beginnings of pervasive computing, sometimes referred to as ubiquitous computing.

To fill up the vacuum created by absence of OTA and in an effort to balance commerce with consumer privacy needs, the Federal Trade Commission (FTC) has relied on fair information principles to guide privacy regulation and industry practice in the United States (FTC 1999b). These principles mostly based on self regulatory mechanism include notice/awareness, choice/consent, access/participation, security/integrity, and redress/enforcement.

5.2.1) Self Regulation

There are two approaches for regulation viz. self regulation by the industry and other done by law enforcing agencies. Self-regulation differs from a pure market approach in which consumer preferences drive company behavior. Under a pure market approach, it is assumed that consumers prefer to do business with firms that have implemented strong privacy protections and avoid firms that have breached privacy. In contrast, self-regulation is based on the three traditional components of government**--legislation, enforcement, and adjudication**--and these functions are carried out by the private sector rather than the government (Swire 1997). Legislation refers to the question of defining the appropriate rules,

enforcement to the initiation of an enforcement action when the rules are broken, and adjudication to whether or not a company has violated the privacy rules (Swire 1997).

Despite industry self-regulation efforts, according to privacy advocates, many database owners are not following fair information practices. In addition to the lack of fair information practices followed by database owners, other privacy issues exist. In particular, the Internet has made it possible for organizations to disseminate information without the immediate knowledge of consumers. The major concern is that this data collected with help of RFID will be accessed at a later date and used for purposes other than that for which it was intended. It is argued further that even firms that make a commitment to privacy may at times compromise privacy standards if it is competitively necessary.

Following the Self Regulatory framework, Simson Grafinkel, of MIT Auto- Id proposes 'The 'RFID Bill of Rights', a set of principles which consist of five articles as a voluntary framework for commercial deployment of RFID tags.

The articles are:

1. The right of the consumer to know what items possess RFID tags
2. The right to have tags removed or deactivated upon purchase of these items
3. The right of the consumer to access of the data associated with an RFID tag
4. The right to access of services without mandatory use of RFID tags and
5. The right to know to when, where, and why the data in RFID tags is accessed.

The spirit of above articles is also similarly conveyed in a proposal submitted by CASPIAN, 'The RFID Right to Know Act of 2003'. The proposal requires mandatory labeling to inform consumers when an item contains an RFID tag. It would also prohibit companies from linking the chips with personally identifying information.

Conclusion:
These five rights themselves would not be able on standalone basis to completely assuage fears of consumers and privacy activists. But nevertheless these regulations would go long way in coming years to bring acceptability among consumers as barcodes had been twenty years ago. Manufacturers, Suppliers and Retailers need to rollout comprehensive framework covering all aspects such as policies and procedures that ensure complete privacy concerns and make these policies public to bring wider acceptability among consumers.

5.3) Ethics and RFID

The foundation of ethics lies in following adage 'Power and responsibility should be in equilibrium'. Whichever partner in a relationship has more power also has the responsibility to ensure an environment of trust and confidence. Accordingly, if RFID proponents or an organization using RFID choose a strategy of greater power and less responsibility, it might benefit in the short run; however, that organization will lose power in the long run (e.g.,

increased government regulation). In contrast, a company in balance with its customers should benefit both in the short run and the long run.
To maintain such balance, facilitate trust and advancement of information technologies in society, organizations such as 'Computer Ethics Institute' laid down 'The Ten Commandments of Computer Ethics'. The RFID ethics can be laid down on same lines:

Comment: It is a research, education, and policy study organization that focuses on the interface of advances in information technologies, ethics, and corporate and public policy.

5.3.1) The Policy for RFID privacy mapped on to "The Ten Commandments of Computer Ethics":

1. Thou shalt not use a computer (RFID) to harm other people.
2. Thou shalt not interfere with other people's computer (RFID) work.
3. Thou shalt not snoop around in other people's computer (RFID) files.
4. Thou shalt not use a computer (RFID) to steal.
5. Thou shalt not use a computer (RFID) to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer (RFID) resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer (RFID) in ways that insure consideration and respect for your fellow humans.

