

Draft

**A NEW CHALLENGE TO PRIVACY MANAGEMENT:
ADAPTING FAIR INFORMATION PRACTICES TO
RADIO FREQUENCY IDENTIFICATION TECHNOLOGY**

By

Gal Eschet

May 2004

Table of Contents

INTRODUCTION	2
I. RFID and the Danger to Consumers’ Information Privacy	6
<i>1. Information Privacy to Collide with RFID</i>	6
<i>2. The Technology</i>	8
<i>3. The Threats to Privacy</i>	13
II. RFID and Modes of Regulation	19
III. Privacy Enhancing Technologies and their Deficiencies	23
<i>1. Protective Mesh of Foil (The Faraday Cage Approach)</i>	24
<i>2. Authentication Technologies</i>	25
<i>3. Tags Killing Technologies</i>	26
<i>4. “Blocker Tags”</i>	28
<i>5. User Controllable-Uniqueness Technologies</i>	29
<i>6. Intermediate Conclusion</i>	30
IV. Industry Self-Regulation	31
<i>1. Legislation Not Yet Warranted</i>	31
<i>2. Existing Principles of Fair Information Practices</i>	34
<i>3. Early Birds in Forming RFID Privacy Principles</i>	40
V. Adjustment of Fair Information Principles to RFID	42
VI. Proposal of RFID Fair Information Practices Policy	47
CONCLUSION	51

“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 privacy⁹ 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.

