Privacy Year in Review: America's Privacy Laws Fall Short with RFID Regulation

KATHERINE DELANEY*

ABSTRACT

Radio frequency identification devices (RFIDs) are the next generation of bar codes. They are labels that are placed on merchandise or objects to identify their location. The tags contain, minimally, an identification number and an antenna, so that it is readable to a scanner. More advanced tags may have greater recording and re-writable ability. Various industries have made use of them from warehouses to libraries, the military, and those promoting access for the disabled or the protection of children. Because they are a developing technology, many privacy concerns have not been adequately addressed. Currently, the United States has not done enough to ensure consumer safety. Personally identifiable information is at risk of exploitation by unethical parties. Also, the possibility of an individual being monitored through the use of these tags is achievable. In order to ensure its citizen's safety and the protection of their information, the United States must implement best practices or standards that companies employing RFIDs must use.

I. INTRODUCTION

New technologies promise exciting possibilities, but also create opportunities for abuse. Radio Frequency Identification Devices (RFIDs) are no different. These "smart bar codes" have "become one of the fastest growing and widely used methods to precisely track and identify people, merchandise[,] and animals in numerous environments."[1] Fear of their power is delaying acceptance, however. The Auto-ID Center at the Massachusetts Institute of Technology (MIT) conducted a study in which 78% of respondents reported

---

* Katherine Delaney is a candidate for juris doctor at The Ohio State University Moritz College of Law, class of 2006. She has a B.S. in management information systems from the University of Notre Dame.

[1] DETECTAG, RADIO FREQUENCY IDENTIFICATION (RFID) (Detectag is a Canadian corporation that designs and sells anti-shoplifting systems.), *at* http://www.detectag.com/index.php?Action=viewproducts&category=RFID (last visited Apr. 27, 2005).

privacy concerns involving knowledge of what was being tagged or read.[2] The question is: What is being done to protect the consumer?

RFIDs are not new. As early as World War II, they were being used to recognize the origins of ships and airplanes.[3] More widespread use is now possible because of lower costs and more efficient data analysis. Unfortunately, the wide-spread utilization and analysis is also the cause of concern. Determining whether a vehicle belongs to an ally is not controversial, while tracking someone's movements because he bought an item with an embedded tag is.

With proper constraints, RFIDs can significantly assist in many areas. In Part II of this article, the strengths and limitations of the technology are discussed. Part III evaluates the current and potential uses. Part IV reveals privacy concerns that have arisen, and Part V discusses current and potential legislation and constraints.

II. RFIDS ARE CAPABLE OF ITEM SPECIFIC IDENTIFICATION

Universal Product Codes (UPCs) are a part of daily life. RFIDs are a more advanced replacement. While capable of much more functionality, the premise is the same: a number is assigned to a product to identify it. The difference is that UPCs identify a type of product, such as a given brand of toothpaste. RFIDs are more specific, and would be able to inform the retailer exactly which tube was taken off the shelf and where it was relocated.

RFID is defined by some as "a non-contact, non-line-of-sight technology that employs radio signals to effect communications between a reader and a RFID tag."[4] This means that whenever a tagged item is in proximity to a reader, it can be detected, whether it is physically "visible" to the device or not. Each tag contains an antenna that can be read when it passes into the "capture window."[5] Size can

---

[2] Meridith Levinson, *Customers to Retailers: Take Us Seriously: Privacy Advocates Turn up the Pressure*, CIO MAGAZINE, Dec. 1, 2003, *available at* http://www.cio.com/archive/120103/retail_sidebar_2.html (last visited Feb. 16, 2005).

[3] Meridith Levinson, *The RFID Imperative*, CIO MAGAZINE, Dec. 1, 2003, *available at* http://www.cio.com/archive/120103/retail.html (last visited Feb. 16, 2005).

[4] ODIN TECHNOLOGIES, SUMMARY INFORMATION: ANALYSIS OF AUTOMATIC IDENTIFICATION TECHNOLOGY (AIT) FOR ASSET TRACKING AND INVENTORY MANAGEMENT (Oct. 1, 2003), *available at* http://www.odintechnologies.com/ (last visited Apr. 27, 2005) [hereinafter SUMMARY INFORMATION].

[5] *Id.*

vary depending on the antenna size and the capabilities built into the reader. "The length of the antenna is based on the length of the signal wave," so high frequency tags can be much smaller than low frequency ones.[6]

The standard RFID is approximately the size of a grain of rice, although most of its size is the antenna.[7] Because of their small size, RFIDs are easily attached to most products. Some tags can only be read, but others can transmit messages or have information saved on them. The tags vary as to the amount of memory and rewrite capability they contain.

A. KINDS

RFIDs include active, semi-passive, and passive products.[8] The difference is whether the tag has its own power source and if it is capable of both sending and receiving information. Active tags are two-way devices that have battery power so that they can send and receive information. Passive tags, at the other end of the spectrum, contain minimal information and are only capable of being scanned. Semi-passive tags lay somewhere in between active and passive tags.

The Department of Defense uses active tags for tracking and identifying cargo containers.[9] However, an active tag is usually not necessary for this sort of asset tracking. The reason the government utilizes this higher-capability tag is that passive tags often have difficulty when hardware that creates ambient "noise, " such as a router or switch, is nearby.[10] Active tags also have a bigger read range, which means the signal from the tag can be picked up at a greater distance.[11] Finally, active tags have the unique capability of

---

[6] R MOROZ, LTD., UNDERSTANDING RADIO FREQUENCY IDENTIFICATION (RFID) 6 (July 2004), *available at* http://www.torwug.org/WhitePapers/PDF/Understanding_RFID_b-1.pdf (last visited Apr. 27, 2004).

[7] Tom Mead, *Let Me Talk You Through It: RFID TAGS: Can the Visual Cues by Which We Find Our Way Be Conveyed to the Blind?*, THE LONDON FINANCIAL TIMES LIMITED 14, Nov. 6, 2003.

[8] SUMMARY INFORMATION, *supra* note 4, at 7.

[9] *Id.*

[10] *Id.*

[11] *Id.* at 9; *see also* ACTIVEWAVE, PRODUCTS (Activewave advertises that their active tags have a read range of up to 279 feet.), *at* http://www.activewaveinc.com/products_active_tags.html

acting as a "parent" tag. This occurs when a container is marked with an overarching tag, and the contents inside the container are tracked with passive tags. A greater level of organization is possible with this hierarchical system.[12] While the benefits are great, so is the cost, with active tags often ranging from $16 to $50 each.[13]

Most of the retail community has made use of the 13.56 MHz passive tag, as its readability is sufficient for the desired tracking and inventory purposes.[14] Frequently, tags that employ backscatter technology are employed. Backscatter technology means that the tags "reflect back to the reader a portion of the radio waves that reach them."[15] This is the type of tag that is known as a "smart label."[16] There are two versions of this form of backscatter tag: ISO 18000 and EPC. They each have different standards,[17] but both standards work essentially the same way.