While following the above mentioned ethics, the policy makers on RFID privacy have to deal two conflicting realities. On the one hand, the general perception of privacy is broader in many respects than the scope of clearly defined legal rights. On the other hand, the privacy law/ethics structure ranges from clearly defined to wildly obscure because it flows from multiple sources - constitutional law, tort law, statutes and changing public perceptions.

When faced with a privacy issue policy makers have to first determine if existing law addresses the issue. One must examine privacy policy to avoid permitting a RFID supporter to pursue a strategy that will raise the specter of legislation or litigation. However, it is not wise to conclude that every issue that seems to involve privacy in fact creates a privacy problem. Often if one defines the harm caused by a supposed invasion of privacy, one can tailor a RFID implementation strategy to avoid that harm. Thus, we see that RFID privacy issues often beg for self-regulatory and technological solutions.

5.3.1) The 10 Commandments and RFID

The Commandments are readily applicable to the topic of privacy in RFID. Some general examples and illustrations are listed below.

1. **Respect confidentiality (1, 2 and 8)** If the data repository owners or data vendors desires to forward or otherwise share with other agencies (both Government and non-Government) they must make sure it is permissible. If that is somehow impossible, they must strip off all personal and identifying information with the product item purchased by the consumer.
2. **Don't "flame" (Commandments 1,10)** The data collected must not be edited and be in original format and spirit otherwise it may cause great harm to the customer about whom data is collected. The data delivered electronically is easy to transfer, replicate and modified than any other type of media with potential for long lasting effects.
3. **Don't be anonymous (Commandments 1,5,10)** Data collectors and repository holders must use the services with proper authentication, unless whistleblowing or otherwise fear recrimination for telling the truth. They must tell when, where and how and for what purpose the data was collected while disseminating the data to third party
4. **Don't allow third party to access other's data (Commandment 3)** Gaining access to another's data is not justifiable unless expressly acting as their agent. Looking at someone's data and information without valid and authentic reasons would be made unlawful.
5. **Don't misrepresent or lie (Commandment 5)** Given the issue of the lack of privacy with the data collected by using RFID, the potential exists for a misrepresentation or falsehood to revisit the sender.
6. **Follow government's general guidelines (Commandment 7)** The repository owners/managers must check to see if the service provider, or the data solicitor, has RFID privacy policy. If one in place, repository holders must know what is delineated. If not, they must follow the guidelines framed by law. Anything transmitted may be publicly aired if a privacy policy is not in effect.
7. **Consider presentation of message (Commandment 10)** The repository owners must evaluate the content of data to be disseminated. They must be aware of cultural differences or other issues that may affect the recipient adversely.

If a repository owner does not have an RFID privacy policy, it should, as well as establish privacy solutions that deal with all issues and assuages consumer's privacy concerns.

5.3.2) Framing the RFID Policy

The following aspects of policy formation have to be given critical review by the policy framers and law makers while framing the RFID policy, along with the additional concerns which is listed below:

Policy Questions

1. Who has a stake in establishing a responsible policy regarding access to and disclosure of repository's data? How will the policy affect the consumers, retailers, manufacturers, third parties, law enforcement authorities, data connectivity and data repository service providers?
2. What baseline legal rights and duties constrain any policy?
3. What operational features of RFID and data collection, storage and dissemination systems should affect any policy on access, use and disclosure?
4. What analogies can be used to help formulate a consistent set of policies?
5. What criteria should be used to evaluate a proposed policy?
6. Has your policy been disclosed in advance to all concerned?

Additional Concerns

1. Who from the commercial organization, privacy advocates and Government agencies should participate in the development of the policy?
2. What corporate resources in terms of cost and time and personnel should be considered in formulating overall RFID privacy policies?
3. "What information will you want to gather in advance or during the course of formulating your policy?"
4. What kind of research methods would the policy makers' use while eliciting and analyzing public opinion and till what confidence level?

