This product is part of the Pardee RAND Graduate School (PRGS) dissertation series. PRGS dissertations are produced by graduate fellows of the Pardee RAND Graduate School, the world's leading producer of Ph.D.'s in policy analysis. The dissertation has been supervised, reviewed, and approved by the graduate fellow's faculty committee.

DISSERTATION

RFID in the Retail Sector

A Methodology for Analysis of Policy Proposals and Their Implications for Privacy, Economic Efficiency and Security

Gordon Bitko

This document was submitted as a dissertation in October 2006 in partial fulfillment of the requirements of the doctoral degree in public policy analysis at the Pardee RAND Graduate School. The faculty committee that supervised and approved the dissertation consisted of Bob Anderson (Chair), Tora Bikson, and Jim Dertouzos.

PARDEE RAND GRADUATE SCHOOL

The Pardee RAND Graduate School dissertation series reproduces dissertations that have been approved by the student's dissertation committee.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Abstract

Radio Frequency Identification (RFID), a low cost and potentially covert method of remotely retrieving stored information, is a technology with the potential for substantial social, economic, and legal impacts, including a wide range of individual and social costs and benefits. Broad recent growth of RFID applications, especially in the retail sector, has raised several specific privacy and data protection concerns derived from the potential that RFID offers for surreptitious monitoring, and the linking of personal and obscure or private information into large databases. The result of these concerns has been an active policy debate, with legislative proposals at the US state and federal levels, as well as in Europe. Despite these proposals, a clear and comprehensive analysis of policies, and their implications for security, economic efficiency, and individual privacy and civil liberties, does not yet exist.

This dissertation fills that gap by constructing both a qualitative framework for analyzing policies, and a simple economic model that allows for a quantitative understanding, and assessing several of the leading policy proposals with those two tools. The qualitative framework provides a description of the key stakeholders in the debate, and the issues concerning each. The economic analysis shows that all of the assessed policies involve substantial tradeoffs in firm and individual behaviors and that a true understanding of uncertainties such as market structure and individual preferences about privacy is critical in assessing the impact of any policy. The analysis also shows that policies with costs more evenly distributed across all stakeholder groups result in more information collection. Although additional analysis and more sophisticated planning tools are needed, current policymakers should consider policies that address all stakeholder concerns, and are able to adapt to the inherent uncertainties in markets and individual behaviors.

Acknowledgements

I would like to thank the many people who have supported my writing this dissertation. First, my dissertation committee members, Bob Anderson, Tora Bikson, and Jim Dertouzos, were instrumental in providing valuable feedback and encouragement throughout the process. In particular, Jim's guidance, patience, and desire for me to learn and apply economics were essential. Among many other RAND researchers, I'd particularly like to thank Ed Balkovich, Rich Silberglitt, and Shari Lawrence Pfleeger. While they were not members of my committee, all have shown continued support of my work, throughout my time at RAND. Ed and Tora were both especially supportive while I was developing the initial research ideas behind this work. I'd also like to thank my external reviewer, Andrew Odlyzko, for taking time from a very busy schedule to make substantive comments.

Second, the RAND National Security Research Division (NSRD) was the key sponsor of this research. In particular, I'd like to thank Phil Anton for sponsoring me within NSRD, and the rest of NSRD's leadership for recognizing the value in sponsoring multiply PRGS dissertations. I'd also like to recognize the persistence of Rachel Swanger in convincing NSRD of that value, and the rest of the PRGS staff for their continuing encouragement.

Finally, I am grateful to family and friends for their patience during trying times. In particular, Sai has been a source of encouragement and inspiration at all times.

Thank you all!

Table of Contents

List of Figures

List of Tables

Glossary

ANOVA	Analysis of Variance
Auto-ID	Automatic Identification Technology, such as RFID or bar codes
BoR	Bill of Rights, an RFID policy proposal
CALEA	Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994
CDT	Center for Democracy and Technology
ECPA	Electronic Communications Privacy Act of 1986
EPC	Electronic Product Code
GHz	Gigahertz, a frequency range used by some RFID technology
ISR	Industry Self Regulation, an RFID policy proposal
kHz	kilohertz, a frequency range used by some RFID technology
MHz	Megahertz, a frequency range used by some RFID technology
OECD	Organization for Economic Co-operation and Development
OLS	Ordinary Least Squares, a basic regression analysis technique
POS	Point of Sale
RFID	Radio Frequency Identification
UHF	Ultra High Frequency