EPC stands for an Electronic Product Code. Such a code is similar to the familiar printed UPC "bar codes," in that stores can use it to identify an item, but the EPC goes further. Each EPC is unique to a given item, so each item is distinct from the next on the shelf. "Essentially, the EPC is a number designed to uniquely identify a specific item in the supply chain. The EPC number sits on a tag comprised of a silicon chip and an antenna, which is attached to an item. Using radio identification technology (RFID), a tag 'communicates' its number to a reader."[18]

(last visited Apr. 2, 2005); *see also* TRIVALENT SOLUTIONS, INC., RFID FAQs (Trivalent states that they can be read "100 feet or more away."), *at* http://www.trivalentsolutions.com/solutions.php?sp=3&ssp=2 (last visited Apr. 2, 2005).

[11] SUMMARY INFORMATION, *supra* note 4, at 7.

[12] *Id.*

[13] Jennifer Maselli, *New Active Tags for Access Control*, RFID JOURNAL (May 14, 2003), *available at* http://www.rfidjournal.com/article/articleview/422/1/1/definitions_off; *see also* TRIVALENT SOLUTIONS, INC., *supra* note 11 (Active tags retail for $20).

[14] SUMMARY INFORMATION, *supra* note 4, at 7.

[15] TRIVALENT SOLUTIONS, INC., *supra* note 11.

[16] SUMMARY INFORMATION, *supra* note 4, at 8.

[17] *Id.*

[18] EPC GLOBAL, FREQUENTLY ASKED QUESTIONS, *at* http://www.epcglobalinc.org/about/faqs.html#6 (last visited Apr. 27, 2005).

B. CAPABILITIES

With item-specific identification, the functionality of bar codes is increased. It is no longer merely an inventory tool for reordering. Items can be located regardless of whether they are being manufactured, in the warehouse, on the shelf, or on the way out the door. At any point in time, a customer's needs may be better met because of this knowledge. The item is always where it can be best utilized.

Unlike a linear bar code, which must be in the reader's line of sight to be scanned, an RFID can typically be read through "dirt, paint or thin layers of obscuring material."[19] "For unattended reading, there is a 99.8% or better success rate."[20] Therefore, an employee no longer must touch each individual item, but rather can monitor an area by a central reader. Efficiency is increased and simultaneous knowledge of an item's whereabouts is possible. Passive tags typically have a range of five to seven feet.[21] Thus, either readers can be placed in such intervals, at the entrances and exits of the monitored area, or attached to a transportable cart. "Effective read range depends on a variety of factors including antenna design, acceptable reader power levels, material on which the tag is applied, and tag-to-antenna orientation."[22]

The extensive tracking capability also allows for what is known as "silent commerce." Human involvement is no longer needed on the business end for a transaction to occur. "When combined with continuous and pervasive Internet connectivity, they form a new infrastructure that enables companies to collect data and deliver services without human interaction."[23] Tags are automatically read, rather than scanned by a cashier.

---

[19] SUMMARY INFORMATION, *supra* note 4, at 8.

[20] *Id.*

[21] RETAIL INDUSTRY LEADERS ASSOCIATION (RILA), CONFERENCE OF STATE RETAIL ASSOCIATIONS: RFID PUBLIC POLICY CHALLENGES at slide 6 (Aug. 8, 2004), *at* http://www.retail-leaders.org/new/admin/imagebox/Final%20CSRA%20RFID.ppt#686,7 (last visited Apr. 27, 2005).

[22] SUMMARY INFORMATION, *supra* note 4, at 8.

[23] TRIVALENT SOLUTIONS, INC., *supra* note 11.

C. LIMITATIONS

Cost has restricted mass implementation. A typical bar code only costs a fraction of a cent, unless printed on more durable materials.[24] An inexpensive RFID currently costs approximately $.50, though costs are falling rapidly.[25] Price also depends on the volume of the purchase to some extent.[26] "Buy 1,000 chips and they may cost $1 each. Buy 1 million and each may cost 50 cents."[27] However, more than the tag must be considered. A reader can cost between $20 and several thousand dollars.[28] Stores are currently set up with UPC or other security monitors, so conversion takes substantial investment.

Although the monitoring of items within the store is much more vigilant, theft is still possible. Range and effectiveness are affected by metal and large quantities of liquid.[29] Therefore, "tags can be 'hidden' by wrapping a tagged item in a thick newspaper...or placing it in a metal briefcase. Small items tagged with some orientation-sensitive tags can be 'hidden' from a reader by being placed in an armpit."[30] Strong electromagnetic pulses can also alter the tag's

---

[24] ASSOCIATION FOR AUTOMATIC IDENTIFICATION AND MOBILITY (AIM), BAR CODE LABELS: THE MAKE OR BUY DECISION, *at* http://www.aimglobal.org/technologies/barcode/makebuy.htm (last visited Apr. 27, 2005); *see also*, SUMMARY INFORMATION, *supra* note 4, at 11.

[25] SUMMARY INFORMATION, *supra* note 4, at 11; *see also* Larry Dignan, *RFID: Hit or Myth?*, BASELINE, Feb. 9, 2004 (Simon Langford, manager of global RFID strategies for Wal–Mart, says tags currently run between 15 cents and 65 cents each.), *available at* http://www.baselinemag.com/article2/0,1397,1522175,00.asp (last visited Apr. 3, 2005).

[26] SUMMARY INFORMATION, *supra* note 4, at 11.

[27] Mark Roberti, *Trends: RFID, From Just-In-Time to Real Time*, CIO INSIGHT, Apr. 12, 2002, *available at* http://www.cioinsight.com/article2/0,1397,1515,00.asp (last visited Apr. 27, 2005).

[28] SUMMARY INFORMATION, *supra* note 4, at 11; *see also, Toppan to Produce $20 RFID Reader*, RFID JOURNAL, Jan. 23, 2003 (Toppan will produce a low-power reader that will retail for $17.), *available at* http://rfidjournal.com/article/articleview/279/1/26/ (last visited Apr. 27, 2005).

[29] *Id.* at 9. *See also*, Dignan, *supra* note 25 (Proctor & Gamble tested RFIDs on shampoo to ensure that liquid would not block the transmission.).

[30] *Id.*

effectiveness.[31] So while the technology has improved, it is still far from perfect.

D. "KILL" SWITCH

According to privacy advocates, one of the more important features of a RFID is its ability to be "killed."[32] The tag should be capable of being disabled. The fear is that if it is not rendered inoperative after the item is bought, then the consumer could continue to be tracked through that item.[33] Suggestions have included either automatically killing the tag at the point of sale, giving the consumer notice that it will not be killed, or giving the consumer the option of leaving it active at that time. The "kill" feature is not a possibility in some situations. For instance, a library would not want the tags within the books to be disabled, because once they are shut down, they cannot be re-activated.[34] The library would have to purchase new tags every time an item was returned. Refreshing them would be costly and inefficient. Consequently, any potential legislation must consider legitimate reasons that the "kill" function would be harmful.

III. VARIOUS USES ARE POSSIBLE

The usefulness of RFIDs is not limited to taking inventories. While the business use of tracking an item through the supply chain has been one of the main rationales for developing the technology, it is far from the only possibility.

