Draft

A NEW CHALLENGE TO PRIVACY MANAGEMENT:

ADAPTING FAIR INFORMATION PRACTICES TO RADIO FREQUENCY IDENTIFICATION TECHNOLOGY

By

Gal Eschet

May 2004

Table of Contents

"Technology by itself doesn't violate our privacy... It's the people using this technology and the policies they carry out that create violations"[1]

INTRODUCTION

Radio Frequency Identification ("RFID"), like many other technologies, is a two-edged sword. On the one hand, this automatic identification technology, has frequently been lauded in the media, in the last couple of years, as the technology that would enable entirely unobstructed visibility into the supply chain,[2] and would dramatically streamline inventory and cut down on theft, administrative errors and, most significantly, on industry's costs.[3] Retail giants and manufacturers, including Wal-Mart, Tesco, Proctor &

▪ Post-graduate researcher, Center for Information Technology Research in the Interest of Society (CITRIS), University of California, Berkeley; *LL.M.*, UC Berkeley, School of Law (Boalt Hall), 2004; *LL.B.*, University of Haifa, 2002; *B.A.* (Econ.), University of Haifa, 2002. This paper is based on the LL.M. thesis submitted to UC Berkeley, School of Law, in partial fulfillment of the requirements for the degree of Master of Laws. I wish to express my deep appreciation to my thesis advisor, Professor Pamela Samuelson, for her instructive guidance and academic advice, comments, and assistance in focusing this topic and developing and completing this paper. My thanks also extend to the National Science Foundation for having provided the funding that enabled my research that allowed me to produce this paper (Grant No. EIA-0122599). I also wish to thank Michael Birnhack for providing helpful comments on earlier drafts of this paper. Last but not least, I would like to thank my wife, Yael Bregman-Eschet, both for her excellent comments on this paper and for her constant love and support. Any inaccuracies are, of course, my responsibility. For questions or comments, please email me at Gal@berkeley.edu.

▪▪ All Internet citations were current as of May 20, 2004.

[1] SIMSON GARFINKEL, DATABASE NATION, 4-5 (2000).

[2] The term "supply chain" includes manufacturing, distribution, and retail operations.

[3] For example, Sanford C. Bernstein & Co., a New York investment research house, estimates that Wal-Mart could save over $8.35 Billion per year when RFID is fully deployed throughout its supply chain and in stores (followed by a 40 percent increase in Wal-Mart's earnings per share): $6.7 Billion from reducing labor costs by 15 percent as a result of eliminating the need to have people scan bar codes on pallets and cases in the supply chain and on items in the store; $600 Million from using smart shelves to monitor on-shelf availability; $575 Million from reduction in employee theft, administrative error, and vendor fraud; $300 Million from better tracking of the more than 1 billion pallets and cases that move through Wal-Mart's distribution centers each year; and $180 Million from the possible reduction in inventory due to the improved visibility of what products are in the supply chain in Wal-Mart's distribution centers and its suppliers' warehouses. *See* Mark Roberti, *Analysis: RFID - Walmart's*

Gamble, Philips Semiconductors, and Gillette, in one accord with the United States Department of Defense, have endorsed RFID technology and announced major initiatives to increase the use and deployment of RFID tags, especially in the retail environment.[4] These enterprises are not surprising since RFID has some great applications and advantages both for the industry and the public—a portion of which includes inventory management, access control, equipment and personnel tracking, livestock tracking, library books checkout, and pharmaceuticals monitoring. On the other hand, RFID carries less glamorous prospects for the other end of the supply chain – the individual level. RFID technology raises consumer privacy issues both in, and outside of, the retail surroundings. Not only are there extended capabilities of data collection furnished by RFID technology, a new threat of tracking individuals has appeared. Some players in the industry have acknowledged the privacy concerns and have pushed towards the development of suitable technologies to address them. Nonetheless, inherent drawbacks and flaws in those Privacy Enhancing Technologies make it impossible, at least at this stage of development, for the technologies to independently provide a satisfactory response to the privacy concerns. This is not to say that Privacy Enhancing Technologies are not necessary. On the contrary, these technologies do play an important role in

Network Effect, CIO INSIGHT (September 15, 2003), *at* http://www.cioinsight.com/article2/0,1397,1455103,00.asp.

[4] For instance, Wal-Mart required its top 100 suppliers to affix RFID tags to cases and pallets of products that they ship to Wal-Mart's warehouses and distribution centers, by 2005; *See* Richard Shim, *Wal-Mart to Throw Its Weight Behind RFID*, CNET NEWS.COM (June 5, 2003), *at* http://news.com.com/2100-1022_3-1013767.html?tag=rn. Similarly, the United States Department of Defense required all of its suppliers to use passive RFID tags on all cases and pallets of practically all the merchandise that is purchased by the United States military, by 2005; *See* Bob Brewin, *Defense Dept. Orders Its Suppliers to Use RFID Tags by 2005*, COMPUTERWORLD (October 8, 2003), *at* http://www.computerworld.com/mobiletopics/mobile/story/0,10801,85869,00.html. Moreover, computer and software giants like I.B.M., Microsoft, Oracle and Sun Microsystems have begun marketing products and services designed to help manufacturers and retailers gather and store data that RFID tagging is expected to generate; *See*, for example, Paul Krill, *Microsoft Eyes RFID opportunities*, INFOWORLD (April 5, 2004), *at* http://www.infoworld.com/article/04/04/05/HNmicrfid_1.html.

strengthening consumers' information privacy; yet, in order to achieve adequate privacy protection, industry's behavior should not only be directed by technology, but must also be regulated otherwise. Accordingly, several proposals for RFID legislation have already begun germinating across the United States.[5] This paper will argue that at this point, legislation or other governmental regulation are not yet warranted, as it may deny businesses and consumers of the benefits of the technology. Hence, it would be advisable for firms that wish to prevent these kinds of preemptive rules from taking place, to embrace self-regulation measures.[6] For this purpose, existing self-regulation policies, known as Fair Information Practices, offer a good baseline, but cannot be adopted in their present form to RFID technology.

This paper attempts to assess what fair information practices are to be adopted and how some of the existing principles should be modified to better deal with the unique privacy concerns posed by RFID technology. The corollary of this assessment provides that a new set of principles of fair information practices should be adopted and that it should include a new prohibition regarding the usage of RFID technology for the purpose of tracking individuals; while also adjusting the important principles of notice and choice. Furthermore, proper education of customers with respect to the risks and benefits of the technology is especially important and shall serve to reinforce the firmness and authenticity of the principles of notice and choice.

---

[5] Such legislations have recently been initiated in California (S.B. 1834), Missouri (S.B. 867), and Utah (H.B. 251); *See infra* note 109 for further details.

[6] If firms want to precede federal legislation proposals, they should act rather quickly. Democratic Senator Patrick Leahy has already suggested that RFID technology may need to be regulated at the federal level and called for a congressional hearing on the technology; *See* U.S. Senator Patrick Leahy, *The Dawn of Micro Monitoring: Its Promise, and Its Challenges to Privacy and Security*, Conference On "Video Surveillance: Legal And Technological Challenges," Georgetown University Law Center, March 23, 2004, *available at* http://www.leahy.senate.gov/press/200403/032304.html.

Part I begins with a brief review of the evolution of information privacy towards its current conflict with RFID technology. Next, it provides a concise overview of RFID technology, followed by an examination of the unique threats to information privacy that it poses. *Part II* examines different modes of regulation—market, technology, norms, and law—and their potential role in regulating the use of RFID technology. *Part III* explores the major technologies that were developed explicitly to address the privacy concerns stemming from the usage of RFID systems. This part demonstrates the weaknesses of these privacy enhancing technologies and their inability, on a stand alone basis, to provide adequate protection for consumers' privacy. In light of this finding, *Part IV* focuses on the advantages of the self-regulation approach, as compared to legislation, in complementing the protection offered to privacy by the privacy enhancing technologies. It then surveys the two comprehensive privacy guidelines that were set forth by the Education & Welfare's Advisory Committee on Automated Personal Data Systems of the Department of Health, in 1973, and by the Organization for Economic Cooperation and Development, in 1980. These guidelines served as the basis for all later developments of principles of fair information practices, and the first initiatives to form such principles in the domain of RFID. *Part V* probes the suitability of these existing principles to RFID technology. It concludes that the current form of fair information practices should be adapted and tailored to the distinctive characteristics of RFID technology and its repercussions. Accordingly, *Part VI* lays down ten RFID-customized principles of fair information practices that could serve as the foundations of a strong privacy policy with respect to the usage of RFID tags, hopefully to be adopted by the industry.

I. RFID and the Danger to Consumers' Information Privacy

1. Information Privacy to Collide with RFID

The evolution of the right to privacy parallels the development of the humanist tradition. The foundations for the legal recognition of privacy and the borders between the public and private spheres of social lives date back to Ancient China and Ancient Greece.[7] Such rights are also recognized in the *Mishnah*, the code of the Jewish law compiled in the second century of the Common Era.[8] Common law has adopted privacy[9] as a principle of the individual's expectation to full protection in maintaining a personal sphere, free from outside interference; or as articulated by Samuel D. Warren and Louis Brandeis in 1890, the right of privacy is "the right [of the individual] to be let alone."[10] As common law grew to meet the demands of society, it has been found necessary from time to time to redefine the nature and scope of such protection. In general, at first the law gave remedy only for physical interference with life and property. Gradually, there also came recognition of humans' spiritual nature, feelings and intellect.[11]

The modern society, in which we live today, is characterized by the existence of an immense amount of information. Modern western societies have developed a new

---

[7] *See* CÉDRIC LAURANT, ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS, Overview chapter (2003), *available at* http://www.privacyinternational.org/survey/phr2003/overview.htm#ftnref20.

[8] The *Mishnah (Baba Batra 3:7)* states: "In a shared courtyard, a man should not build a door facing another person's door nor a window facing another person's window. If it is small, he should not enlarge it."

[9] The English words "private" and "privacy" come from the Latin *privatus*, meaning "withdrawn from public life, deprived of office, peculiar to oneself."

[10] Samuel D. Warren and Louis Brandeis, *The Right to Privacy*, 4 *HARVARD LAW REVIEW* 193 (1890).