The most important concept is development of a RFID privacy policy with procedures for implementation and communication to all the parties whose stakes are involved in full-scale RFID implementation. This is because, according to privacy advocates, commercial firms and the governments all over the world in the information intensive society often use public opinions as an alibi to frame their arguments in support of or in opposition to specific privacy policies.

One of the most important stake holders is consumer and for getting its views, perception and opinion research studies must be done by independent and neutral bodies.

5.3.3) Formation of Privacy Policies on Public Opinions

The consumer research brings consumers together on a single platform and gives policy makers a handle, who rely on consumer research, to understand consumer psyche. The research is important how consumers think and more importantly why they think that way. Correctly gathering, analyzing and disseminating public opinion would go in long way to frame most widely acceptable privacy policies.

The flip side of relying on public opinion is that the laws which consumers obey from their childhood **conditions** the boundaries that separate the public from the private spheres and finally help in shaping expectations of privacy. This turns out to be a kind of circular loop where both public opinion and privacy policy reinforce each other. Also, the expectations from the privacy policies which are yet to be framed are culture and country specific. This is due to different economic and social conditions (recession, unemployment, socialist or capitalist economy etc.), level of trust of public in Government policies that whether the government would look after them and create laws to protect them.

Also, commercial firms have been the major sponsors for professionally administered public surveys, which according to privacy advocates skew this research reports in favor of commercial firms, and often introduce them into testimony as the will of public.

To avoid skew ness, consumer research must be done by an independent and respected body and must cover the following points:

1. Major expectation (both implicit and explicit) regarding the privacy of personal information
2. Major concerns (both rational and emotional)
3. Rules regarding consumer's control of information provided
4. Rules governing the access the personal information
5. Rules governing the collection of personal information
6. Rules governing the use of information
7. Rules governing the exchange of information

When the public opinion is collected, filtered for relevant information, analyzed and finally interpreted the issues involved in implementing the public opinion must be analyzed. Few issues which may arise while incorporating public opinion into privacy policy are:

1. Cost of implementation of the recommendations of the public survey
2. Implementation scope in terms of number of man days.
3. Level of acceptability among different players involved in RFID imbroglio.
4. Competition among the commercial firms who accept and don't accept the recommendation.

Comment: 1.According to Canadian Direct Marketing Association, which has called for enforceable legal privacy rights, that without a clear legal framework in place, Companies that want to protect consumer privacy will not be able to compete effectively with companies that do not. In fact same kind of statement was made by America Online when it explained the sale of its customer database by saying that it could not otherwise compete with other online service providers.

5.3.4) Differences across cultures and continents

The United States and Europe exhibit very different approaches to information privacy--a condition of limited access to identifiable information about individuals--from both regulatory and managerial perspectives. Grounded in different cultural values and assumptions about the meaning of privacy (a "human rights" issue in Europe versus a contractual issue in the United States), these differences have led to regulatory and managerial conflicts. U.S. corporations would be well served to embrace some of the premises of the European perspective. However, the United States would be poorly served by the creation of a federal regulatory structure such as some commonly found in Europe.

Thus we see if US doesn't come up with a comprehensive privacy policy soon, covering both human rights and contractual perspective, following problems may arise:

1. Conducting business by US firms nationally and internationally
2. Business in Europe: Since the US lacks complimentary safeguards in many sectors, some US business may be unable to do business in Europe and European Union privacy officials may restrict the flow of personal data to the US because of inadequate consumer protection. An interested twist to NAFTA problem.
3. Increase of distrust and antipathy by public in institutions, both public and private.

Comment: European Union has adopted a comprehensive privacy directive to protect the flow of personal information within EU

Conclusion

The ethical implications of privacy for RFID implementation is not explored much by RFID policy makers, but it can be mapped on existing policies and procedures followed by online marketers and online community.