The potential applications are many and varied. Businesses, the Department of Defense, and libraries have all been using RFIDs for essentially asset tracking purposes. Some more creative possibilities involve monitoring children at water parks or schools, tracking vehicles for toll systems, labeling patients at hospitals, and providing access to the physically disabled.

---

[31] *Id.*

[32] PRIVACY RIGHTS CLEARINGHOUSE, RFID POSITION STATEMENT OF CONSUMER PRIVACY AND CIVIL LIBERTIES ORGANIZATIONS: A CRITIQUE OF PROPOSED INDUSTRY SOLUTIONS (Nov. 14, 2003), *at* http://www.privacyrights.org/ar/RFIDposition.htm#Attach2 (last visited Apr. 27, 2005).

[33] *Id.*

[34] Norman Oder, *RFID Use Raises Privacy Concerns*, LIBRARY JOURNAL, Nov. 15, 2003, *available at* http://www.libraryjournal.com/article/CA332556 (last visited Feb. 21, 2005).

A. BUSINESS CASE

By increasing supply chain visibility, it is predicted that 180 billion dollars could be saved annually.[35] Retailers can benefit because they do not have to keep as much "safety stock" on hand, will have lower transfer costs due to better supply management, will have fewer "out of stock" instances, and will have less worry about theft.[36] Consumers also benefit from the retailer's increased ability to serve their needs. The chances of having to wait indefinite amounts of time for an item to come into stock are substantially decreased.

Large retailers have provided the push needed to convince manufacturers to label their products. "Wal-Mart has mandated its top 100 suppliers to begin pallet marking with EPC tags on January 1, 2005."[37] Because of Wal-Mart's insistence, virtually every manufacturer in the country is now investigating placing labels on their products. Unfortunately, the rollout has not been proceeding as smoothly as had been hoped because the savings have not proved to be as substantial as predicted.[38] Part of the reason for the delay is the common myth that return on investment does not exist.[39] Often, costs may seem to cancel out benefits, but a greater return can be seen if manufacturing and inventory processes are altered.[40]

Not only can RFIDs track locations, but they can accomplish inventory management on a smaller scale. Tags can be placed on items in kitchens or refrigerators that can then be interpreted by readers within the appliance or room.[41] Potentially, your cupboard could tell you what items you have run out of or your refrigerator could warn you of expiration dates.[42] Knowledge of what is behind the closed door will be at one's fingertips.

---

[35] RILA, *supra* note 21, at slide 9.

[36] *Id.*

[37] SUMMARY INFORMATION, *supra* note 4, at 3.

[38] Demir Barlas, *Wal-Mart RFID Mandate Lag*, LINE 56, Nov. 19, 2004, *available at* http://www.line56.com/articles/default.asp?NewsID=6147 (last visited Feb. 21, 2005).

[39] Dignan, *supra* note 25.

[40] *Id.*

[41] Cliff Edwards, et. al., *Digital Homes*, BUSINESS WEEK, July 21, 2003, at 58.

[42] *Id.*

Inventory methods are also being used to help law-enforcement personnel track evidence.[43] By tracking each item individually, chain of command issues are lessened. A complete record is kept for use in court. Conflict over mishandling should be substantially lessened, as evidence movements can be tracked.

B. DEPARTMENT OF DEFENSE (DOD)

Essential shipments are transported overseas daily. With heightened world tensions, it is imperative that the military gets its shipments in a timely manner. Therefore, "the Defense Department's policy requires that by January 2005 all suppliers embed passive RFID chips in each individual product if possible, or otherwise at the level of cases or pallets."[44] Most items going to Iraq or Afghanistan already require tags.[45] This deadline has been no more successful than the Wal-Mart one.[46] In a survey of DoD suppliers, 60.6% reported that they had no intention of tagging their products and 19.8% said that implementation of RFIDs was still at least a year away.[47] Maj. Gen. Daniel Mongeon announced at the RFID Summit for Industry on February 9, 2005 that the Department of Defense is still on track to have RFID implementation for the entire supply chain by 2007.[48] The government has made it a priority to track its assets efficiently.

---

[43] Houston Craig Crawford & Raphael Feldman, *The Project Group RFID Subsidiary to Develop Handheld Enabled RFID Based Evidence Tracking System for Federal, State & Local Law Enforcement Agencies*, BUSINESS WIRE, Feb. 10, 2005.

[44] VIRGINIA JOINT COMMISSION ON TECHNOLOGY AND SCIENCE (JCOTS), 2004-2005 COMMISSION WORK PLAN (May 26, 2004), *available* at http://jcots.state.va.us/Publications/Work%20Plans/workplan04.htm (last visited Feb. 19, 2005).

[45] *Pentagon Remains Committed to RFID Rollout*, COMMUNICATIONS DAILY, Feb. 10, 2005.

[46] Barlas, *supra*, note 38.

[47] Jonathan Collins, *Defense Sector May Miss Deadline*, RFID JOURNAL, Nov. 29, 2004, *available at* http://www.rfidjournal.com/article/articleview/1258/1/1/ (last visited Feb. 20, 2005).

[48] *Pentagon Remains Committed to RFID Rollout*, *supra* note 45.

C. LIBRARIES

Libraries have started to use RFIDs so that materials can be accurately tracked.[49] With the tags, books can be located within the library. This use of RFIDs also allows borrowing without going to a checkout desk. Surprisingly, more concerns are associated with libraries than almost any other situation.

For example, as mentioned above, the "kill" function that would be so beneficial for consumers in other situations does not pass the balancing test of privacy outweighing utility in this case. The purpose of using the tags would be defeated by the tremendous costs associated with disabling the tags and replacing them every time a book is checked out.

The required linking of personal information is also problematic. In order for someone to walk out the door with the book and have it recorded, identification information must be linked to the EPC associated with the book. A record would then exist as to the consumer's behavior, and potentially could track that individual any place that he or she took the book.

In response to this concern, California Senator Joe Simitian has recently introduced S.B. 682.[50] It would not allow any ID card, including a library card, to contain an RFID tag because it prohibits a "contactless integrated circuit,"[51] defined as "a data carrying unit, such as an integrated circuit or computer chip that can be read remotely."[52] However, the bill would not completely eliminate the problem, as even linking the borrowed item to a remote database where personal information is stored or connecting it to a number that resides on the card would create the potential for abuse.

Protecting privacy in libraries is complex because the reason RFIDs are used is the reason that privacy is at risk. "Silent commerce" requires that the party exiting the library can be identified so that the items he is borrowing can be linked to him. This link is the concern. Once personally identifiable information is connected to the borrowed

---

[49] American Library Association, *RFID: Radio Frequency IDentification Chips and Systems*, *at* http://www.ala.org/Template.cfm?Section=ifissues&Template=/ContentManagement/ContentDisplay.cfm&ContentID=77689 (last visited May 11, 2005).

[50] S.B. 682, 2004-05 Reg. Sess. (Ca. 2005), *available* at http://info.sen.ca.gov/pub/bill/sen/sb_0651-0700/sb_682_bill_20050222_introduced.html (last visited Apr. 2, 2005).

[51] *Id.*

[52] *Id.*

item, a pattern of behavior can be established, or the party can be tracked. Unfortunately, killing the tag is not an option, as the library would like to reuse it and replacement would be costly. Weighty arguments exist on each side of the debate.