[11] MADELEINE SCHACHTER, INFORMATION AND DECISIONAL PRIVACY, 9 (2003).

version of privacy, known as "Information Privacy." Information privacy—the ability to control information about oneself—is one of the defining concerns of the American public at the beginning of the 21st Century.[12] This concern has become relevant especially because modern culture emphasizes reliance on extensive information for important personal, commercial, and governmental decisions.[13] A central feature of information privacy is the notion of independent determination of the circumstances, under which personal information may be divulged, and the scope and nature of such disclosures.[14] Naturally, there is an inherent tension between society's need for information and the individual right to privacy.[15] The most publicized debate over privacy in our time, the Internet age, has concerned the collection and use of consumer information by commercial website operators. Yet, the privacy concerns do not stop there. As new data collecting technologies emerge onto the marketplace, new challenges of protecting our privacy are imposed on us. Such challenges are derived from the cutting-edge technology of RFID tags.

Information privacy signifies a shift of the focal point from protected interests correlated to confidentiality, like protected secrecy and spatial zones of privacy, to control over personal information and the allocation of rights with respect thereto. The centrality of control, today, entails a need to define what treatment should be conferred to

---

[12] ALAN CHARLES RAUL, PRIVACY AND THE DIGITAL STATE: BALANCING PUBLIC INFORMATION AND PERSONAL PRIVACY, 1 (2002).

[13] RAYMOND T. NIMMER, INFORMATION LAW, volume 1, chapter 8, p. 3 (2003)

[14] SCHACHTER, *supra* note 11, p. 199.

[15] "The right to receive information and ideas, regardless of their social worth… is fundamental to our free society", *Stanley v. Georgia*, 394 U.S. 557, 564 n.8 (1969).

personal information by governments, private entities, and individuals.[16] This concept manifests itself in the formation of principles of fair information practices—a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. Fair information practices exist for already three decades; the discussion in this paper explores their pertinence to the modern applications and uses of RFID technology. However, prior to arguing for the necessity and the proposed modification of these principles in the context of RFID, it is important to be knowledgeable of the characteristics of the technology that ultimately shape the risks to information privacy and the ways to deal with it.[17]

2. The Technology

RFID is an automatic identification technology, similar in concept to bar code. An RFID tag consists of a small integrated circuit attached to miniature antennae, capable of transmitting a unique serial number to a reading device in response to a query. Most RFID tags are passive: they are battery-less and obtain the power necessary to operate from the query signal itself.[18] These passive tags can transmit their identification number a distance ranging from a few millimeters to several meters, depending on their power consumption. Tags can also be active, meaning that they are equipped with a power

[16] NIMMER, *supra* note 13, at chapter 8, p. 8.

[17] For a detailed description of RFID technology, listen to Matt Ream, *RFID Webinar*, *at* http://www.rfid.zebra.com/RFID_webinar.html.

[18] Ari Juels, Ronald L. Rivest and Michael Szydlo, *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, p. 1, *at* http://theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.pdf.

source for sending their responses,[19] and they can be read over distances of several tens of meters.[20] Basically, RFID is a non-contact, non line of sight technology that uses radio waves,[21] such that the automatic identification is based on electronic tags that are embedded in the product, and are read using a wireless transceiver and not printed-on optical patterns that are read with an optical scanner.[22] Moreover, RFID tags can be read through fabric, paper, cardboard and other materials that are transparent to the frequency of operation. This makes the technology very well suited for harsh environments (environments where it is hard to get a good read on a bar code) and environments where a lot more functionality is needed from an automated identification system or an automated data collection system, as well. Every RFID tag has an identification number. The identification number is unique to a given tag. It includes not only the traditional information contained in a printed barcode (indicating manufacturer and product type),[23] but also a unique serial number for that tag, meaning that each product or item will be uniquely identified.

The core technology has been around since the 1940's; and was employed, for instance, in military applications by the British, who used RFID signals to confirm the

---

[19] Active tags sometimes have some data logging capabilities, such as monitoring temperature or pressure or shock.

[20] There is also a gray area of battery system passive tags, often referred to as "semi-active tags." These tags use an embedded battery to power the electronics, but still employ passive response such as radio frequency backscatter for uplink from the tag to the reader. *See* Simson Garfinkel, *Adopting Fair Information Practices to Low Cost RFID Systems*, p. 1, *at* http://www.simson.net/clips/academic/2002_Ubicomp_RFID.pdf.

[21] Depending on the locality (Europe, U.S., etc.) and mainly on the application, RFID systems typically operate in the frequencies of 9-135 kHz, 13.56 MHz, 868-870 MHz, and 902-928 MHz.

[22] Garfinkel, *supra* note 20, p.1.

[23] The Universal Product Code (UPC) / European Article Number (EAN) bar code, which is present on most consumer items sold worldwide, is one of the most commonly used automatic identification systems today; more than 5 billion UPC/EAN codes are scanned worldwide on a daily basis. *See* Garfinkel, *id.* This data illustrates the great potential for RFID deployment in the retail environment.

identity of their own aircraft in flight during World War II.[24] Much of the early RFID technology started to get commercialized in the 1980's, when microchip-based RFID tags appeared in the consumer markets. Their first uses were in access systems for office buildings and toll roads. Lately, the technology has grown and improved, and consequently countless new applications have materialized. These applications include: prevention of counterfeiting of consumer goods;[25] pinpointing location of theft;[26] library book check-out;[27] tracking passenger bags in airports;[28] residential garbage collection;[29] sensitive document tracking;[30] asset management;[31] equipment and personnel tracking in

---

[24] Jack M. Germain, *RFID Tags and the Question of Personal Privacy*, TECHNEWSWORLD, *at* http://www.technewsworld.com/perl/story/32161.html.

[25] Even if the counterfeit good also contains an RFID tag, the serial number in the tag will not be registered as a genuine article. *See* Garfinkel, *supra* note 20, p. 3.

[26] For example, by determining that a certain number of packages were scanned leaving a warehouse and were not subsequently scanned when loaded in a shipping dock.

[27] The library activities that can benefit from tagging library collection include: circulation of books and other items, ensuring that items are properly located in the collection, and adding items to library's collection. The usage of RFID tags in libraries will definitely reduce labor costs of staffing circulation desks. *See* Karen G. Schneider, *RFID and Libraries: Both Sides of the Chip*, *at* http://www.senate.ca.gov/ftp/SEN/COMMITTEE/STANDING/ENERGY/_home/11-20-03karen.pdf. The San Francisco, Seattle, Santa Clara and Berkeley Public Libraries are among the libraries across the U.S. that have recently decided to adopt RFID systems; *see* Ron Harris, *SF Library Wants to Track Books with Computer Chips* (October 3, 2003), USA TODAY, *available at* http://www.usatoday.com/tech/news/internetprivacy/2003-10-03-sf-library-rfid_x.htm, and Joe Garofoli & Pamela J. Podger, *Ethics of Library Tag Plan Doubted Privacy Advocates Skeptical of Tracking via Computer Chip* (October 6, 2003), SAN FRANCISCO CHRONICLE, p. A-15, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/10/06/BA255441.DTL. The Berkeley Public Library has stepped forward and published best practices policy for using the technology in the library; *see* http://berkeleypubliclibrary.org/BESTPRAC.pdf.

[28] McCarran International Airport in Las Vegas will be the first facility in the world to use RFID technology to tag luggage airport-wide; *see Las Vegas Airport Bets on RFID*, RFID JOURNAL (November 6, 2003), *at* http://www.rfidjournal.com/article/articleview/643/1/1.

[29] According to an experiment conducted by Motorola in San Jose, California, residents will be able to pay tax by the weight of their garbage. RFID tags were put on residents' garbage cans. The garbage tracks were installed with automatic loading devices that have an RFID reader and a weight scale embedded in them. The RFID tag was read when the lift was hoisted. Essentially the data is collected without intervention of the operator, making it very efficient.

[30] *CrossID*, an Israeli startup, has developed an innovative, chipless RFID system that can protect sensitive documents, such as intelligence agency reports, financial securities and banknotes. Tiny chemical particles can be embedded in or printed on paper; then, readers can be placed inside copy machines to prevent unauthorized copying. One application would be to require that any document printed on

hospitals;[32] parcel and post management;[33] livestock management;[34] inmate and guard tracking systems for prison security management;[35] parking permits;[36] tire pressure monitoring;[37] and pharmaceutical labeling for monitoring of location, expiration, and

---

CrossID's special paper be photocopied onto the same type of paper. That way, an intelligence agency, financial institution or even a company wanting to protect its intellectual property could prevent unauthorized people from copying documents. Similar applications were developed by *Inkode* using tiny aluminum fibers. *See Firewall Protection for Paper Documents*, RFID JOURNAL (February 11, 2004), *at* http://www.rfidjournal.com/article/view/790/1.

[31] For example, by putting RFID tags on things like personal computers and installing a tracking check-out/check-in system - an alarm will sound if an item with an RFID tag leaves a building through a gate, without first being logged in.

[32] *See Equipment Tracking in Hospitals*, *at* http://www.activewaveinc.com/applications_hospitals.html.

[33] The United States Postal Service, which handles billions of pieces of mail annually, is considering putting RFID capabilities on postage stamps, in order to track and locate mail much more quickly and to boost the efficiency of its operations; *see RFID Streamlines Processes, Saves Tax Dollars*, *at* http://www.sun.com/br/government_1216/feature_rfid.html.

[34] Embedded dog tags and ear tags on cows are already in use today. These tags serve to identify the animal and give instant information about its medical records, shots and drugs history. *See* Bob Brewin, *Industry and government have plans for nationwide cattle ID system, but funding is lacking*, COMPUTERWORLD (December 29, 2003), *at* http://www.computerworld.com/mobiletopics/mobile/story/0,10801,88625,00.html. Farmers have started putting RFID meters in cow feeding and drinking stations in dairy farms. By putting RFID tags in the feed station they know how much food the cow has ingested that day, and they can also track that against the milk output, in which case they would have an RFID meter at the milk station, as well. They can figure out which cows are their best performances; they can change food mix; and even use it for breeding instances.

[35] The system, called PRISM RFID, was developed by *Technology Systems International, Inc.* and leased, *inter alia*, to Calipatria State Prison in California. With this system, inmates and guards wear miniature RFID transmitters in a tamper-proof wristband. The guards' transmitter has an additional "man down" button. Each transmitter broadcasts a signal every two seconds to readers throughout a prison. The signals identify and track everyone in a facility through a computer network displaying real-time location of the entire prison population and recording this information in a permanent database. The system not only protects correctional officers, it reduces prison costs. Since inmates know they can be placed at the scene of an incident, the system reduces property damage, inmate violence and escape attempts. Description of the system is available on the website of Technology Systems International, Inc. *at* http://www.tsilink.com; also, *see Financing for RFID Prison System*, RFID JOURNAL (December 31, 2002), *at* http://www.rfidjournal.com/article/articleview/241/1/1.