UPC	Universal Product Code
VPPA	Video Privacy Protection Act of 1998

1. Introduction

1.1. Research Overview and Objectives

Historically, policy response has lagged the advent of technologies that have the power to affect the tradeoffs between national security, economic efficiency, and personal privacy and identity. Inevitably, though, policies associated with these technologies have been established, resulting in substantial social, economic, and legal impact to individuals, firms, governmental organizations, and society as a whole. Although new laws, such as the USA PATRIOT Act, contain an implicit recognition of the changing nature of personal information and privacy, they are already outdated in the face of new technologies that are enabled by the proliferation of cheap and ubiquitous sensing, computing and data storage.

One such technology is Radio Frequency Identification (RFID), a low cost and potentially covert method of reading tagged items from a distance, which is already used in diverse applications such as proximity sensors for facility security, electronic toll collectors for automated entry to numerous fee-access bridges, tunnels and roads, and retail operations such as ExxonMobil's Speedpass™ system. More recent widespread uses of RFID have been spearheaded by both the US Department of Defense (DoD) and many large retailers, such as Wal-Mart, Target, and Tesco, who are already engaged in deploying RFID for asset tracking across their entire supply chains.

While many of these applications collect information at the aggregate level, other new uses of RFID, such as tags that can be implanted into individuals and the Department of State's plan to incorporate an RFID tag into future US passports raise several specific privacy and data protection concerns derived from the potential that RFID offers for surreptitious monitoring. The first of these is the collection of information linked to personal data. An

example of this would be when a retail store tags products with unique codes that are linked to an individual at the point-of-sale, and used to create a customer database. This could be used for guarantee purposes, but would also enable direct and targeted marketing, or even price discrimination, as consumer habits are learned. (Such applications already exist, but RFID technology can simplify and expand their market reach.) A second concern is when personal data are actually stored on an RFID tag. This is less likely in the short-term retail setting, due to the extra cost of tags with this capability, but it has already been proposed for applications such as airline baggage tracking. It is conceivable that declining costs would allow this approach in the retail sector. Finally, as RFID tags proliferate, it might be possible to uniquely identify individuals from their "RFID signature." This could be done through either an actual RFID identifier, such as future US passports, or through the presence of specific and unique combinations of individually non-specific tags. Such applications could result in the collection and dissemination of traditionally obscure personal information.

These development activities and concerns have spurred an active policy debate. In a 2004 speech, Senator Patrick Leahy of Vermont, the ranking Democratic member of the Senate Judiciary Committee, described the issues arising from RFID technology as "the defining privacy challenge of the information age." He wants to "encourage public dialogue in both the commercial and public sectors before the RFID genie is let fully out of its bottle." (Leahy 2004) Several legislative bodies, including at least sixteen state legislatures and the US House of Representatives, are debating regulations that limit the uses of RFID technology in retail settings. They have proposed policies such as mandatory labeling of packages with RFID tags, mandatory consent for data collection, and required detaching or destruction of tags before a consumer leaves a retail setting. Simultaneously, consumer advocacy groups, in the US and elsewhere, are protesting retailer plans for RFID and are

already organizing a boycott of Tesco. Despite these reactions, a clear and comprehensive analysis of whether such policy approaches take into account the impact of RFID technology on national security, economic efficiency, and individual privacy and civil liberties does not yet exist. This work addresses that void by providing answers to two key research questions:

- What is an appropriate conceptual and economic framework that will consider the costs and benefits, across many stakeholders, of using RFID information systems?
- Using the developed framework, what are the implications for costs and benefits, and for the adoption of RFID technology, for a range of different proposed policies?

The bulk of this chapter provides a more thorough overview of the essential issues of the debate: the nature of privacy and personal information, some key historical examples that demonstrate the technology–policy interaction as it impacts privacy, efficiency, and security, and the basics of RFID technology, applications and policy-relevant issues.

1.2. Privacy and Personal Information

Consideration of the tradeoffs between security and privacy first requires an understanding of what is meant by privacy. The American Heritage dictionary defines privacy as "a. The quality or condition of being secluded from the presence or view of others. b. The state of being free from unsanctioned intrusion: *a person's right to privacy*." This definition seems clear, and further, many people are comfortable with a practical approach, akin to Justice Potter Stewart's view that he couldn't define obscenity, but would know it when he saw it. But, upon deeper investigation, a more nuanced and contextual nature of privacy becomes evident.