D. CHILDREN

Recent consideration has been given to tagging and tracking elementary school children. Parents and teachers obviously have the children's best interest at heart, but there is a concern that this could change to tracking the adult population. By requiring children to carry IDs with embedded RFID tags, attendance becomes much more efficient. A missing child can immediately be located. Also, in settings where emotionally disturbed classes have trouble with escapees, the school can instantly be put on notice when someone crosses a sensor near an exit.

Cedric Laurant, policy counsel at the Electronic Privacy Information Center (EPIC) said, "[i]t treats children like livestock or shipment pallets, thereby breaching their right to dignity and privacy they have as human beings. Any small gain in administrative efficiency and security is not worth the money spent and the privacy and dignity lost."[53] For these reasons, Britton Elementary School, outside of Sacramento, has put their plan to tag the students on hold.[54]

Other organizations have not stopped tagging children. Starting in 2002, Dolly's Splash Country has made a watch-like tracking device available to those attending its water park.[55] Gene Scherrer, Director of Operations, is enthusiastic, stating

> The SafeTzone System is the premier technology of its kind in the country and we are proud to be making it available to our guests. If we can bring some added peace of mind to our guests' visit, then we have accomplished one more step in

---

[53] Alorie Gilbert, *Elementary School Nixes Electronic IDs*, CNET NEWS.COM, Feb. 17, 2005, *available* at http://news.com.com/Elementary+school+nixes+electronic+IDs/2100-1029_3-5581275.html?tag=html.alert (last visited Feb. 18, 2005).

[54] *Id.*

[55] Press Release, SafeTzone, Dolly's Splash Country Signs Agreement to Bring SafeTzone's Electronic Child Locating Services to Pigeon Forge Waterpark (Apr. 24, 2002), *available at* http://www.safetzone.com/stz_press_dolly.html (last visited Apr. 27, 2005).

> our goal of making Dolly's Splash Country the region's safest and most fun family destination.[56]

Safety is a valid balancing point to privacy concerns. The question of where to draw the line must still be answered, however.

E. SURGICAL

Hospitals can be intimidating for patients. The patient must submit himself entirely to the capable hands of another. He can feel helpless. The purpose of using RFIDs in a medical setting is to ensure that all relevant information about a patient travels with him, whether he is directly able to communicate it or not. A system developed by Zebra Technologies "embeds and prints information on an RFID 'smart' label that travels with the patient into surgery to help prevent errors."[57] The tag can list the proscribed procedures, any current medications, dosages, prior treatment, or allergies. The "smart" label acts as a traveling chart that is literally attached to the patient.

Dr. Hijzai of the University of Chicago reflects that, "[w]e also recognize the importance of RFID-based technology to enable our staff to spend more quality time with our patients and less time manually performing administrative tasks such as billing and reordering."[58] Hospitals now use RFIDs for purposes such as tracking medicine, patients, and general assets, as well as the delivery of drugs.[59] Not only are patients protected by the new system, but the hospital's assets are as well.

F. ACCESS FOR THE DISABLED

To aid the blind, Professor Jack Mottley and students at the University of Rochester have created a system similar to a CD player

---

[56] *Id.*

[57] Zebra Technologies, *U.S. FDA approves SurgiChip Solution designed to prevent surgical errors*, AGING & ELDER HEALTH WEEK 147, January 2, 2005, *available at* http://biz.yahoo.com/prnews/041119/cgf044_1.html (last visited Feb. 16, 2005).

[58] *University of Chicago Comer Children's Hospital Selects Mobile Aspects*, BUSINESS WIRE, Feb. 9, 2005, *available at* http://www.integratedsolutionsmag.com/RFID/PDFs/2005_02_10_MobileAspects.pdf (last visited Feb. 19, 2005).

[59] *Id.*

that incorporates RFIDs.[60] Tags are placed in locations of interest, such as a library.[61] The person being assisted wears the player and when he passes the tag, a pre-recorded message is transmitted through a headset.[62] By placing the tags on items, their locations can be known without visually seeing them.

Jordan Hill of Brunel University has also designed a method to help blind shoppers.[63] By using a "retail-scanning" device, they are able to determine the price, style, color, and size of the item they are considering. The shopper does not have to rely on another party to aid in the personal decision of what he would like to purchase. Personal freedom is enhanced.

IV. OUR PRIVACY IS AT RISK

There are always two sides to a debate. Many fantastic possibilities exist. Many concerns arise, as well. By marking everything a person carries, or possibly even the person himself, there is a certain loss of privacy. How the data is used once it is collected determines the extent of this privacy loss. If the data on the item is kept separate from personally identifiable information, the risk of privacy intrusion is lessened.

A. PERSONAL INFORMATION

An immense amount of information is available online or in databases due to public records and other sources. Consumers have little or no control in suppressing or editing most of it. "Paying just $26 for each person, the Foundation [for Taxpayer and Consumer Rights] obtained the [social security numbers] and home addresses of CIA Director George Tenet, Attorney General John Ashcroft, and Presidential Chief Political Advisor Karl Rove."[64] Information about

---

[60] Mead, *supra* note 7.

[61] *Id.*

[62] *Id.*

[63] Craig Hillsley, *Clothes Scanner for Visually Impaired Wins Top Award*, THE PRESS ASSOCIATION LIMITED, Sept. 14, 2003, *available at* http://www.rnib.org.uk/xpedio/groups/public/documents/publicwebsite/public_topscan.hcsp (last visited Feb. 19, 2005).

[64] Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, around n161 (2004) (referencing *Group Gets Private Data on Tenet, Ashcroft to Underscore Need for Tougher Laws*, USA TODAY.COM, Aug. 28,

almost anyone can be acquired if data about these high profile figures are so easily accessible.

RFIDs do not necessarily contain personally identifiable information. It is only after the specific identification number of a purchased item is linked to a person that the person is at risk. Some people have chosen to be tagged of their own accord. For example, the tags of hospital patients are more likely to contain personal information. Another example is the EZ-Pass system that has enabled marked cars to drive through a toll booth without stopping since 1992.[65] It is convenient, but also enables an individual to be monitored, because his or her personal information be combined with a tracking device.[66] However, this is only true assuming the person billed for the pass is the one using it.

EZ-Passes allow for real-time tracking of the card-holder. If a person owns an EZ-Pass, each time he goes by a reader, his action is recorded. Data residing on a pass is of greater concern. Outside readers may be able to scan the data if it is on the card. In either instance, personally identifiable information is linked to movement, creating a record of consumer behavior.

B. TRACKING CAPABILITY

Some religious commentators point out that Revelations 13:16-17 reads:

> And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: And that no man might buy or sell, save he that

---

2003, *available at* http://www.usatoday.com/tech/news/internetprivacy/2003-08-28-privacy-tenet_x.htm (last visited Mar. 21, 2004)).

[65] Don Flint, *Electronic Toll Collection: An Introduction and Brief Look at Potential Vulnerabilities*, SANS INSTITUTE ii, Apr. 27, 2004, *available at* http://www.giac.org/practical/GSEC/Don_Flint_GSEC.pdf (last visited Feb. 20, 2005).