[36] The Parking and Transportation Services of the University of Arizona is already using RFID technology for gate monitoring purposes: Instead of a traditional parking permit, a small RFID device is attached to the inside of the vehicle windshield; the driver just drives up to the gate, stops briefly and the gate automatically opens; *see* http://parking.arizona.edu/permits/rfid.php.

[37] Philips Semiconductors, Texas Instruments and others have developed an RFID chip for directly measuring vehicle tire pressure. The benefit of this system is obvious: the tag warns the driver when a tire is significantly underinflated, thus helping to avoid accidents due to underinflated tires. *See RFID Chip to Monitor Tire Pressure*, RFID JOURNAL (October 17, 2002), *at* http://www.rfidjournal.com/article/view/93/1/1.

anti-counterfeiting; [38] Other, very controversial, applications involve RFID tags implantable in human beings. The potential uses of such tags are their subdermal implantation in children as an anti-kidnapping device (such service was launched in Mexico), scanning unconscious patients to obtain their medical records, and restricting access to high-security buildings by scanning workers to verify their clearance.[39] [40] Yet, the most common use of the technology today, around which most of the current debate is taking place, is retail security and supply chain[41] and inventory management.[42]

---

[38] The FDA is looking at putting RFID tags into pharmaceutical labels. The aim is to be able to find exactly where on the shelf a drug is, how long it has been there, and also to prevent counterfeiting of drugs. *See Combating Counterfeit Drugs, A Report of the Food and Drug Administration* (February, 2004), *at* http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html.

[39] *Applied Digital Solutions, Inc.* has recently introduced "VeriChip," a rice-size microchip that is injected beneath the skin to be used for the indicated applications. *See* Julia Scheeres, *Tracking Junior With a Microchip* (October 10, 2003), WIRED NEWS, available at http://www.wired.com/news/technology/0,1282,60771,00.html.

[40] According to various publications, it is claimed that the United States Department of Health and Human Services has recently announced that it was about to begin a pilot program, named Homeless Management Information System (HMIS), designed to closely monitor the nation's homeless population. Under the pilot program, homeless people in participating cities will be implanted with mandatory RFID tags that social workers and police can use to track their movements. *See* Declan McCullagh, *HHS announces program to implant RFID tags in homeless*, POLITECH (April 1, 2004), *at* http://politechbot.com/pipermail/politech/2004-April/000573.html and Electronic Privacy Information Center, *Homeless Tracking Fact Sheet*, *at* http://www.epic.org/privacy/poverty/hmisfactsheet.pdf.

[41] The Auto-ID Center, headquartered at the Massachusetts Institute of Technology, has developed the *Electronic Product Code (EPC)*, which is a unique number, stored on an RFID tag, which identifies a specific item in the supply chain. Once the EPC is retrieved from the tag, it can be associated with dynamic data such as from where an item originated or the date of its production. EPCglobal, Inc., a non-profit joint venture between EAN International and the Uniform Code Council (UCC), was entrusted by industry to support the EPC Network as the "global standard for immediate, automatic, and accurate identification of any item in the supply chain of any company, in any industry, anywhere in the world." For further information about the organization *see* http://www.epcglobalinc.org/index.html. An auxiliary project, developed by the Auto-ID Center, is the *Object Name Service (ONS)*, which provides a global lookup service to translate an EPC into one or more Internet URLs where further information on the object may be found; *see Auto-ID Object Name Service (ONS) 1.0* (working draft, edited by Michael Mealling, August 12, 2003), *at* http://www.epcglobalinc.org/standards_technology/Secure/v1.0/WD-ons-1.0-20030930.pdf.

[42] In a trial conducted in Spain, Proctor & Gamble found that RFID tags embedded in reusable pallets, can boost throughput at its transport docks – pallets could be loaded 40 percent faster into containers when using RFID tags as opposed to bar codes.

3. The Threats to Privacy

Although RFID technology offers great opportunities both for businesses and consumers,[43] it holds in store acute and grim privacy concerns. However, the reader should keep in mind that, at present, the threats to consumers' privacy are not as intimidating as the reader may perceive from the following paragraphs. A slew of major technical and cultural hurdles impede the progression of RFID into the mainstream, and make some of the risks that RFID technology inflicts on privacy, speculative and hypothetical today. Besides the problem of a very limited read range of today's tiny tags, one main obstacle involves the physical conditions in the typical warehouse and shipping environment, such as the presence of metal, liquids and competing radio transmissions that can interfere with RFID signals. Other factors that impede the deployment of the technology are the relatively high costs of RFID systems, particularly the tags;[44] and the lack of sufficient industry standards that will allow various systems to work together smoothly.[45] There are also political hindrances in the form of labor unions that object to

---

[43] RFID applications that mainly benefit consumers are, for example, compliance monitoring of medication dosage in elderly people and Alzheimer patients (an RFID reader could note if a medicine bottle is taken out of a cabinet), and automatic replenishment of refrigerators and pantries. *See* Garfinkel, *supra* note 20, p. 3.

[44] Simple passive RFID tags alone cost 25 cents to 30 cents each. Analysts contend that for many users the price needs to fall to 5 cents or less before the investments can be recovered; *See* Barnaby J. Feder, *Wal-Mart Hits Snags in Push to Use Radio Tags to Track Goods*, THE NEW YORK TIMES: TECHNOLOGY, *available at* http://www.nytimes.com/2004/03/29/technology/29radio.html?ex=1082433600&en=a4bd4214bff22885&ei=5070. On the other hand, some voices call for immediate deployment of RFID systems and claim that firms will benefit from deploying the tags even at their present prices; *See* Mark Roberti, *Tag Cost and ROI*, RFID JOURNAL (February 16, 2004), *at* http://www.rfidjournal.com/article/articleview/796/1/2.

[45] There is some effort today to place some standards into the RFID technology. The biggest and most readily available standard for RFID applications is the *ISO 15693*. It is an international technical standard that defines how a reader talks to a tag. The *ISO 14443* standard has also been around for a while and is now starting to be used in smart labels (*i.e.*, low-cost packaging and product identification labels that are laminated with RFID-enabled paper or plastic layers that give the labels the ability to interact with RFID readers). This standard spells out a little more security in RFID, and was invented for financial transactions. A new standard which is in the process of being ratified is the *ISO 18000*,

warehouse and shipment workers' livelihoods being automated away by computers.[46] Yet, society has learned a lesson from computerization—that is that technologies never stand still. Any socially responsible technology policy must anticipate how RFID technology shall widespread throughout society and grow in power;[47] and therefore should take into consideration all reasonably foreseeable uses and threats to privacy.

Many technologists and privacy advocates vision a dystopian digital future, in which RFID tags are attached to all existing goods; the tags can be found anytime via RFID readers and the networked database system, and they can be managed through out their life cycle.[48] If RFID technology is deployed without adequate regard for its social and political implications, the scene from Steven Spielberg's 2002 movie *Minority Report* (starring Tom Cruise), in which commercial advertisements were pitched to individuals by name and consumer profile, may seem plausible. In such a ubiquitous computing world with wide-scale deployment of RFID tags, the potential for widespread dissemination, misuse, unauthorized access, and disclosure of personal information[49] of

---

which covers a broad range of technologies and will essentially incorporate the functions and features that are contained within the *ISO 15693* standard. Additionally, the Uniform Code Council (UCC) is proposing the *GTAG* standard. This is a global tag standard for global tagging of containers and pallets. It would allow the technology to be used in a standard way for a wide variety of logistics applications. For more information on the standardization of RFID technology, *see* http://www.insidefr.com/pdf/ISO Standards.pdf and http://www.rfid-handbook.de/rfid/standardization.html.

[46] *See* Alorie Gilbert, *Retail takes stock of radio tags,* ZDNET (September 8, 2003), http://zdnet.com.com/2100-1103-5071569.html?tag=nl.

[47] *See* Lee Tien, Electronic Frontier Foundation, *Letter to San Francisco Public Library: Privacy Risks of Radio Frequency Identification "tagging" of Library Book*, (October 1, 2003), *at* http://www.eff.org/Privacy/Surveillance/RFID/20031002_sfpl_comments.php.

[48] Sozo Inoue and Hiroto Yasuura, *RFID Privacy Using User-controllable Uniqueness*, *at* http://www.rfidprivacy.org/papers/sozo_inoue.pdf.

[49] Personal identifying information generally includes such information as name, postal address, email, phone or fax number, credit card number or Social Security number. Non-identifying information includes information, such as age, gender, income, education level, hobbies, and interests, which *alone* (*i.e.*, when not combined with other information) cannot be used to locate or identify individuals. Similarly, "Personal Data" is defined in article 2(a) of Directive 95/46/EC of the European Parliament

individuals would increase exponentially. As a result, the technology will grow to be a threat to individuals' privacy which is second to none, and may imperil rendering a society nearly devoid of privacy.

Almost all American shoppers today carry several shopping cards in their wallets. Based on that fact, data collectors claim that there is general willingness to trade one's personal demographics in exchange for supermarket discounts, contest entries and the like, and consequently, privacy is usually not an issue because consumers agree to waive this right. In other words, the industry's representatives argue that there is a growing perception of the public that the greater need for information and the proliferation of computerized systems would ultimately mean a reduction in the power of individuals to control the personal information collected and stored about them,[50] and more specifically that modern consumers do not have confidence or expectations that the personal information they leave behind will remain confidential, hence their voluntary compliance is an adequate protection.[51] In other words, they argue that we are in the midst of a mindset transformation, in which consumers realize that giving up data is in their interest.

---

and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, as follows: "*personal data* shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[50] Directorate for Science, Technology and Industry & Committee for Information, Computer and Communications Policy, *Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet*, p. 5. The report can be viewed at http://www.oecd.org/dataoecd/33/43/2096272.pdf.

[51] Robert Ellis Smith, *Consumer Privacy in the 108th Congress* in CONSIDERING CONSUMER PRIVACY, A RESOURCE FOR POLICYMAKERS AND PRACTITIONERS, *Center for Democracy & Technology* (March 2003) p. 3, *at* http://www.cdt.org/privacy/ccp/ccp.pdf.

On the other hand, we should take into account that the average shopper is usually unaware of all the potential uses and privacy violations regarding his personal information. Therefore, the so-called willingness to trade personal information can frequently not be the true free will of a well-informed consumer. Moreover, the proponents of intensive data collection may face particular difficulties raising their argument when it comes to RFID tags.