The Governments all over the world while framing public policy must make provisions in their privacy policies that would ensure that consumer's data are gathered and used by organizations using RFID within above given ethical framework.

The big legal-umbrella strategy adopted by commercial organisations, as put by Michael Beresik, national director for PricewaterhouseCooper's privacy practice, must be discouraged to protect consumers who would always and had been valued and demanded the right to privacy. There is no escape as this issue of privacy will continue to compete with other values in our global society and within the information technology era. The clash of old inherent freedoms and new emergent technologies will continue to generate ethical issues for discussion, reflection and action.

Comment: "The 'big umbrella' policies are designed by attorneys to give companies the greatest possible latitude to gather and share information inside and outside the company. It covers them for anything they do or might conceivably down the road."

5.4) Branding the RFID right

Public backlash against RFID, cloning, virtual reality, biometrics and other commonplace concepts today is partly due to representations of the technologies in film, print media and science-fiction literature. Artists are generally very good at reflecting human nature in the tenor of their times and sometimes that leads to very valuable insights, according to Dr Dean Economou, Chief Technologist, CSIRO. Symbiotically, scientists have taken many cues from what they've seen take place on screen and try to replicate in real world.

Steven Spielberg, in his movie 'Minority Report' has accomplished with his team of MIT futurists a form of technology assessment, that is, a holistic look at the impacts of technology on all aspects of societal behavior in the not-so-distant future. It is just this sort of analysis that so far has been missing in the public policy arena regarding the deployment of RFID at product level and consequent privacy concerns.

It is imperative that what serves as technology assessment today comes from the public policy realm and not from paranoid version of Hollywood movies so that policy makers can frame correct privacy policies.

Commercial organizations propounding and using RFID have the responsibility to put public relations in proper order to avoid backlash from the privacy activists and consumers in general. Organizations must have clearly stated guidelines educating the consumers how RFID implementation is going to benefit them and the industry in general. The guideline must state any drawbacks if any customer might face. The organizations must invite privacy activists, retailers, suppliers, policy makers and all other parties involved in the issue to answer and pre-empt any query pre rollout. They must be prepared to all questions posed by media pre and post RFID implementation.

Same sentiments are reflected in the documents prepared by Fleishman-Hillard, a communications consultancy. The document suggests that one method of doing is through the creation of a Privacy Advisory Council made up of "well known, credible, and credentialed experts" who may be "potentially adversarial advocates" having varied backgrounds viz. political, legal and technology .All these would lead to increase in trust in RFID technology and wider acceptance among consumers.

6) Conclusions

Privacy is already challenged everywhere-with video surveillance cameras, mobile phones, GPS and credit cards and the customers are aware of the fact. The opposition for RFID lies for its ubiquitous ness, automatic identification without prior information of the consumer, immense data collection prowess and networking in mobile environments.

RFID industry is still in a state of experimentation. All of the customers are participating in a phase of extensive field trials. During this inception stage, organizations and policy makers need to develop stringent safeguards on how RFID systems are implemented and used. All new technologies require a good hard look at their implications, which RFID supporters must not forget in their quest for the efficiency and profitability.

Like many new technologies, there are both benefits and dangers in implementation of RFID. What's needed is public awareness, and developing the technology such that it meets legitimate needs, while protecting the privacy of end users. RFID industry members must respond to consumer concerns about threats to their privacy and clearly define the scope and limitations of the information-handling and dissemination practices they intend to follow.

Ideally, RFID industry self-regulation could be preferable to government regulation because RFID industry is more familiar with its own operations and with the special vulnerabilities of its data repositories to abuse. However, to date, with the possible exception of Marks & Spencers , industry self-regulation has not been conspicuous by its ability to resolve the problems that give rise to demands for enforceable governmental and privacy advocates' performance standards.

Comment: Marks & Spencer adhered to all of the requirements in legislation CASPIAN has proposed in the United States. It informed customers about the trial, placed tags on the clothes in such a way that they would be disposed of when the consumer removed the packaging and price tags, and didn't use RFID to collect any data on the customer at the point of sale.