[66] NATIONAL CONFERENCE OF STATE LEGISLATURES, STATE LEGISLATURES ADDRESS USE OF RFID TECHNOLOGY (excerpt from: *"News From the States," Communications, Technology and Interstate Commerce Committee Newsletter*, Summer 2004), *available at* http://www.ncsl.org/standcomm/sctech/NCSL-RFID.htm (last visited Apr. 27, 2005).

> had the mark, or the name of the beast, or the number of his name.[67]

These concerned believers have expressed that the choice to identify oneself may be the mark of the beast that is to occur before the apocalypse. An uproar occurred when Washington, D.C. implemented the use of SmarTrip Cards to use the Metro parking garages, because people were forced to identify who they were and where they were traveling in order to have access to transportation.[68] Consequently, the Washington Metropolitan Area Transport Authority has decided to amend its privacy policy so that access to the collected information is limited.[69]

RFIDs promote convenience, but at an expense of privacy if that data is combined with personally identifiable information. Systems are already available that combine these types of data. The vast amount of memory that would be required to track a person is cited as a reason that this is unrealistic. However, storage capability grows every year at an astounding rate. Further, the argument that one must be close to a reader to be scanned is not compelling, as the scanner may be secreted in a doorway or other narrow passage where a person is forced to come within read range. Therefore, many of the implemented "safeguards" are not as secure as one might hope.

V. CONSTRAINTS MAKE THE TECHNOLOGY VIABLE

In the United States, there is no explicit right to privacy, though certain areas, such as reproductive rights, have been interpreted as deserving of protection implied in the Bill of Rights.[70] Most

---

[67] Michael Kanellos, *RFID Tags: The people say no*, CNET NEWS.COM, Sept. 7, 2004, *available at* http://news.com.com/RFID+tags+The+people+say+no/2010-1039_3-5332478.html?tag=nl (last visited Feb. 16, 2005). *See also*, Revelations 13:16-17, King James Version of the Holy Bible.

[68] Letter from Cédric Laurant, Electronic Privacy Information Center (EPIC), *Comments on Washington Metropolitan Area Transit Authority's Proposed Amendments to the Public Access to Records Policy*, Feb. 14, 2005, *at* http://www.epic.org/open_gov/foia/wmata/parp_cmts-021405.html (last visited Apr. 27, 2005).

[69] *Id.* (Proposed language Section 6.1.8. provides that "All SmarTrip information [is exempted from disclosure], unless the request is made: (1) pursuant to a court order; or (2) by a law enforcement official that meets the requirements of Section 6.1 (D) of the WMATA's Privacy Policy; or (3) by the registered user of the SmarTrip card upon proof of identity for release only to that user. (...)").

[70] Roe v. Wade, 410 U.S. 113 (1973); Griswold v. Connecticut, 381 U.S. 479 (1965).

protections that consumers have acquired have been through statute or industry standards.[71] Currently, no state has passed a bill that specifically speaks to RFIDs, although many have considered possible legislation.[72]

"Some experts argue that no significant shift in U.S. policy is likely to occur until some crisis or highly publicized event forces us to look at the issue from a new perspective."[73] The events of September 11th prompted many privacy erosions. Regulations have been imposed, but often ones that the government can bypass. For instance, the passage of the USA PATRIOT Act allowed for simpler approval for wiretaps.[74] Assistant Attorney General William E. Moschella revealed that while only 1,003 warrants were approved in 2000 under the 1978 Foreign Intelligence Surveillance Act, the USA PATRIOT Act allowed for 1,754 to be approved in 2004.[75] Senator Patrick Leahy acknowledged this recently, reflecting that, "[i]n our constitutional system there is always tension between liberty and security – and never more so than since September 11th."[76] For

---

[71] Valetk, *supra* note 64 at around n156.

[72] California, Virginia, Maryland and Utah have considered statutes. *See* S.B. 1834, 2003-04 Reg. Sess. (Cal. 2004), *available at* http://info.sen.ca.gov/pub/03-04/bill/sen/sb_1801-1850/sb_1834_bill_20040614_amended_asm.html (last visited Feb. 19, 2005); *see also*, H.B. 1304, 2004 Gen. Assem., Reg. Sess. (Va. 2004), *available at* http://leg1.state.va.us/cgi-bin/legp504.exe?041+ful+HB1304 (last visited Feb. 19, 2005); *see also*, NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 66 (referencing Maryland (H.B. 32) and Utah (S.J.R. 10)); *see also*, RILA, *supra* note 21, at slides 12-16.

[73] Valetk, *supra* note 64, at n189 (referencing James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 83 (2003)).

[74] Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. III, 315, 2001 U.S.C.C.A.N. (115 Stat.) 272, 308 (to be codified at 18 U.S.C. 1956(c)(7)(B)(iv)).

[75] Mark Sherman, *Record Number of Wiretaps, Searches Approved Last Year*, AOL NEWS, Apr. 2, 2005, *available at* http://aolsvc.news.aol.com/news/article.adp?id=20050401190209990002 (last visited Apr. 3, 2005); *see also*, William E. Moschella, U.S. DEPARTMENT OF JUSTICE *Delayed Notice Search Warrants: A Vital and Time Honored Tool for Fighting Crime*, Sept. 22, 2004 (Assistant Attorney General Moschella explains the changes that have resulted because of the PATRIOT act are minimal.), *available at* http://www.lifeandliberty.gov/docs/patriotact213report.pdf (last visited Apr. 27, 2005). *See also*, Pub. L. No. 95-511, tit. I, 101, 92 Stat. 1783 (1983) (codified at 50 U.S.C. 1801-11 (1996)).

[76] Senator Patrick Leahy, The Dawn of Micro Monitoring: It's Promise, And Its Challenges To Privacy And Security, Remarks at the Conference on "Video Surveillance: Legal And

instance, as part of the new US-VISIT program, there has been discussion of imbedding RFIDs into foreign national's identification documentation in order to protect American citizens.[77] To do this, the visitors' freedoms are suppressed. The Department of Homeland Security denies that it will be inserting RFIDs in agency identification cards, however.[78] It clarified that it intends to employ wireless technology controlled by ISO 14443, rather than ISO 15693, which is commonly referred to as an RFID.[79] The difference is that the read range on an ISO 14443 tag is smaller.[80] Privacy issues are still relevant, and tracking can still occur, even if the read range is decreased.

A. CURRENT LEGISLATION

No single law specifically covers RFIDs, but many may have the potential to be expanded to protect against abuses. The Privacy Act, Identity Theft and Assumption Deterrence Act (ITADA), and the Electronic Communication Privacy Act (ECPA) all contain elements that are relevant. Clear delineation is doubtful, however. For example "no single federal law regulates how the SSN is used in the private sector."[81] The status of personally identifiable information must be determined before restrictions on its transmission, distribution, and use may be adequately enacted.

The Privacy Act requires government agencies to protect the privacy of individuals, but still allows for potential abuse of information for criminal investigations.[82] A wide exception exists for

---

Technological Challenges" (March 23, 2004), *available at* http://leahy.senate.gov/press/200403/032304.html (last visited Apr.27, 2005).