RFID tags possess new and bigger privacy threats, beyond the mere collection of personal information. First, tags could be read by unauthorized readers,[52] and as humans are not sensitive to radio signals, the tags would be read covertly. Thus, for instance, a pervert can possibly inventory the undergarments of people in close proximity and a cutpurse can surreptitiously scan the contents of pedestrians' hand bags in order to know who is a more "lucrative victim." Second, the communication between the reader and the RFID tag could be secretly monitored, resulting in similar threats to privacy. The main concern about RFID tags seems to be that it may enable third parties to track individuals by their possessions (*e.g.*, books, shoes,[53] or clothes).[54] After the RFID tag is attached to a product and its consumer is set to be related in a point-of-sale system, the product can be traced by RFID readers, leading to a violation of the consumer's privacy as he or she

---

[52] While tags that use radio frequency of 13.56 MHz cannot be read from more than a meter away, unshielded passive 915 MHz tags can be read from many meters. *See* Garfinkel, *supra* note 20, p. 3.

[53] In a successful tracking experiment, all of the official entrants in the 2004 Boston Marathon were issued a "ChampionChip," a small token that is tied onto the runner's shoe. The chip contains RFID technology, and as a runner crosses stationary mats, located throughout the race, the chip transmits the runner's time through RFID readers to certain databases. The runner's time and location are then delivered to his pre-indicated family members and friends. *See* Liane Cassavoy, *Boston Marathon Gets Wired*, PC WORLD (April 16, 2004), *at* http://www.pcworld.com/news/article/0,aid,115719,00.asp. Although in this case the tracking was overt and the time and location data was transmitted to designated individuals, the experiment demonstrates the tracking capabilities of RFID technology.

[54] Yvo Desmedt, *Broader Privacy Issues*, p. 8, *at* http://www.rfidprivacy.org/papers/desmedt.pdf.

can be traced through the location of the product.[55] In fact, it is unnecessary that the RFID tag itself contain the personal identifying information in order to track a person; it may be possible to track a person carrying a tag through links to other records—thus, for example, if the government had access to library's borrowing records, it could link a person to the books he or she borrowed even if the RFID tag itself does not identify the borrower.[56] Moreover, when combined with visual tracking systems, RFID can yield precise coordinate location information of the subject of the surveillance.[57] In other words, there is a true threat of electronic peeping Toms being able to piece together what we like, what we carry and where we are, from information compiled in massive computer databases that are correlated with other databases and matched with location information derived from the many items embedded with RFID tags wirelessly transmitting the items' identification and location. Government snoops (or unauthorized third parties) could also use RFID-based consumer profiles in an investigation, and track the radio tags in public places to keep tabs on certain individuals.[58] Envision a political protest in which thousands of people take part. As demonstrators mingle, law

---

[55] The barcode system allows tracking purchases made by individuals, but it is impossible to use this system to identify which consumer purchased which pair of shoes or can of coke.

[56] Where books are concerned both privacy and freedom of expression are at stake. Implementation of RFID tags in books and other library materials will have a chilling effect - people might hesitate to check out books from a public library if they care for their privacy. This concern only increases in light of the power given to the government in the USA-PATRIOT Act to subpoena reading records. *See* Lee Tien, *Letter to San Francisco Public Library*, *supra* note 47.

[57] RFID systems provide specific identity information and approximate location information (*e.g.*, which room a person is in but not where in the room). By combining RFID systems with visual sensing systems, which provide precise coordination information without identity, more precise location information can be produced. Such development is under way at Georgia Institute of Technology (*see* http://www.cc.gatech.edu/fce/ahri). *See* Timothy P. Terrel & Anne R. Jacobs, Privacy, *Technology, and Terrorism: Bartnicki, Kyllo, and the Normative Struggle Behind Competing Claims to Solitude and Security*, 51 EMORY LAW JOURNAL 1469, at footnote 128.

[58] Mark Baard, *Is RFID Technology Easy to Foil?*, WIRED NEWS, *at* http://www.wired.com/news/privacy/0,1848,61264,00.html.

enforcement officers with hidden readers capture the unique RFID codes on clothing worn by the participants. Later, when participants pass through checkpoints, or when they board public transportation or an airplane, the ciphers can be matched and demonstrators can be detained and/or then identified.[59]

[59] *See* Testimony of Beth Givens, Privacy Clearinghouse, *RFID and the Public Policy Void* (August 18, 2003) (Presented to Joint Committee on Preparing California for the 21st Century, California Legislature, Senator Debra Bowen, Chair), *available at http*://www.privacyrights.org/ar/RFIDHearing.htm.

II. RFID and Modes of Regulation

The portrayal of the threats that RFID technology poses on consumers' information privacy emphasizes the need to regulate and adjust firms' behavior to specific standards so as to facilitate the protection of such privacy. Generally, as Professor Lawrence Lessig put it, there are four different modes of regulation; each constrains the behavior of its subjects: the market, law, norms, and technology.[60] In the following paragraph I will examine how each of these modes of regulation can respond to the privacy concerns raised by RFID technology.

Market, basically, regulates by price. The high price of the RFID tags today may limit the extent that firms use it. A future fall in their price is likely to encourage the industry to widely deploy the tags. Additionally, the effect that the use of RFID systems will have on revenues will have direct and immediate ramifications on the scope of RFID deployment and usage by the industry. Companies, driven by the goal of maximizing profits, will conduct a cost-benefit analysis; if they observe that consumers avoid shopping in stores where RFID tags are embedded into merchandise, the level of usage of RFID technology will be reduced to its efficient level—the equilibrium point where the marginal benefit from further using RFID technology equals the marginal loss of revenue. Accordingly, if this objective is reached through self-regulation that satisfies consumers, companies will carry out such action; namely, the market can affect companies to push for the adoption of fair information practices. The market will have its effect regardless the presence or absence of other forms of regulation. However, the constraints that the

[60] *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARVARD LAW REVIEW 501, pp. 506-508.

market shall place on companies using RFID system may not be enough to satisfy the level of privacy that society desires to have. Therefore, the market regulatory effect ought to be complemented by additional methods of regulation. Moreover, the existence of market failures—such as government subsidization of RFID, and information asymmetry between the company and the customer, which results in lack of information to consumers regarding the possible violations of their information privacy—sustains the necessity for additional regulation.

Technology, a specific instance of what Lessig calls "Architecture," is also a method of regulation, and refers to the physical world as we find it.[61] Technology determines what actions are feasible and what options become available. For example, encryption and technology standards constitute constraints on how users of a certain technology can behave. It has been said that the ability to design the technology granted private companies with regulatory power to shape the information environment, and may prove more effective than legal rules in directing human behavior.[62] In the context of RFID, the architecture is the technology that makes RFID systems the way it is, together with other technologies which aim at eliminating or diminishing the privacy intrusive characteristics of RFID. Technologies of the latter kind are known as "Privacy Enhancing Technologies" or shortly, PETs. Generally, privacy enhancing technologies have many constructive features, such as minimizing collection of data; anonymizing

[61] Lessig, id, p. 507.

[62] *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VIRGINIA JOURNAL OF LAW AND TECHNOLOGY 6. The authors claim that although the private sector in the digital environment enjoyed more power in setting the agenda and shaping the priorities, the role of the state has not declined. The power of the State as a significant social and political institution and the force of law should not be underestimates. Tracking the involvement of the State in the digital environment reveals that the State's actions, and inactions, were always substantial; hence, the State played a significant role in shaping the environment all along.

data and destroying raw data; security features (*e.g.*, encryption and access control) where data is collected, processed and transmitted; and obscuring techniques for data already revealed. In the case of RFID, some privacy enhancing technologies have already been developed—the prominent ones are appraised in the following chapter. Undeniably, there is no need for law to protect privacy if technology does not enable violation of it, and as Professor Pamela Samuelson eloquently stated "there is a substantial appeal in the idea of a technological solution to a problem that technology itself seems to have created, in part because such technologies are self-enforcing and appear to reduce the need for regulatory intervention."[63] However, as appealing as it may seem, the deficiencies in the RFID privacy enhancing technologies, which are discussed in the next chapter, make this mode of regulation too, incapable of satisfying the privacy protection that consumers and probably part of the industry wish for.[64]

As a result of the insufficiency of the market and technology modes, when trying to regulate companies' use of RFID technology, law and norms as complementing methods of regulation should be considered. *Law* orders people to behave in certain ways, and threatens punishment if they do not obey. *Norms*, like law, threaten punishment ex-post, but unlike law, the punishments of norms are not centralized, *i.e.*, norms are enforced by a community, not by the government. Self-regulation is a

[63] *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STANFORD LAW REVIEW 1125, pp. 1167-1168.

[64] It is not the conclusion of this paper that privacy enhancing technologies are not necessary. On the contrary, privacy enhancing technologies play an important role in technically allowing some of the fair information practices and reinforce the ability of the consumers to implement their rights and choices thereunder.

common way of putting norms into practice.[65] Self-regulation differs from a pure market approach, where consumer preferences drive companies' 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.[66] In contrast, self-regulation is based on the three traditional components of government[67]—legislation (defining appropriate rules), enforcement (*e.g.*, initiating actions against violators), and adjudication (deciding whether a violation has taken place and imposing an appropriate sanction)—only carried out by the private sector rather than by the government.[68] Before further discussing the role of law and self-regulation in regulating the use of RFID technology in light of the shortcomings in the other modes, I will set aside the examination of the privacy enhancing technologies that have been developed expressly to address the privacy concerns of RFID.

---

[65] The meaning of the term "self-regulation" may vary between different people and contexts. Assistant Secretary of Commerce Larry Irving illustrated it clearly: "Most basically, we need to define what we mean, as the term 'self- regulation' itself has a range of definitions. At one end of the spectrum, the term is used quite narrowly, to refer only to those instances where the government has formally delegated the power to regulate, as in the delegation of securities industry oversight to the stock exchanges. At the other end of the spectrum, the term is used when the private sector perceives the need to regulate itself for whatever reason—to respond to consumer demand, to carry out its ethical beliefs, to enhance industry reputation, or to level the market playing field—and does so." *See* Larry Irving, *Introduction to Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration (June, 1997), *available at* http://www.ntia.doc.gov/reports/privacy/intro.htm. In this paper, when I use the term "self-regulation" I connote to the latter end of the spectrum referred to in Irving's distinction.

[66] Rakesh Kumar, *Interaction of RFID Technology and Public Policy*, p. 12, *at* http://www.rfidprivacy.org/papers/kumar-interaction.pdf.

[67] *Id.* at 12-13.