The need of the hour is to act together and take a coordinated approach by all parties concerned, look into privacy issues more deeply, listening and acting on consumer concerns and finally make recommendations and build industry consensus.

Acceptance of RFID will grow phenomenally if the confidence is reinforced by proactive efforts (self-regulatory) by companies and industries to ensure consumers have an effective recourse for privacy complaints.

The comprehensive solution for alleviating privacy concern can be either one of the proposed systems mentioned above in the paper or it can be combination of two or more. The solution depends on the quality of data being collected, stored and disseminated; the users of the data and finally the expectations of consumers regarding security and trust in both public and private institutions.

Some of the brief solutions are given below:

1. **Technical Solution:** Either 'Kill- Tag', 'Farady Cage' or 'Smart Card' or combination of any three can be utilized by the retailers at point of sale depending upon context and customer's choice.
2. **Regulation approach:**
    a. Business shall not combine or link an individual's nonpublic personal information with RFID tag identification information
    b. Consumer must be informed about RFID data collection system and what would be done in future to the data collected.
3. **Self Regulation:** Each commercial organization can determine its own policy within a given framework – but failure to meet that policy should be considered a deceptive act subject to Federal Trade Commission (FTC) enforcement.

4. **Protocol Setup:** A well designed system must be set in place at data repositories and exchanges which will protect consumers by implementing the proper protocol to achieve a level of security comparable and even beyond more mature technologies.
5. **Data Integrity:** Business shall not, directly or through an affiliate, disclose to a nonaffiliated third party an individual's nonpublic personal information in association with RFID tag identification information.
6. **Non Identification:** Business shall not, directly or through an affiliate or nonaffiliated third party, use RFID tag identification information to identify an individual. To mitigate identification risks, it is essential that authentication systems be designed to support effective privacy practices and offer individuals greater control over their personal information.
7. **Limited access to the personal data:** Mechanisms in form of passwords (both permanent and temporary) must be set in the data exchange system.
    a. Permanent password - Attorneys, Government agencies, Police can be given permanent passwords and they can download a file but must give valid reasons for doing so. They must have subpoena in their possession. The data protection responsibility lies in hands of the permanent password holders once they download the file.
    b. Temporary password – Temporary passwords can be issued by data vendors to the parties of interest only after setting proper privacy mechanism both at their and the client's site. The retail exchanges where data is stored and disseminated must post - in clear and conspicuous language - a disclosure of its privacy policy, so consumers know how their personal information will be handled.
8. **Branding RFID and Educating the public:** Effective efforts must be taken by RFID sponsors and supporters to educate shoppers about the potential benefits they will receive if they agree to allow retailers to track their purchases and simultaneously assuring them that it will not intrude their privacy.

Finally, to attain legitimacy in the public mind, these solutions must accept the basic privacy principles now reflected in a piecemeal fashion in much of the self regulatory measures and legislation. They must provide adequate standards of security, respecting interception and access; acceptance of the basic confidentiality of personal information collected by an organization during RFID implementation and application; clear limitations on the use and disclosure of this information to third parties; and full and open disclosure to consumers of record keepers' information practices and their rights with respect to the accuracy of their own information and to withhold consent to its disclosure.

References:

1. Roberti, Mark (2003, September 1). IT Does Matter. [Online]. Available: http://www.rfidjournal.com/article/articleview/553/1/2/ [October 31, 2003].

2. The association for Automatic Identification and Data Capture Technologies (2003). What is Radio Frequency Identification (RFID)? [Online]. Available: http://www.aimglobal.org/technologies/rfid/what_is_rfid.htm[September12, 2003]

3. Shim, Richard (2003, May 5). Radio ID chips to come with kill switch. [Online]. Available: http://news.com.com/2100-1039_3-999794.html?tag=rn [September 14, 2003].

4. Gilster, Paul (2003, July 2003). RFID threatens privacy. [Online]. Available: http://newsobserver.com/business/story/2717267p-2519499c.html [October 27, 2003].