[77] Alorie Gilbert, *States to test ID chips on visitors*, ZDNET (Jan. 26, 2005), *available* at http://netscape.com.com/2100-1035_22-5552120.html (last visited Feb. 20, 2005).

[78] Jacqueline Emigh, *Homeland Security Officials Refute RFID Reports*, CIO INSIGHT, Mar. 17, 2005, *available at* http://www.cioinsight.com/article2/0,1397,1777403,00.asp (last visited Apr. 3, 2005).

[79] *Id.*

[80] *Id. See also*, R MOROZ, LTD., *supra* note 6.

[81] Valetk, *supra* note 64, at around n66.

[82] *Id. at* n65. 5 U.S.C. § 552a(8) states:

(8) the term "matching program"--

evidence gathering.[83] Hopefully, the definition of privacy might include the distribution of information after it has been collected. The above mentioned limitations regarding SmarTrip may be an example of how this might apply to the information collected by RFIDs, by restricting it to sharing only upon court or customer request.[84]

ITADA makes identity theft a federal crime.[85] The statute may apply to the possible uses of information obtained by using RFIDs because "[u]nder 18 U.S.C. § 1028(a)(7), 'means of identification' does not require the production, possession, or use of an actual identification document."[86] Consequently, a social security number or, perhaps, its association with the tracking number of a particular item, could be used as a means of identification.

One of the easier solutions would be to amend the ECPA.[87] The Act already covers interception of wireless transmissions. Such provisions could be employed to protect unauthorized persons from accessing tags. If the transmission from a tag to a reader can be deemed a "communication," it may be protected. The ECPA makes it a crime for any person who, "intentionally intercepts, endeavors to

---

(A) means any computerized comparison of--

(i) two or more automated systems of records or a system of records with non-Federal records...

(B) but does not include—...

(iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons....

[83] *Id.*

[84] Laurant, *supra* note 68.

[85] 18 U.S.C. § 1028 (2005).

[86] Valetk, *supra* note 64, at n64. (18 U.S.C. § 1028(a)(7) makes punishable one who: "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.")

[87] Reuven R. Levary, *RFID, Electronic Eavesdropping and the Law*, RFID JOURNAL, Feb. 14, 2005, *available at* http://www.rfidjournal.com/article/article view/1401 (last visited Feb. 19, 2005).

intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[88]

Personally identifiable information is valuable to companies that could make use of it for marketing purposes. If a company could identify who had bought competitors' products in the past, the company could efficiently market to those interested in its type of product. "Sample legislative proposals include bills that would prohibit the sale, purchase, or display of SSNs by governmental agencies or private companies."[89] Consumers would then be protected from potential misuse. "To be effective, however, new SSN protection laws must prevent private companies from denying goods or services to anyone unwilling to furnish their SSN."[90]

Reselling of personal information is a common phenomenon known as the "second exchange." "People disclose personal information to gain the benefits of a relationship; the benefits of disclosure are balanced with an assessment of the risks of disclosure."[91] Retailers may offer incentives to have consumers sign off on the kill provision, authorizing disclosure to third parties. In this manner, the databases may be further supplemented if there are not restrictions on use of personal information.

The Federal Communication Commission (FCC) has provided some guidance for government use of RFIDs. As the tags must transmit on the bandwidth, restrictions can be placed on its use. For instance, 47 C.F.R. § 15.240 restricts use of the tags to "commercial and industrial areas."[92] There is no restriction on the type of data that may be collected, however. The FCC does require that the grantees notify the Office of Engineering and Technology of the locations of any of the devices.[93] At least with knowledge of a reader's whereabouts, covert monitoring is not possible.

---

[88] Electronic Communications Privacy Act, 18 USC § 2511(a) (1989), *available at* http://www.usiia.org/legis/ecpa.html (last visited Feb. 21, 2005).

[89] Valetk, *supra* note 64, at n79 (referencing the Social Security Number Privacy and Identity Theft Act, S. 1014, H.R. 2036, 107th Cong. (2001)).

[90] *Id.* at n81.

[91] Mary J. Culnan & Robert J. Bies, *Consumer Privacy: Balancing Economic and Justice Considerations*, JOURNAL OF SOCIAL ISSUES, Vol. 59, No. 2, 323, 327 (2003).

[92] Intentional Radiators Radiated Emission Limits, Additional Provisions, 47 C.F.R. § 15.240 (2005).

[93] 47 C.F.R. § 15.240(f).

States have considered bills that would affect RFID use. In November, California's S.B. 1834 was dismissed from the assembly without further action.[94] The bill had potentially huge ramifications, however. The bill sought to limit use of RFIDs to actual purchases, rather than to monitor browsing behavior.[95] In earlier editions, the bill called for a kill provision and required consumer permission before sharing the collected information with a third party.[96]

Virginia has begun to consider the implications of adopting RFIDs for governmental use. In the 2004-2005 work plan for the Joint Commission on Technology and Science, the Commission recognized that "as RFID use hits the main stream, Virginia will have to determine whether and how it will utilize RFID in its procurement processes and otherwise."[97] Consequently, it considered H.B. 1304 which would require public bodies "to conduct a privacy impact analysis when authorizing or prohibiting the use of invasive technologies."[98] Invasive technologies specifically encompass RFIDs and tracking systems. Maryland and Utah have introduced similar bills, though all three bills have seemingly died.[99]

Other states have added to the possible regulations. "Two states–Missouri (S.B. 867) and Utah (H.B. 251)–have introduced legislation that would require all products containing RFID tags, to be appropriately labeled."[100] Utah also has a bill that would require stores to inform consumers about how to kill tags after purchase.[101] Further, Senator Jarrett Barrios of Massachusetts anticipates introducing a bill in 2005 that would require RFIDs to be killed at the point of sale, or

---

[94] S.B. 1834, 2003-04 Reg. Sess. (Cal. 2004), *available at* http://info.sen.ca.gov/pub/03-04/bill/sen/sb_1801-1850/sb_1834_bill_20040614_amended_asm.html (last visited Feb. 19, 2005).

[95] *Id.*

[96] Claire Swedberg, *States Move on RFID Privacy Issue*, RFID JOURNAL, Apr. 30, 2004, *available* at http://www.rfid journal.com/article/view/924 (last visited Feb. 19, 2005).

[97] JCOTS, *supra* note 44.

[98] H.B. 1304, 2004 Gen. Assem., Reg. Sess. (Va. 2004), *available at* http://leg1.state.va.us/cgi-bin/legp504.exe?041+ful+HB1304 (last visited Feb. 19, 2005).

[99] NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 66. (referencing Maryland (H.B. 32) and Utah (S.J.R. 10)); *see also*, RILA, *supra* note 21, at slides 12-16.

[100] *Id.*

[101] *Id.* (referencing Utah (H.B. 314)).

requiring retailers to obtain written consent from the consumer to keep them active.[102]

Generally, requirements that would encourage notice for consumers seem to be the preference. If people have the option of disabling a tag, or at least the knowledge of how it will affect them, they regain control of their decisions.

B. INTERNATIONAL LAW

Generally, the international community has been much more concerned with protecting their citizens' privacy. According to Interpol, however, around one hundred countries have no laws that cover computer crimes.[103] Hence, control of RFIDs outside of the United States is mixed.