For example, even operating strictly within the legal domain, scholars (e.g., (Gormley 1992) have proposed fairly complex and situational structures:

> "1)Tort Privacy (Warren and Brandeis's original privacy); 2) Fourth Amendment privacy (relating to warrantless governmental searches and seizures); 3) First Amendment privacy (a "quasi-constitutional" privacy which exists when one individual's free speech collides with another individual's freedom of thought and solitude); 4)Fundamental-decision privacy (involving fundamental personal decisions protected by the Due Process Clause of the Fourteenth Amendment, often necessary to clarify and "plug gaps" in the original social contract); 5)State constitutional privacy (a mish-mash of the four species, above, but premised upon distinct state constitutional guarantees often yielding distinct hybrids)."

More recent works have attempted to create a general classification based on some of the recurrent characteristics of privacy conceptions in a wide range of fields. Solove (2002b) sees six general categories:

> "(1) the right to be let alone – Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; (2) limited access to the self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of certain matters from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one's personality, individuality, and dignity; and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life"

Solove recognizes several criticisms of this typology, and then goes on to argue that a pragmatic approach, grounded in specific practices, is more useful. This practical approach embeds an understanding that much of the contemporary debate is centered on the impact of technologies that are specific to the digital world and the heightened importance of personal information (Etzioni 2002; Slobogin 2002; Stanley and Steinhardt 2003). Bezanson (1992) is more explicit in making the same point when he asserts, "Social attitudes are too diverse and decentralized, and the emphasis on individualism too great, to argue for any one set of social norms about communication. Accordingly, … privacy should be premised on the individual's control of information." In keeping with these views, subsequent discussion is restricted to information privacy, a subset where one definition, alluded to by Bezanson,

predominates, and has for many years, partly due to strong advocacy by its original proponent, the influential Alan Westin. (Westin 1967)

1.2.1. Personal information

The dominant view with respect to information privacy is that "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Westin 1967) Various versions or extensions of this definition are widely accepted and have been applied regularly since Westin's formulation, especially when considering the electronic collection or dissemination of information. (e.g., Ware 1977; Cranor, Reagle et al. 1999; Harris Interactive 1999; Sheehan 2002) Thus, the notion of information privacy, although of special relevance in today's "digital" world, has already been advocated for more than thirty years.

A number of scholars have recently taken different approaches in specifically considering the case of Internet privacy. For example, Byford (1998) argues that while privacy is based on cultural notions of property, this model can be applied to cyberspace which "represents not merely a set of technological innovations but also a cultural context for social interaction which is shaped and defined by those moving within it." Byford goes on to argue "collecting personal data affects not only the individual's sense of self but also the formation of structural relations and the distribution of social power…." This is evidently a different notion of privacy than Westin's, which implies that, despite the popularity of the Westin conception, it is very difficult to reach a simple and encompassing definition of privacy. One essential difference between these two is that while Westin values personal information as the property of the subjects of that information, Byford places value on the social relations and power that arise from collecting personal information.

Research in alternative fields, such as the economic value of information, presents other views of the nature of information privacy. Posner, for example, argued for an economic efficiency definition of privacy that contains several aspects:

> "(1) [T]he protection of trade and business secrets by which businessmen exploit their superior knowledge or skills (applied to the personal level, as it should be, the principle would, for example, entitle the social host or hostess to conceal the recipe of successful dinner); (2) generally no protection for facts about people-my ill health, evil temper, even my income would not be facts over which I had property rights although I might be able to prevent their discovery by methods unduly intrusive; (3) the limitation, so far as possible, of eavesdropping and other forms of intrusive surveillance to surveillance of illegal activities." (Posner 1978)

In Posner's eyes, there are types of information that should be treated as private property, and that markets will suffice as a management mechanism, but personal information ("facts about people") is not among them. Instead, he proposes that such information should be treated as a public good. In economic terms, this means that personal information possesses two attributes: it is non-exclusive, and non-rival. Facts about people are non-rival because the use of them by one individual does not prevent similar consumption by other individuals, and they are non-exclusive because once those facts become general knowledge, it is very difficult to prohibit other individuals from using them. (Nicholson 2002) Posner's idea of personal facts as a public good is counter to Westin's definition, which views personal information as a private good. Contrary to both views, though, some empirical research has shown that consumers behave as if they do believe that their (online) personal information is a private good, while only the collectors of such information believe that it is public. (Rose 2001) In contrast to Posner, Varian and Shapiro (1999) offer an economic view of personal information that is more in keeping with Westin. Although they do not refer to private information as an economic good, they suggest that firms (especially Internet-based) can and should collect personal information about

customers, in order to understand their behavior, and be able to offer differentiated products and prices.