[68] Instead of taking over all three components of regulation, industry may be involved in only one or two. For instance, an industry may be involved at the legislation stage by developing a code of practice, while leaving enforcement to the government; or the government may establish regulations, but delegate enforcement to the private sector. *See* Angela J. Campbell, *Self-Regulation and the Media*, 51 FEDERAL COMMUNICATIONS BAR ASSOCIATION 711, 715.

III. Privacy Enhancing Technologies and their Deficiencies

Corporations do not want to lose their customers that will eventually learn about the new threats.[69] Therefore, corporate responsibility and business incentives go hand in hand where customers have tangible privacy concerns.[70] Accordingly, corporations, which perceive that greater protection of personal privacy will benefit businesses as well as consumers by increasing their confidence in the company, have already started developing an arsenal of technologies that aim to enhance privacy when RFID tags are in use.[71] The development of such privacy enhancing technologies by the industry should be fostered by consumers as well as by the government, as regulation is only one tool for protecting privacy.[72] However, as I discuss below, relying solely on technology to resolve the privacy concerns will not provide a satisfying solution, both because all technologies have their weaknesses and drawbacks and because the technologies need to be implemented according to guidelines that assure the protection of privacy. Put differently, the best method for confronting the privacy threats that derive from the usage

---

[69] According to survey conducted in May 2003 by research firm *Gartner*, about 16 percent of consumers would probably or definitely stop shopping in a store that uses RFID technology; *see* Alorie Gilbert, *Wal-Mart Cancels 'Smart Shelf' Trial*, CNET NEWS.COM (July 9, 2003), *at* http://news.com.com/2100-1019_3-1023934.html?tag=rn.

[70] Larry Lessig articulated that decisions regarding the architecture of evolving communication infrastructure exercise control over individuals much like legal code, and therefore should be subject to democratic considerations such as accountability and public participation. Hence, if we observe RFID technology as a kind of communication infrastructure, then we could find another justification for going along with consumers concerns. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, p. 6 (1999).

[71] Other companies seem to scorn consumers' concerns and instead of trying to tailor RFID technology to address privacy concerns, seek to "neutralize opposition" and "mitigate consumer backlash" by emphasizing the "inevitability" of RFID technology and by describing RFID as a simple evolution of the bar code, rather than a new technology with "futuristic capabilities." *See* Jane Black, *Playing Tag with Shoppers' Anonymity*, BUSINESS WEEK ONLINE (July 21, 2003), *at* http://www.businessweek.com/technology/content/jul2003/tc20030721_8408_tc073.htm.

[72] *See* Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA LAW REVIEW 551, p. 573-575.

of RFID tags is combining both measures: successful technological means and good policies of fair information practices. In the following paragraphs I briefly review the main privacy enhancing technologies in the context of RFID; each followed by a description of its weaknesses, which reinforces the argument that privacy enhancing technologies are often not successful in completely achieving their goal, and cannot by themselves provide perfect solution to the privacy problem caused by RFID.

1. Protective Mesh of Foil (The Faraday Cage Approach)

The simplest technology for solving the privacy problem is the usage of protective mesh of foil, known as Faraday Cage, by consumers carrying the RFID tags. A container made of metal mesh or foil is impenetrable by radio signals (of certain frequencies). Once an RFID tag is placed inside such container its transmission is blocked, and obviously cannot be received by a reader.[73]

Clearly, this measure is not an overall solution since RFID tags can be embedded in every single product that a person is carrying or wearing, and consumers cannot stroll while wearing a human-size foil sack to cover all RFID tags carried on them at a certain time—locomotion would become a trouble. Perhaps, aluminum wallets can be a partial

[73] This simple technology is already in use today—for example, by FasTrak, the electronic toll collection system in the bridges of California's Bay Area. The main purpose for providing the aluminum bag to drivers has nothing to do with privacy: placing the transponder in the static bag serves to prevent the FasTrak system from deducting a toll from the owner's account when traveling as a carpool. However, an additional reason for the provision of the bags, which is stated on FasTrak's website, is that drivers who do not want their transponder read for the purpose of providing traffic flow data, can place the transponder in the bag when not using the transponder for payment of tolls at a toll plaza. *See* http://www.dot.ca.gov/fastrak/faq.htm.

solution to controlling transmission of RFID tags embedded in credit cards, notes, and so forth.[74]

2. Authentication Technologies

Other technologies approach the authentication for using an RFID reader when a user is to communicate with an RFID tag through the reader.[75] Yet, it is easy to observe that technologies that intend to limit the access to RFID tags to authenticated readers are insufficient to protect privacy. First, the users who are authenticated to use a reader can communicate with the RFID tags in the zone of the reader. Therefore, the users can identify the objects owned by another person if the objects are located in the zone. Second, users lacking authentication, can identify an object on the site with a private reader, even if the reader is not connected to the network. Third, the communication between an RFID tag and a reader can be easily tapped by a third party (efficient encryption is difficult in the current stage).[76]

These "gentle"[77] privacy enhancing technologies will most likely not appease the consumers' privacy concerns as the power to override them is in the hands of the

---

[74] At least one company, *Mobile Cloak,* already offers a Faraday Cage based device for such privacy purposes. For a description of the product; *see* http://startsimple.com/mobilecloak/mobilecloak/index.html.

[75] Sozo *et al.*, *supra* note 48, at 4.

[76] See *id.*

[77] Roger Clarke discerns between "Savage privacy enhancing technologies" and "gentle privacy enhancing technologies." The first combat privacy-intrusive behaviors by setting out to deny identity and to provide genuine, untraceable anonymity; the latter are intended to balance the interests of privacy and accountability, and are oriented towards protected pseudonymity rather than anonymity. *See*, Roger

organization that has an incentive to furtively flout the purpose of protecting the personal information of the consumers. Technical protection must be trustworthy. Unfortunately, governments, whose interests were threatened, and corporations, who are, in essence, solely dedicated to their shareholders' interests, have proven throughout history that their trustworthiness, with respect to the protection of privacy, is frail and that they comply with the privacy enhancing goal only when subject to sufficient preventive mechanisms and sanctions.[78] [79]

A similar approach is to require authentication whenever trying to read a tag rather than when accessing a reader. According to this approach, passwords could be assigned to the tags by the purchasing consumer, thus preventing the tags from being read absent the owner's permission. The problem with this method, beyond the obvious necessity for consumers to be aware of the existence of the tag, is that it would be very inefficient and create a big burden to consumers, requiring their patience and technical ability.

3. Tags Killing Technologies

The most straightforward approach for the protection of consumer privacy is to "kill" RFID tags before they are placed in the hands of consumers. The standard mode of operation proposed by the Massachusetts Institute of Technology AutoID Center is

---

Clarke, *Introducing PITs and PETs: Technologies Affecting Privacy*, PRIVACY LAW & POLICY REPORTER, *available at* http://www.anu.edu.au/people/Roger.Clarke/D V/PITsPETs.html.

[78] Clarke, *id*, p. 5.

[79] To satisfy this end, fair information practices include the principle of accountability.

indeed for tags to be killed upon purchase of the tagged product. With their proposed tag design, a tag can be killed by sending it a special "kill" command.[80] [81]

Certainly, the tags-killing technology can be helpful in pacifying the civil libertarians advocating for privacy, but it cannot, by itself fully solve the privacy problem. Killing tags at the point of sale leaves some privacy threats unaddressed. First, in-store tracking will not be encountered. Second, unless the killing device truly destroys the tag, a dormant tag could possibly be reactivated.[82] In addition, retailers may offer incentives to consumers to not exterminate the RFID tags (or disincentives to kill it), for instance, by creating two classes of customers, or simply by artificially constructing a long line in front of the RFID tags' killing device at the exit of the store, or by forcing consumers to buy special equipment in order to be able to carry out this measure. Another problem is that individuals may also be secretly given tags so they can be tracked or identified by an overzealous merchant, by a private detective, by a spouse, parent, or other relative.[83] Clearly, when the RFID tag carrier is unaware of the presence of the tag, he or she will not bother deactivating it. From a different point of view, the tags-killing technologies are undesirable, because many RFID tags are useful for consumers who may wish that the RFID tags remain operative while in their possession (*e.g.*, for the purpose of using smart refrigerators that automatically create shopping lists, or smart ovens that know how

---

[80] *See* Kumar, *supra* note 66, p. 9.

[81] A potential problem with a common "kill" password is the idea that a saboteur might enter a store for the purpose of deactivating all the RFID tags in it. To protect against such actions, stores could be equipped with RFID sensing systems that will report any such activity. *See*, Garfinkel, *supra* note 20, p. 5.

[82] A University of Pittsburgh's engineer has developed a tag containing an internal fuse that blows on command; once the fuse blows there is no way to reactivate the tag. *See* Dan Nephin, *Pitt Smart Tag May Alleviate Privacy Concern in Product Tracking* (October 3, 2003), USA TODAY, *available at* http://www.usatoday.com/tech/news/techinnovations/2003-10-03-alt-rfid-chip_x.htm.

[83] Juels *et al.*, *supra* note 18, p. 4.

to cook pre-packages food, based on the data they receive from the RFID tags on the products placed in them).

4. "Blocker Tags"

The idea of "blocker tags" technology is to simulate all (billions of) possible IDs (tag serial numbers) in a desired zone of ID values, thus make it seem like all possible tags are present and make the reader unable to figure out which tags are actually present (this technique may be thought of as a kind of passive jamming).[84] The enormous amount of serial numbers transmitted by the tag causes the reader to stall. When carried by a consumer, a blocker tag induces a physical region of privacy protection in which a reader is incapable of singulating tags. This approach is available in "tree-walking protocol,"[85] widely used in UHF frequency, and is cost effective since RFID tags on objects needs no additional enhancement. In order to preserve the commercial security purpose of the tags, the technology should be smart enough not to block items not yet purchased. Therefore, the blocker tag should be selective and only block certain ranges of RFID tag serial numbers ("Privacy Zones"), and the technology should allow shops to move items into privacy zone upon purchase ("Zone Mobility").

Similar belittling reasoning to what was mentioned above pertaining to tags-killing technologies, shall apply for using the (so far, theoretical) technology of "blocker

[84] Juels *et al.*, *supra* note 18, p. 9.

[85] In a nutshell, "Tree-walking protocol" for identifying tags recursively asks the question "what is you next bit?"; blocker tags always answer both '0' and '1'.

tags" devoid of a complementary privacy policy. Here also, retailers may create two classes of customers. Furthermore, this technology may add a burden to consumers, and will fail to protect consumers when products are separated from the blocker device.