The European Union has some of the highest standards for privacy and protection of personal information.

> By implementing the 1995 European Community Directive on Data Protection, the European Union mandated that all fifteen E.U. Member States ensure that citizens have the right to access their data, fix incorrect information, remedy violations, and keep their information from being used for any marketing purpose without their permission.[104]

In encouraging this philosophy, the EU has implemented provisions that require companies using RFIDs to notify customers of the presence of RFID tags.[105]

---

[102] RILA, *supra* note 21, at slide 17; *see also*, Swedberg, *supra* note 96.

[103] Valetk, *supra* note 64, at n13.

[104] *Id.* at n183 (referencing Council Directive 95/46/EC of the European Parliament and of the Council, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281)(Oct. 24, 1995)).

[105] *European Laws Require Notification about RFIDs,* PRIVACY.ORG, Mar. 7, 2005, *available at* http://www.privacy.org/archives/001487.html (last visited Apr. 2, 2005); *see also,* Laurie Sullivan, *Privacy Laws: Europe Protects Against RFID Abuses*, INFORMATION WEEK 38, Mar. 7, 2005, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=60405595&tid=13692 (last visited Apr. 2, 2005). *See also*, Foreign Intelligence Surveillance Act (FISA) Pub. L. No. 95-511, tit. I, 101, 92 Stat. 1783 (1983) (codified at 50 U.S.C. 1801-11 (1996)).

The United Nations also has standards that could cover potential misuse. The Universal Declaration of Human Rights states, "No one should 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 interferences or attacks."[106] A right to privacy is created, yet specific mandates are not in place.

India has started using RFID technology for purposes as varied as tagging buffaloes at a dairy farm or tagging clothing to streamline inventory. Yet, India is still largely unregulated.[107] Both industry and government regulations should come out in the next year, as India's Ministry of Information Technology and the National Association of Software and Service Companies (Nasscom) in New Delhi have begun considerations.[108] The European Union's requirement for protection of personal information has prompted this action.[109] The United States does not have an equivalent prohibition on exportation of information, although protection of the data is usually written into the contracts of outsourcing deals.[110]

"The provincial government of Ontario, Canada, has issued guidelines about how RFID fits with existing privacy laws, as have the governments of Portugal and Japan."[111] All of these countries have slightly altered existing privacy laws to incorporate the new technology. In Japan, recent guidelines provide that:

> 1) consumers must be notified of the presence of RFID tags; 2) consumers have the right to choose whether they want to use the tags; 3) RFID tag users must provide information about the public benefits of RFID tags;

---

[106] *Universal Declaration of Human Rights*, Article 12, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948, *available at* http://www.un.org/Overview/rights.html (last visited Feb. 18, 2005).

[107] Nitya Varadarajan, et al., *The Wired 20*, BUSINESS TODAY 72, Feb. 13, 2005.

[108] Stephanie Overby, *India to Adopt Data Privacy Rules*, CIO MAGAZINE, Sept. 1, 2003, *available at* http://www.cio.com/archive/090103/tl_data.html (last visited Apr. 27, 2005).

[109] *Id.*

[110] *Id.*

[111] Mark Roberti, *Legislation isn't the Answer*, RFID JOURNAL, July 19, 2004, *available* at http://www.rfidjournal.com/article/articleview/1031/1/2/ (last visited Feb. 20, 2005).

> 4) the Personal Information Protection Act applies when there is matching between RFID tag-related data and databases; 5) tag users must restrict their use of personal information gathered through RFID tags; 6) tag users must ensure the accuracy of the personal information recorded through RFID tags; 7) appointment of information administrators; 8) accountability and provision of information to consumers.[112]

Important features in the legislation include the focus on notice and the restriction on the use of personal information. In Portugal, similar guidelines were passed by the *Comissão Nacional de Protecção de Dados* (CNPD) in 2004.[113] These guidelines also require notice, but also specify that there must be a reasonably defined purpose for the collection of information.[114]

Canada already had protections for information in place. For instance, in Ontario, The Municipal Freedom of Information and Protection of Privacy Act has been in place since 1992.[115] The act does not apply specifically to RFIDs, but it does protect the information that could be compromised. It deals with access to databases, notice, and consent for disclosure.[116] Personal information is protected by allowing consumers to have control of the use of their data.

---

[112] PRIVACY INTERNATIONAL, PRIVACY PROFILE: PHR2004 – JAPAN, Nov. 16, 2004, *at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-83523 (last visited Apr. 27, 2005); *see also* Nihon Keizai Shimbun, June 8, 2004, *available at* http://nikkeibp.jp/wcs/leaf/CID/onair/jp/flash/312386 (in Japanese) (last visited Feb. 21, 2005)); *see also* Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan, MPHPT COMMUNICATIONS NEWS, Vol. 15, No. 6 (July 5, 2005), *available at* http://www.soumu.go.jp/joho_tsusin/eng/Releases/NewsLetter/Vol15/Vol15_06/ Vol15_06.html#2 (last visited Feb. 21, 2005).

[113] PRIVACY INTERNATIONAL, PRIVACY PROFILE: PHR2004 - THE REPUBLIC OF PORTUGAL, Nov. 16, 2004, *at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-83775 (last visited Apr. 27, 2005); *see also Comissão Nacional para a Protecção de Dados*, "*Identificação por radiofrequência*," January 13, 2004 (in Portuguese), *available* at http://www.cnpd.pt/actos/del/2004/del%20009-04.htm (last visited Feb. 21, 2005).

[114] *Comissão Nacional para a Protecção de Dados*, *supra* note 113.

[115] Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56 (2004), *available at* http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90m56_e.htm (last visited Apr. 3, 2005).

[116] *Id.*

While the United States remains substantially unregulated, foreign countries have taken a stricter stance on privacy issues. Many provisions, such as notice, choice, and accuracy checks are found in recommendations for state and federal statutes. So far, none have been adopted, and Americans receive protection through companies' compliance with international or industry standards.

C. INDUSTRY STANDARDS

Both industry and ISO standards apply to regulation of RFIDs.[117] Fortunately for consumers, standards are becoming stricter. ISO 15693 speaks to three areas: physical characteristics, radio frequency power and signal interference, and anti-collision and transmission protocol.[118] ISO 14443 and 18000-3 also are part of the controlling global standards.[119] ISO 14443 controls devices with a read range of fewer than 10 cm, while ISO 15693 controls devices with a greater range.[120] ISO 18000-3 is the controlling standard for the commonly-used 13.56 MHz tag.[121]

Concern over privacy has encouraged protection of information stored on RFID chips.[122] The risks were highlighted at the Black Hat 2004 conference where a program called RFDump was presented.[123] By using the Black Hat program, a passive RFID chip is readable to anyone within 3 feet.[124] Sue Hutchinson of EPCglobal US, an industry trade association, reassures customers that no personally identifiable information is contained on the tags that would violate Gramm-Leach-

---

[117] SUMMARY INFORMATION, *supra* note 4, at 11.