1.2.2. Why Privacy Matters

These different and largely abstract theoretical, legal and economic views of privacy have substantial policy significance; they have lead a number of international legislative and policy generating organizations to establish information privacy as a basic right within a free society. Some of the principal instruments establishing this are:

> The European Data Privacy Directive 95/46/EC (1995), which sets the mandatory standards for the legislative framework in each European member state; the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) (2000), which does the same thing for Canada and its provinces; and the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), which underpin much of the US privacy law. (Perrin 2005)

Beginning with its preamble, European Directive 95/46 clearly draws on the Westin model when it states "Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals," and then goes on to define personal data as:

> [A]ny 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; (1995)

The loss of control of personal information raises a number of possible concerns for individuals. One assessment of the central privacy loss dimensions reports that they are collection, internal, and external unauthorized secondary use of personal information, errors in personal information, and improper access to personal information. (Smith, Milberg et al.

1996) With item-level RFID tagging, these concerns give rise to several specific threats. The first of these is profiling, which is the collection of information linked to personal data and the classification of that information into expected behaviors. (Weinberg 2005) An example of this would be when a retail store tags products with unique codes that are linked to an individual at the point-of-sale, and used to create a customer database.

A profiling capability leads directly to a second threat, which is action based on the profile. (Weinberg 2005) As RFID systems proliferate, it might be possible to uniquely identify individuals from their "RFID signature" and trigger specific responses such as direct and targeted marketing as a consumer's habits are learned. This could be done through either an actual RFID identifier, such as planned next generation US passports, or through the presence of specific and unique combinations of non-specific tags. Even without the ability to identify a specific individual, the presence of personal information that sorts an individual into a particular category can be used as a trigger. Finally, RFID technology in particular can be used to locate individuals. A large RFID network thus offers the possibility of global surveillance, and has been referred to by some using ominous terms such as big brother, or the Panopticon (the prison architecture proposed by Jeremy Bentham, enabling an observer to monitor all prisoners surreptitiously.) (Weinberg 2005)

Other potential costs and benefits, arising from specific aspects of RFID technology, are discussed later. The threats described here are more general, and in many cases technologies enabling these capabilities already exist. RFID as a means of collecting information, operating in conjunction with today's large-scale storage and data mining tools, greatly simplifies each of these intrusions, and expands their potential reach, but is not the sole or even necessary cause of these more general threats. Indeed, it is merely one of the latest in a

long line of technologies that have raised similar concerns. A brief review of some historically significant examples is illustrative of the implications that such technologies can have.

1.3. Technology/Privacy tradeoffs

Information privacy has been a matter of public debate in the U.S. since late in the nineteenth century. Prior to that era, the American conception of privacy, such as it was, was tied to physical notions of property, territory, and the ability to find solitude within one's home. (Byford 1998) As today, there was not an explicit constitutionally guaranteed right to privacy, but today's technologies were unimagined, the federal government collected little information about citizens, and physical privacy could be found within the home ("a man's home is his castle") or by simply moving to the frontier. (Smith 2000) Along with the closing of the frontier (as per the "Turner thesis"), the last decades of the 1800s also saw rapid population growth and the first "modern" technologies that threatened to intrude upon people's lives. (Lester 2001)

1.3.1. Instant Photography

Among the many new technologies of that era, the high-speed printing press, introduced in 1886, and the Kodak camera, in 1888, had particular impact, and led some to perceive that an invasion of the private life had begun. (Smith 2000) In particular, they inspired the 1890 publication of one of the most influential of all legal publications, "The Right to Privacy", by Samuel Warren, and future Supreme Court Justice Louis Brandeis. Warren and Brandeis claimed that "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical

devices threaten to make good the predication that 'what is whispered in the closet shall be proclaimed from the house-tops.'" (Brandeis and Warren 1890)