5. User Controllable-Uniqueness Technologies

Some more intricate technologies developed from the view that careless disclosure of the relationship between a user and an object is the main cause for the privacy invasion. The private information may leak either via the wired network or involving the communication between an RFID tag and a reader. These new technologies focus on the latter problem, since the former problem can be solved in a similar way to the old-fashioned computer networks, such as data encryption. Among these technologies is one that seeks to conceal the permanent ID under a private ID that the users give onto rewritable memory in an RFID tag; and one that seeks to assign partial ID sequence to an object while the rest is given by user-assignable RFID tags. These approaches attempt to give users the controllability of the uniqueness of IDs. The problem with these technologies, beyond being a burden to consumers, is that a given ID may conflict with other IDs in the world. Even if the controllable-uniqueness technologies develop to deal with this problem by using real world information, such as the location or physical shape of objects,[86] it seems that it will only be a partial solution to the problem, as similar items in the same location would not be distinguished. This setback clashes with the key

[86] Sozo *et al.*, *supra* note 48, at 5.

purpose of RFID tags, which is to provide a unique identifier to every single item worldwide, and shall eventually lead the industry to avoid adopting these technologies.

6. Intermediate Conclusion

A certain conclusion can be drawn from the above discussion: privacy enhancing technologies are unlikely to be able on a standalone basis to completely assuage the danger to privacy that is engendered by RFID technology. That would remain true even if these technologies are widely implemented and strictly used. I, therefore, turn now to discuss the complementary approaches to the technological alternatives.

IV. Industry Self-Regulation

1. Legislation Not Yet Warranted

It may be argued that if advances in technology enable new surveillance capabilities, it is no longer reasonable for individuals to expect the same level of privacy as they previously did;[87] In the case of RFID it would mean that privacy interest erodes in the face of the technology. This argument is inconsistent both with privacy law, such as the Wiretap Act,[88] and the ruling of the United States Supreme Court in renowned case of Kyllo v. United States.[89] Rapid development and increasing technological sophistication and intrusiveness of surveillance means—first, photography, then, close-circuit television, and, finally, RFID technology—only attest that "Judicial implementations of the Fourth Amendment need constant accommodation to the ever-intensifying technology of surveillance."[90] Nevertheless, for the reasons stated below I believe that legislation,

---

[87] Office e-mail and silent video surveillance in the workplace are two examples; *see,* respectively, *Smyth v. Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa. 1996), and *Vega-Rodriguez v. Puerto Rico Tel. Co.*, 110 F.3d 174 (1st Cir. 1997).

[88] The Wiretap Act, 18 U.S.C. §§ 2510-2522, determines that it is illegal to intercept wire or electronic communication, even if it is easy to do so. Clearly, this means that even if wiretapping technology can easily harm privacy, individuals' expectations for privacy should not be corroded.

[89] 533 U.S. 27. In Kyllo, the Court concluded that where the government uses a device (in that case, heat-sensing technology) that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant. On the other hand, if the device was in common use, the court could have decided differently. In fact, the Supreme Court has approved warrantless visual surveillance of a home, ruling that visual observation is no "search" at all, *see California* v. *Ciraolo,* 476 U.S. 207, 213, and *Dow Chemical Co.* v. *United States*, 476 U.S. 227, 234-235, 239. In assessing when a search is not a "search," the Court has adapted a principle first proclaimed in *Katz* v. *United States*, 389 U.S. 347, 361, according to which a "search" does not occur–even when its object is a house explicitly protected by the Fourth Amendment–unless the individual manifested a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable.

[90] *Dean v. Superior Court* (1973) 35 Cal.App.3d 112, 116.

aimed at fulfilling this need, is not yet warranted, and in order to regulate the use of RFID technology we should turn to norms in the form of fair information practices.

Several primary factors explain the government's inability to effectively set the rules for new technologies.[91] First, private industry enjoys a financial and technical advantage as compared to the financial constraints of the government and its being short of technical expertise. It is more efficient for the government to rely on the industry's collective expertise than to reproduce it at the agency level.[92] Second, self-regulation is less costly to the government because it shifts the cost of developing and enforcing rules to the industry.[93] Furthermore, self-regulation saves unnecessary transaction costs as well (*e.g.*, getting permissions from government agencies). Third, self-regulation is more flexible than government regulation and legislation. Because of administrative and political causes, it is easier for an industry to alter its fair information practices rules in response to changing circumstances than for a government agency to amend its rules or for the legislature to modify a law. Also, self-regulation is more flexible by allows more diversity in methods of compliance. Fourth, self-regulation can be better tailored to the particular industry than government regulation; whereas paternalistic general laws or

---

[91] For further discussion on the advantages and disadvantages of self-regulation, *see* Angela J. Campbell, *supra* note 68, pp. 715-720; Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation as Regulatory Technique*, 47 ADMINISTRATIVE LAW REVIEW 171, 181-191; Mark L. Gordon & Diana J.P. McKenzie, *A Lawyer's Roadmap of the Information Superhighway*, 13 JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 177, 194-195; Peter P. Swire, *Markets, Self-Regulation and the Government Enforcement in the Protection of Personal Information*, in Irving, *supra* note 65, *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1A.

[92] Critics question whether companies will use their expertise to the benefit of the public, implying that they are more likely to employ their expertise to maximize the industry's profits; *see* Swire, *id.*

[93] Self-regulation will only result in a net reduction of cost if the costs to industry are lower than the government's cost savings. This will usually be the case when technical expertise is essential for creating the rules. It is possible, however, to argue that such costs should have been borne by the regulated entities in any event. *See* IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 120-121 (1992).

government regulation may be overbroad and thus impede many socially beneficial uses and lead to absurd results. Fifth, self-regulation purports to provide greater incentives for compliance. If rules are developed by the industry, the parties are more likely to perceive them as reasonable, and therefore comply.[94] Finally, there is the speed of the evolving technology as compared to the speed at which the government is able to operate. Legislatures and government agencies do not appear to be percipient in anticipating the economic and social impact of new technology. This lack of foresight suggests that these institutions should not necessarily exercise their authority to regulate technology until the technology and its implications mature.[95] Given time, we may have sufficient experience with RFID to justify general legislation to govern it, but as of today, governments should encourage a self- regulation model.[96]

Critics of self-regulation assert that the private nature of self-regulation may fail to give adequate attention to the needs of the public or the views of affected parties outside the industry, and may also fail to vigorously conduct adequate self-enforcement.[97] In view of that, if privacy concerns are not addressed by industry through satisfactory self-regulation, the government will face increasing pressure to play a direct role in

---

[94] However, this argument is weaker when the industry plays a major role in the rule making process, whether at the agency level or legislature hearings.

[95] *See* Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL JOURNAL OF LAW AND PUBLIC POLICY 475, 509-510.

[96] The Clinton administration seemed to have acknowledged these factors with respect to the Internet. The administration called for industry self-regulation to address consumer privacy concerns, and supported private sector efforts underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes; *see* President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (1997), *available at* http://dcc.syr.edu/ford/course/e-commerce-framework.pdf.

[97] These critics also point to the benefits of legislation (*e.g.*, it is comprehensive, provides firms and technology developers some guidance regarding system design, and is likely to reassure public about respect for privacy). Nonetheless, I infer that the considerations in favor of self-regulation prevail, at least at the current stage.

safeguarding consumers' privacy; and indeed, documented abuses of privacy in particular contexts have historically led to the legislation of new context-dependent laws in the United Sates.[98] Therefore, while bearing that in mind, the industry should engage in self-regulation and exert fair information practices, so as to evade privacy abuses deriving from the use of RFID technology and to stave off government regulation and legislation. Moreover, although self-regulation may not be perfect and has disadvantages, adopting fair information practices will only contribute to enacting better legislation in the future if so pursued.

At this stage, after the basis for industry self-regulation with respect to the employment of RFID has been established, I shall move to discuss what particular principles of fair information practices should be promoted for this technology.

2. Existing Principles of Fair Information Practices

The earliest comprehensive formulation of the concept of fair information practices is found in a 1973 Report of the Secretary of the United States Department of Health, Education & Welfare's Advisory Committee on Automated Personal Data Systems entitled, "Records, Computers and the Rights of Citizens (Report)." The Committee assessed the impact of computer-based record keeping on private and public matters, and

[98] For example, the Fair Credit Reporting Act, which was enacted in 1970, imposes responsibilities on credit report agencies to protect confidential personal data and ensure that the information is up-to-date and accurate; other specialized laws protect, *inter alia*, cable subscribers' information (Cable Communications Policy Act of 1984), children information collected online (Children's Online Privacy Protection Act of 1998), health data received by health care providers (Health Insurance Portability and Accountability Act of 1996), and personally identifiable financial information (Gramm-Leach-Bliley Financial Services Modernization Act of 1999).

recommended safeguard requirements for the administration of personal data systems, together with certain rights of individual data subjects against the computer-based record's potential adverse effects.

The safeguard requirements generally included:

(1) annual public notice of the existence and nature of the data system;

(2) identifying someone with responsibility for the system;

(3) taking reasonable steps to insure the security of the data in the system and data transferred to other systems;

(4) maintaining an accurate account of access and use of personal data; and

(5) only retaining data that is accurate, timely and reasonably necessary to achieve the data system's purpose.

The rights of individual data subjects included:

(1) notice of the kind and use of personal data that is reasonably necessary to achieve the data system's purpose.[99]

(2) the right to access personal data in the system, contest its accuracy and have the opportunity to correct or amend inaccurate or incomplete data; and

(3) the right to consent to uses and disclosures of the data beyond the stated purpose of the system as understood by the individual.

[99] Prima facie, the notice required here is not of what is actually collected!

It is worth noting that in Chapter VI of the Report, the Advisory Commission recommended that legislation be enacted establishing a code of fair information practices for all automated personal data systems. In addition, a later report examining private and public record systems that was issued in 1977 by the Privacy Protection Study Committee also called for the establishment of federal data privacy law.[100] Although the United States Congress has enacted several context-based privacy laws,[101] it has not adopted these recommendations thus far.

An important later codification of similar principles was completed in 1980 by the Organization for Economic Cooperation and Development ("OECD"), which was the first international organization to issue an international policy for the protection of privacy in computerized data processing. The drafters of these guidelines, known as the OECD Guidelines on Protection of Privacy and Transborder Flow of Personal Data (the "OECD Privacy Guidelines,")[102] foresaw that technology would develop rapidly, and tried to design the principles set forth in the guidelines in a technology-neutral way to accommodate future developments. Hence, in 1998 when attempting to apply the OECD Privacy Guidelines to more modern technologies, particularly to data collection applications on the Internet, the OECD's Information, Computer and Communications Policy Committee and Group of Experts on Information Security and Privacy have

[100] The U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977). The Privacy Protection Study Commission was established by the Privacy Act of 1974 and was subject to a sunset provision set out in the Privacy Act itself (Section 5).