[118] Bob Scher, *ISO 15693 and What It Means for You*, *available at* http://rfidusa.com/superstore/pdf/ISO_15693.pdf (last visited Apr. 3, 2005).

[119] R MOROZ, LTD., *supra* note 6.

[120] *Id.* at 11.

[121] *Id.*

[122] Mark Willoughby, *Securing RFID Information: Industry standards are being strengthened to protect information stored on RFID chips*, COMPUTERWORLD (Dec. 20, 2004), *available at* http://www.computerworld.com/printthis/2004/0,4814,96051,00.html (last visited Feb. 21, 2005).

[123] *Id.*

[124] *Id.*

Bliley Act or the Health Insurance Portability and Accountability Act (HIPAA).[125] Only product information is available on the passive RFIDs that would be susceptible to attack by this program.[126] Such scares are likely to prompt "best practices" in the industry.

Unfortunately for consumers, industry standards are lacking in covering the use of personal information. Privacy advocates, such as the Privacy Rights Clearinghouse have voiced their concern and have requested that the Federal Trade Commission regulate the use of RFID.[127] However, no real headway has been made by either group.

D. RECOMMENDATIONS

Many privacy advocates have recommendations on how RFIDs should be handled. Most suggestions are concerned with notification and consent provisions. For example, the Privacy Rights Clearinghouse suggests that users be informed of the presence of RFIDs and when and where they are being read.[128] CASPIAN

---

[125] *Id.*

[126] *Id.*

[127] *RFID 101*, RFID GAZETTE, June 28, 2004, *available* at http://www.rfidgazette.org/2004/06/rfid_101.html (last visited Feb. 21, 2005).

[128] *Hearing on RFID and the Public Policy Void*, Before the California Legislature Joint Comm. on Preparing California for the 21st Century (posted Aug. 18, 2003) (statement of Beth Givens, Privacy Rights Clearinghouse Director), http://www.privacyrights.org/ar/RFIDHearing.htm#1 (last visited Apr. 27, 2005). Suggested guidelines:

> 1. Individuals have a right to know that products contain RFID tags. Labeling must be clearly displayed and easily understood. (Garfinkel, Caspian, AutoID)
>
> 2. Individuals also must know when, where, and why RFID tags are being read. There should be no tag-reading in secret. (Garfinkel)
>
> 3. Individuals have the right to have RFID tags removed or permanently deactivated (disabled) when they purchase products or otherwise obtain items containing RFID tags. (Garfinkel and AutoID, with the following guidelines by the PRC)
>
> • Merchants must be prohibited from coercing customers into keeping the tags "live" on the product. For example, merchants cannot tell customers that in order to return the item, the RFID tag must not be disabled. The default option - whether to disable a tag or keep it "live" - must be to disable it. In situations where the individual's preference is not known, the system must always disable the tag.

(Consumers Against Supermarket Privacy Invasion And Numbering) proposes that laws such as the Federal Food, Drug and Cosmetic Act Relating to Misbranding and the Federal Alcohol Administration Act be altered to include laws stating that a package that contains a tag must be labeled as such.[129] A consumer should be aware the he has purchased an item with a tag attached to it.

The ability to kill a tag is also a debated provision. An item should not be traceable for an indefinite period of time. If it is kept live, it crosses the line from utility to the company and infringement on privacy rights. EPIC encourages retailers to "introduce clear labeling and easy removal of tags to ensure that consumers receive proper notice of RFID systems and are able to confidently exercise their choice whether or not to go home with live RFID tags in the products they own."[130] By having the ability to kill a tag, a consumer has the choice on whether to be monitored.

• Tags, once disabled, cannot be reactivated without the explicit consent of the individual associated with the tagged item. There can be no "back-door" means to reactivate tags once they have been permanently disabled.

4. Individuals have the right to own and use inexpensive readers so they can both detect tags and permanently disable them. (PRC)

5. The individual has the right to access an RFID's stored data pertaining to him or her. (Garfinkel)

6. To those I would add number 6, the requirement of "security and integrity in transmission, databases, and system access." (AutoID)

In addition I would add a 7th point: An accountability mechanism must be established with the implementation of RFID. Industry processes and operations must be transparent. (AutoID) And individuals must know who they can contact in order to access data pertaining to them.

[129] Zoe Davidson, *RFID Right to Know Act of 2003*, CASPIAN, *available at* http://www.spychips.com/press-releases/right-to-know-bill.html (last visited Apr. 2, 2005).

[130] Electronic Privacy Information Center (EPIC), Comments submitted in consideration of the Article 29 Data Protection Working Party "Working Document on Data Protection Issues related to RFID Technology," Jan. 19, 2005, *available at* http://www.epic.org/privacy/rfid/comments_art29.pdf (last visited Apr. 27, 2005). Suggested guidelines for retail applications:

(1) Consumers should be notified when RFID tags are present in what they're buying;

(2) RFID tags should be disabled by default at the checkout counter;

(3) RFID tags should be placed on the product's packaging instead of on the product when possible; and

Finally, access to one's own information is discussed by privacy advocates. Access is necessary to prevent an incorrect record. The ability to view and change one's information is included in what are generally known as fair information practices. Companies should be aware of the maintenance that is necessary for their databases. Paula Breuning of the Center for Democracy and Technology testified that, "[i]f consumers are to accept the use of this technology, it is critical that they have assurances that information collected through RFID is managed and used in a responsible fashion."[131] Therefore, provisions must be made so that inaccurate information can be corrected and removed.

Many privacy concerns involve the unaware consumer. Through notification of an RFID's presence, the opportunity to disable it, and the chance to correct information that has been collected, the risks can be limited so that they do not outweigh the benefits.

---

(4) RFID tags should be readily visible and easily removable.

[131] *Hearing on Radio Frequency Identification (RFID) Technology* Before the Subcomm. on Commerce, Trade, and Consumer Protection, the House Committee On Energy and Comm. (July 14, 2004) (statement of Paula J. Bruening, Staff Counsel, The Center of Democracy & Technology), *available at* http://www.cdt.org/testimony/20040714bruening.pdf (last visited Apr. 27, 2005). Suggested guidelines:

- *Notice:* Information collection and use should be open and transparent.

- *Purpose specification:* Personal data should be relevant to the purposes for which it is collected.

- *Use limitation:* Data should be used only for the purpose for which it was collected.

- *Accuracy:* Personal data should be accurate, complete, and timely.

- *Security:* Personal data should be protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification or disclosure.

- *Access:* Individuals should have a right to view all information that is collected about them to correct data that is not timely, accurate, relevant or complete.

- *Accountability:* Record keepers should be accountable for complying with fair information practices.

VI. CONCLUSION

Law in the United States does not adequately protect consumer privacy rights. The market is also not likely to provide protection for the consumers. Consumers may be willing to sell their personal information on the secondary market because they do not realize the potential for misuse by third parties. Legislation should dictate notice, at a minimum, and perhaps adopt kill standards or opt-out provisions. Restrictions should be placed on when, or if, personally identifiable information can be linked to data gathered by the systems. Finally, companies should keep their databases containing consumer information and product information separate so that the utility they receive from tagging an item in the supply chain is not outweighed by their consumers being tracked indefinitely through the item in the future.