5. Roberti, Mark (2003, October). Precedents Set. [Online]. Available: http://rfidjournal.com/article/articleview/627/1/2/ [October 27, 2003].

6. Epic top news (2003, Oct). RFID Developers Public Relations Plans Revealed. [Online]. Available: http://www.epic.org/privacy/rfid/ [October 28, 2003].

7. Kuchinskas, Susan (2003, August 15). California Scrutinizes RFID Privacy. [Online]. Available: http://www.wi-fiplanet.com/news/article.php/3064511 [October 28, 2003].

8. Awerdick, John H. (1996): "On-Line Privacy" The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, *Computer Law Association.* [Online]. Available: http://cla.org/RuhBook/chp4.htm [October 28, 2003].

9. Juels, Ari and Rivest, Ronald L. and Szydlo, Michael (2003) : "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy". [Online]. Available: http://theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.pdf [September 12, 2003].

10. Givens, beth (2003) : " RFID and Public Policy Void- Testimony by Beth Givens at Joint Committee on Preparing California for the 21st Century". [Online]. Available: http://www.privacyrights.org/ar/RFIDHearing.htm [October 12, 2003].

11. Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels (Spring 2003): "Radio-Frequency Identification: Security Risks and Challenges," RSA Laboratories Cryptobytes, Vol. 6:1. [Online]. Available: www.csail.mit.edu/research/abstracts/abstracts03/theory/54rivest.pdf [October 28, 2003].

12. Vance, Cathy (2002): "The Broad Reach of Privacy Regulations", Commercial Law Bulletin, Mar/Apr2002, Vol. 17 Issue 2, p16, 3p, 1bw

13. Schoeman, F (1984): "Privacy: Philosophical dimensions of the literature" in Philosophical dimensions of privacy, Cambridge University Press

14. Milne, George R. and Culnan, Mary J. (Oct2002) : "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998–2001 U.S. Web Surveys", Information Society Vol. 18 Issue 5, p345, 15p

15. Milne, George R (Spring 2000) : "Privacy and Ethical Issues in Database/Interactive and Overview of the Special Issue", Journal of Public Policy & Marketing, Vol. 19, Issue 1

16. Jones, Mary Gardiner (Spring 91) : "PRIVACY: A SIGNIFICANT MARKETING ISSUE FOR THE 1990S", Journal of Public Policy & Marketing, Vol. 10, Issue 1

17. Culnan, Mary J(Spring 2000) : "Protecting Privacy Online: Is Self-Regulation Working?", Journal of Public Policy & Marketing, Vol. 19 Issue 1, p20, 7p

About the Author

Rakesh Kumar is currently working with Wipro Technologies as consultant (Supply Chain Solutions) in 'Retail' domain. He completed MBA at Indian Institute of Management (IIM) Ahmedabad, India in year 2003. His focus areas at IIM Ahmedabad were Logistics and Supply Chain Management; Infrastructure and Transportation Systems; International Finance and Marketing.

Prior to his management studies he worked with Mitsui O.S.K. Lines for three years where he gained experience in Logistics and Shipping, Freight Forwarding and Transport Management Systems.
His areas of interest are Retail Sciences, Science Fiction and Psychology.

The author thanks and appreciates the help provided by Mr Mani Subramaniam, Principal Consultant, Wipro Technologies, for constructive comments and encouragement.

The author can be contacted at RAKESH_KUMAR@IITIIM.COM

Wipro in Retail

Visit http://www.wipro.com/retail

Wipro offers world-class software and technology solutions for the retail industry. Wipro combines years of technical experience and domain knowledge in providing solutions to retailers across the globe. We provide end-to-end e-business, DW/BI, CRM, SCM and technology infrastructure solutions and help retailers improve services, convenience and personalization. We have established Centers of Excellence (CoE's) in the areas of point to sales, supply chain execution, merchandizing and pricing to provide best-in-class solutions to our customers.