[101] *See supra* note 98.

[102] The Guidelines can be viewed *at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

articulated that it was unnecessary to revise the guidelines and to define new principles for the protection of privacy in the expanding global electronic environment. They deemed that the relevant question was only what the appropriate means, of putting the established principles into practice, were.[103]

The OECD Privacy Guidelines outline the following basic principles:[104]

1. **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

   This principle contains the requirements which are regularly referred to as *notice* (notifying the individual whose personal data may be collected) and *consent* (obtaining the individual's consent to the collection of the data).

2. **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes, and as are specified on each occasion of change of purpose.

[103] *See Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet*, *supra* note 50, p. 17.

[104] Paragraphs 7 to 14 of the OECD Privacy Guidelines.

4. **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:

    a. with the consent of the data subject; or

    b. by the authority of law.

5. **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. **Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual Participation Principle**: An individual should have the right:

    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

    b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c. to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. **Accountability Principle**: A data controller should be accountable for complying with measures which give effect to the principles stated above.

These principles were claimed to apply to all types of personal information, whether traffic data (such as date, time, duration or location) or content data (*e.g.*, information about personal preferences or information about the transactions conducted) regardless of the technology used.[105] I argue that these principles can and should indeed be the basis for fair information practices in the context of RFID tags, but that they should be revised to accommodate the unique concerns and not adopted as is.

[105] *See Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet, supra* note 50, p. 6.

3. Early Birds in Forming RFID Privacy Principles

Following the self-regulation approach, a set of five principles, as a voluntary framework for commercial deployment of RFID tags, was proposed. These principles are known as the "RFID Bill of Rights"[106] and include:

(1) The right of the consumer to know what items possess RFID tags;

(2) The right to have embedded tags removed, destroyed or deactivated upon purchase of these items;

(3) The right of the consumer to access the data associated with an RFID tag;

(4) The right to access of services without mandatory use of RFID tags (*e.g.*, the right to return a product or to travel on a particular road),[107] and;

(5) The right to know when, where and why the data in RFID tags is accessed and being read.

In the spirit of the these principles, CASPIAN,[108] a civil liberties group, has proposed "The RFID Right to Know Act of 2003," which requires mandatory labeling to inform consumers when an item contains an RFID tag, and also prohibits corporations from linking the tags with personally identifying information.[109]

---

[106] *See* Simson Garfinkel, *An RFID Bill of Rights*, TECHNOLOGY REVIEW, p. 35 (2002), and Garfinkel, *supra* note 20, p. 4.

[107] Garfinkel, *supra* note 20, p. 4.

[108] Short for: Consumers Against Supermarket Privacy Invasion and Numbering.

[109] *See* http://www.nocards.org/rfid/rfidbill.shtml. Based on CASPAIN's draft legislation, Utah's House of Representatives passed the first-ever RFID privacy legislation in February 2004 (sponsored by

From the stand point of the above innovative attempts to define the boundaries of the usage of RFID tags, a clear privacy policy should be embraced by companies dealing with the RFID technology, thus creating strong fair information practices. In fact, some suggestions for such guidelines, which basically adopt the OECD's privacy principles, have recently started sprouting, as a result of initiatives of several interested entities consisting of organizations committed to the protection of privacy,[110] and the industry.[111]

Representative David L. Hogue). This bill, entitled Radio Frequency Identification Right to Know Act (H.B. 251), expired on March 3, 2004, before the Utah State Senate could vote on it. The Act aimed to ensure consumer privacy by prohibiting retailers from matching the data gathered by RFID readers with consumers' personal information. Additionally, it required all goods bearing functioning RFID tags in stores to be labeled as such. A similar bill, the RFID Right to Know Act of 2004 (S.B. 867) is currently before the Missouri State Senate (sponsored by State Senator Maida Coleman). Like the Utah bill, Missouri's bill would mandate that any product containing an RFID tag have a label that the consumer commodity or package contains or bears an RFID tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase. The California Bill (S.B. 1834), introduced to the State Senate by Senator Debra Bowen on February 20, 2004, does not require a labeling environment, but settles for the requirement that a person or entity that uses RFID systems shall comply with certain conditions, including obtaining an individual's written consent before attaching or storing personally identifiable information with data collected via an RFID tag or before any personally identifiable information collected via an RFID system is shared with a third party.

[110] A position statement on the use of RFID on consumer products was issued no November 14, 2003 jointly by Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), the Privacy Rights Clearinghouse, the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), the Electronic Privacy Information Center (EPIC), Junkbusters, Meyda Online, and PrivacyActivism. The statement expresses that the Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD) provides a useful model for RFID. The document also calls for a three-part framework in order to mitigate the potential harmful consequences of RFID to individuals and to society: "First, RFID must undergo a formal technology assessment, and RFID tags should not be affixed to individual consumer products until such assessment takes place. Second, RFID implementation must be guided by Principles of Fair Information Practice. Third, certain uses of RFID should be flatly prohibited." *See* http://www.privacyrights.org/ar/RFIDposition.htm.

[111] EPCglobal Inc., the organization spearheading the development of the electronic product code RFID chips use, issued its own proposed guidelines that require consumers be notified of the presence of EPC devices on products through a logo or identifier. They should be informed of their options for disabling or removing RFID tags from products and be educated about RFID/EPC devices and their applications. Finally, data collected using the devices should be subject to applicable laws about the use, retention, and security for such data. *See* "Guidelines on EPC for Consumers Product" *at* http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html. *See*, also, Kumar, *supra* note 66, p. 15.

V. Adjustment of Fair Information Principles to RFID

Of the numerous privacy guidelines, including those of the Department of Health, Education & Welfare and the Organization for Economic Cooperation and Development, it is clear that notice,[112] choice,[113] access,[114] security,[115] and enforcement[116] are the generally agreed-on key principles and framework that serve as the leitmotif of existing fair information practices.[117] These principles should also provide the hub of the fair information practices that ought to eventually apply to the usage of RFID technology. Nevertheless, the code of privacy principles for RFID must stipulate some additional elements in order to better fit the characteristics of this state-of-the-art technology.

The standard of *notice* basically aims at having no secret data systems. Consequently, in the context of RFID technology (in light of the continuing exposure and implications after leaving the retail environment), a practice of merely notifying the consumer of the subsistence of the technology in the retail environment is a must, but will not suffice on its own. The consumer ought to be alerted about the presence of an RFID tag in every specific product that he considers purchasing and about every environment that is under surveillance by RFID readers. This goal may simply be achieved by

[112] Also referred to as "awareness."

[113] Also referred to as "consent."

[114] Also referred to as "participation."

[115] Also referred to as "integrity."

[116] Also referred to as "redress."

[117] In addition to the two designated reports, other major reports setting forth the core fair information practice principles are: U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: *Principles for Providing and Using Personal Information* (1995); U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); *The European Union Directive on the Protection of Personal Data* (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

adequately marking every such product and environment. Since notice is such a fundamental element of fair information practices and is a prerequisite to implementing other fair information practice principles,[118] it is critical that consumers can invariably rely upon finding the "RFID logo" wherever applicable. This mark, similar to food labels that indicate the level of fat, cholesterol and vitamins, provides the basis for informed choices by consumers.

Consumers should be educated about the essence of the RFID technology, its applications, the benefits to consumers, and the threats to consumers' privacy thereof. Notice, even with respect to every embedded tag, would not be adequate if consumers are unconscious of the privacy threats; similarly, consumers will not be able to make an informed choice if they are unaware of the benefits of the technology.[119] Indeed, education of consumers with respect to risks and benefits is relevant also to Internet privacy and other digital environments like the cellular telephone or digital television, and not solely to RFID technology; but it has not been emphasized and implemented enough in that context. Contrary to that practice, it is important that RFID technology would be applied and implemented after or concurrently with the provision of satisfying instructions and advice to consumers.

[118] United States of America, Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Market Place, A Report to Congress* (May 2000), p. 14.

[119] Research shows that people perform a simple risk-benefit assessment when considering compromising their privacy; *see* Robert S. Laufer & Maxine Wolfe, *Privacy as a Concept and a Social Issue: A Multidimensional Development Theory*, 33 JOURNAL OF SOCIAL SCIENCES 22 (1977).

With respect to the standard of *choice*, the commonly preferable opt-in regime[120] may not suit the practices of RFID. The appropriate regime is an opt-out one, where the consumer can choose to stick with the tag or to get rid of it by taking the affirmative, necessary steps. It does not seem practical to conduct an opt-in regime where the consumer would have to ask for the installation of an RFID tag into its product at the point of sale. Theoretically, a feasible opt-in regime would be one where all RFID tags are deactivated at the checkout counter, unless the consumer requires the contrary; but this would be very costly and inefficient. The best solution for consumers would be, of course, to have two types of every product, one with an RFID tag and one without a tag; but clearly, this would be very uneconomical and would not work in practice. The fact that only an opt-out regime is suitable in the case of RFID tags reinforces the need for a clear and conspicuous notice of consumers' choices, because under this regime vendors are more tempted to "keep silent" and consumers may easily not be aware of their options.[121]

This specific implementation of the core principle of choice in the context of RFID tags—a choice of keeping or getting rid of the tag—does not make unnecessary the original meaning of the principle of choice: a consumer, who decides to keep the tag, should still have the options as to how the personal information collected from him may

[120] Surveys show that public strongly supports opt-in regimes over opt-out regimes. See *Harris Poll: A Growing Threat,* BUSINESS WEEK ONLINE, March 20, 2000, p. 96, *at* http://www.businessweek.com/2000/00_12/b3673010.htm.

[121] *See* Barbara Lawler, *The Opt-In Approach to Choice* in *CONSIDERING CONSUMER PRIVACY, A RESOURCE FOR POLICYMAKERS AND PRACTITIONERS*, Center for Democracy and Technology (March 2003), p. 22, *at* http://www.cdt.org/privacy/ccp/ccp.pdf.

be used; specifically, have control over the secondary uses of information (*i.e.*, uses beyond those necessary to complete the contemplated transaction).[122]

A new principle, which has not been relevant to privacy intrusive technologies thus far, should prohibit the usage of RFID technology for human tracing purposes. Ancillary to this prohibition there should be a principle that grants consumers the right to have their personal identifying information not linked to products' identifying information, *i.e.*, the unique serial number of their RFID tags. RFID backers may utter that the tracking capabilities of RFID tags are not much different and do not impose a greater threat than the tracking capabilities of cellular phones, and therefore no special practices should be executed in order to address this alleged threat. In my view, this potential argument is not true for several reasons, and the peril of tracing by using RFID tags should be distinguished from the parallel threat related to cellular phones. First, there are obviously significant physical and technical differences: RFID tags are enormously smaller than cellular phones. This distinction allows the embedment of hidden tags, while a phone is big and normally chosen to be carried. In addition, cellular phones need a battery to transmit signals, whereas RFID tags usually operate without an internal energy source. Thus, a person, who wishes to eliminate the transmission of signals from a cellular phone that he or she is carrying, can simply take out the battery.[123] In contrast, deactivating an RFID tag requires the proper technology and cannot be done manually without the necessary means. Second, there are differences in the substance of

[122] Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

[123] Turning the phone off may not be enough as some cellular phones still communicate with the network while shut off.

the technology: Cellular networks need to constantly know the location of a phone in order to transfer a call to it. Geographical location is part of their architecture. In consumer products, being traceable is not a substantial or necessary part of the functions of RFID tags, at least from the consumers' point of view. Consequently, one may state that, in the context of being traceable, a consumer agrees to waive his or her privacy when choosing to carry a cellular phone. It would be irrational to bring the same argument when it comes, for instance, to a pair of jeans that a consumer is wearing.

VI. Proposal of RFID Fair Information Practices Policy

At this juncture, I will try to lay down ten principles that could be the foundations of a strong privacy policy with respect to the usage of RFID tags:

1. **Consumer Notice**. Consumers should be given clear notice of the presence of the tag in a product. The notice should be in the form of a label or logo, clearly displayed and easily understood.[124] RFID readers in the retail environment should also be labeled and any tag reading that occurs must be transparent to the consumers.

2. **Consumer Education**. Consumers should be educated about the essence of the RFID technology, its applications, the benefits to consumers, and the threats to consumers' privacy thereof.

3. **Transparency / Openness**. RFID users ought to reveal the purposes for which RFID systems are used. Additionally, RFID users must make public their policies and practices involving the use of RFID tags and the information which is collected, and no secret databases should exist.[125]

[124] If such a logo is standardized and licensed by the responsible entity, it could serve to secure compliance with the fair information practices. This measure is similarly implemented today by MIT, whose licensing arrangement for the EPC Network specifically prohibits the use of technology for tracking or identifying people, with two exceptions: military personnel and medical patients. *See* written testimony of Kevin Ashton, Executive Director, Auto-ID Center, Hearing on RFID and Privacy (August 18, 2003) (submitted to California State Senate Subcommittee on New Technologies), *available at* http://www.sen.ca.gov/ftp/SEN/COMMITTEE/STANDING/ENERGY/_home/08-18-03auto-id.htm.

[125] This principle is based on the sixth principle of the OECD guidelines.

4. **Collection Limitation**. The gathering of information should be limited to what is reasonably necessary for the previously stated purpose.[126]

5. **Consumer Choice**. Consumers should be given a choice to disable or discard the RFID tags from the products they purchase, at the checkout counter. In order to have an effective choice regime, RFID users must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they acquire—a simple and easily-accessible way for consumers to exercise their choice must be provided. Accordingly, there should not be any prohibition on customers to detect RFID tags and readers and disable tags on items in their possession. It is recommended that the tags should be allowed only on packaging, and not in wearable products, so they are easily disposable.

6. **No Tracing**. RFID systems must not be used to track individuals absent informed and written consent, which is provided before data is collected.

7. **Anonymity & Confidentiality**. RFID technology should not be employed in a manner that eliminates or reduces anonymity.[127] Furthermore, a consumer shall have the right to have personal identifying information kept separate from object identifying information (tag's ID), *i.e.*, no linking between the identification numbers of tags and the personal identification data of consumers should take place. Also, in order to prevent unauthorized readers from having access to personal information unnecessary information should not be placed on the tag.

[126] This principle is similar to the second and third principles of the OECD Guidelines.

[127] This principle serves as the rational for the call to abort the European Central Bank's plan to incorporate RFID tags into currency by 2005.

Similarly, if RFID users desire to (permissibly) forward or share with other agencies the data which they have collected, they must strip off all identifying information with the product purchased by the consumer.

8. **Access**. Individuals should be able to access data about them collect by RFID technology—*i.e.*, to view the data in the collector's files—and to contest that data's accuracy and completeness.

9. **Security**. There must be security and integrity in: (1) transmission between RFID tags, readers and the upper level data collection systems (*e.g.*, by way of encryption), (2) databases, and (3) system access to authorized personnel only.[128] It is recommended that these are verified by an outside party and that the assessment becomes publicly disclosed.

10. **Accountability**. RFID users are accountable for the implementation of RFID technology and the collected data. Therefore, they should be responsible for complying with the principles of the fair information practices, and measures should be taken to ensure compliance[129] and appropriate means of recourse by injured consumers. The latter include, at a minimum, the establishment of entities

[128] Both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data, should take place. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem. *See* United States of America, Federal Trade Commission, *Privacy On-Line: A Report to Congress* (June 1998), p. 10; available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[129] Mechanisms to ensure compliance include: making acceptance of, and compliance with, a code of fair information practices a condition of membership in an industry association; external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue. *See* Federal Trade Commission, *Privacy On-Line: A Report to Congress* (June 1998), *id*, p. 10.

within the industry,[130] to which consumers can complain when the provisions of the fair information practices guidelines have been violated.[131]

Pursuant to adopting a privacy policy based on these principles, the final step, towards placating privacy fears among consumers and gaining their trust in RFID technology and the industry that is putting it into practice, could be regarded as more of psychology-related. Consumers need to be convinced that the privacy enhancing technologies truly work (*e.g.*, that the tag was really "killed" at the point of sale) and that the fair information practices are strictly followed. This process could take time, but strong privacy policies rigorously implemented by companies could go long way in coming years to bring acceptability of the RFID technology among consumers.

[130] In the United States, the Federal Trade Commission has legal powers to enforce policies that companies have embraced and breached, by seeking injunctions before U.S. district courts. This enforcement measure, often called "co-regulation," provides a more effective remedy than adjudicative proceedings in cases where voluntary compliance cannot be assured, by avoiding the protracted adjudicative proceedings, and because the violation of the policy can amount to a contempt of court and can be sanctioned as such. *See* Section 13(b) of the Federal Trade Commission Act (15 U.S.C. §53(b)) and Title 16 of the Code of Federal Regulation (16 CFR) § 1.61.

[131] A self-regulatory system not only should provide a means to investigate complaints from individual consumers, but should also ensure that consumers are aware of how to access such a system. If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (*e.g.*, correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer. Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation. *See* Federal Trade Commission, *Privacy On-Line: A Report to Congress* (June 1998), note 128, p. 11.

CONCLUSION

Privacy is not just about hiding things. It is about self-possession, autonomy, and integrity. As we move deeper into the computerized world of the Twenty-First Century, the right of privacy is not only the right of people to close their doors and pull down their window shades. It is the right of people to control what details about their lives stay within their own houses and belongings and more generally, within their control, and what leaks to the outside.[132] It is also the right to exercise control over the subsequent uses of personal information, which an individual agreed to disclose.[133] The cornerstone of this paper was that this important right to privacy should not be corroded in the face of sophisticated new technologies that surface in the market, and that technological enhancements can exist alongside with privacy interests.

This is certainly true with regard to the technology of RFID. Recent advances in this technology, and the emergence of its numerous new applications and initiatives for prospective applications, have brought the industry and consumers to confront serious privacy concerns. The fear of greater intrusiveness, in the form of the expanded tracking and data collection capabilities of RFID technology, has driven several consumer privacy advocates to demand that the development and deployment of RFID technology would be stopped, and to call for a consumer ban on companies that use RFID systems. Indeed, society should not settle for a lower level of privacy. However, these voices are somewhat improvident and not desirable. A technology, such as RFID, that brings numerous benefits to businesses and consumers should not, and probably could not, be

[132] GARFINKEL, *supra* note 1.

[133] *See* Alan Westin, PRIVACY AND FREEDOM (1967).

held back due to privacy concerns. Therefore, further evolvement and dissemination of RFID systems are probably inevitable. In light of this recognition, I believe that the best approach would be to cope with the unique threats of RFID technology, while trying to maximize the opportunities to benefit from its positive modern functions. Consumers may want information privacy, but they also want to enjoy the advantages and benefits of new technologies such as RFID, rendered by strong information economy. As a result, they appear to be willing to balance their interests in keeping certain information about themselves private, with their interests in getting access to improved goods and services that embody RFID technology along with its privacy invasive characteristics.

In order to reach such a balance, which is commensurate with the uniqueness of RFID, this paper began by analyzing the characteristics and applications of RFID technology along with the threats that it bears for consumers' privacy. Thereafter, it has been shown that privacy enhancing technologies cannot solve the privacy problems without being accompanied by additional regulation. The self regulation approach, in the form of strong principles of fair information practices, has been portrayed as superior to legislation and government regulation when addressing the privacy concerns caused by RFID technology. The paper further demonstrated that these principles should not be adopted in their current common structure, but they ought to be altered to fit the distinctiveness of RFID technology. Ultimately, the paper suggests a series of principles of fair information practices that are recommended for companies to adopt when employing and exercising RFID technology.

The RFID-customized principles of fair information practices should adapt the principles of notice and choice to the exceptionality of RFID, assure the anonymity of

consumers, guarantee adequate educating of consumers, and assume a prohibition on using RFID for tracking purposes. By adopting fair information practices that address the unique privacy concerns stemming from RFID technology, consumers' privacy will be protected, while the many fine applications that RFID technology possesses will not be eliminated. As a result, the aforesaid desired balance between using the technology and protecting consumers' privacy will be realized.

I deem that the creation and adoption of privacy policies, which are based upon the ten proposed principles as described in Part VI of this paper, are essential. These principals, in conjunction with further development of privacy enhancing technologies, such as tags-killing devices, "blocker tags," and additional tools as described in Part III, will provide a solution to the privacy threats posed by RFID technology, to the satisfaction of both the industry and consumers. This way the goal of stimulating the development of the technology of Radio Frequency Identification and its avant-garde applications, whilst protecting society's interest in information privacy, will be attained.