Brandeis and Warren recognized that common law already contained a property rights view of privacy, which had been applied by courts as the rationale for protecting various individuals from harm. However, they then famously argued that "the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone." (Brandeis and Warren 1890) The motivation for the article has long been mythologized as a reaction to specious press coverage of members of Warren's family (possibly his daughter's wedding), but that legend has been debunked, and Smith, among others, cites patrician elitist reaction to the rise of mass cultural values as the likeliest foundation for the article. (Smith 2000)

Further inspection of this line of thought reveals that Warren and Brandeis believed that the press, as an institution, was symbolic of an impersonal mass culture, and that it had overstepped "the obvious bounds of propriety and of decency." Bezanson argues that their view of privacy "reflected the fact that personal identity developed in discrete institutions…. [Privacy] represented an attempt to protect the functioning of those discrete social institutions from the monolithic, impersonal, and value-free forces of modern society, by channeling that which is personal to these discrete institutions and foreclosing it to society at large." (Bezanson 1992) Further, the late 1800s were the zenith of "yellow journalism", which took advantage of the new technologies and the rapidly growing cities full of poorly educated (and frequently immigrant) masses, to achieve true mass circulation. (Gormley 1992) Thus, it seems clear that social conflict was at the heart of the matter, but regardless of the true inspiration for the article, it marks a clear and dramatic revolution in the

understanding of privacy beyond the personal property notions that were critical to the common conception of privacy, and to a specific privacy tort allowing individuals to enforce their right to be let alone. It also demonstrates that the development, use, and societal acceptance of new, information-gathering, technologies have been intertwined with a debate between privacy and economic activity for more than a century.

1.3.2. Wiretapping

After "The Right to Privacy" was published, it took more than a decade before the law caught up with the upheaval in technology, society, and ideas about privacy. This occurred with the passage by the New York legislature, of the Civil Rights Act of 1903, explicitly stating that if persons had not given written consent to the use of their name, portrait or picture, they were entitled to legal redress. (Smith 2000) Other states, but not the federal government, followed suit in the ensuing decades. Brandeis continued to exercise and elaborate his views on this matter, extending them from instant photography to other technologies, during his tenure on the Supreme Court, in particular, with the dissenting opinion to *Olmstead v. U.S,* (277 U.S. 438.) Olmstead and his colleagues had been arrested in Washington State for running a cross-Canadian border liquor smuggling ring, based on covert wiretaps of his home and office telephones. While the Court upheld the evidence on the grounds that listening was neither a search nor a seizure, and thus, not a Fourth Amendment violation, Brandeis presciently offered this dissent:

> "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the government, without removing paper from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.
>
> ….

> Whenever a telephone line is tapped, the privacy of persons at both ends of the line is invaded and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping."

Despite Brandeis's foresight, it took forty more years, another explosion in the gadgetry of surveillance, and the notorious use of wiretaps by the FBI in their search for communist sympathizers or other risks to the national defense, before policies were enacted that accepted this view of the tradeoffs between privacy and security. Although this period was marked by technical advances in transmitters, microphones, and miniature televisions, et al., state attempts to curb electronic surveillance failed due to overly broad exceptions, and the courts continued to hold the notion that violation of the Fourth Amendment only occurred when there was a physical trespass or seizure of material goods. (Gormley 1992) This private property view of privacy was still prevalent until *Katz v. United States*, in 1967. Katz was arrested after an electronic listening device attached to the outside of a telephone booth recorded evidence of his bookmaking operations. The Supreme Court decision in this case marked a true turning point in shifting the focus beyond the pure property interest that had been established in *Olmstead*, and established a number of factors for the change.

> "The Court noted that the location of a person's activity should not be the primary factor in determining whether or not the activity deserves Fourth Amendment protection: in modern society, many activities that formerly might have been able to take place in the privacy of our homes now take place in semi-public areas…. Second, the Court was beginning to realize that in an age where pure information was becoming more valuable as a commodity, the Fourth Amendment must protect private speech and conversations as well as more tangible possessions. But primarily, the Court was acknowledging the fact that given the new technologies available in government investigations, a consideration of *how* the government agents (or their devices) carried out surveillance was no longer a meaningful factor." (Simmons 2002)

The *Katz* ruling first established the "reasonable expectation of privacy" criterion. Shortly thereafter, and in reaction to the Court's ruling, came the 1968 passage of the

Omnibus Crime Control and Safe Streets Act. In particular, Title III of the Act attempted to enact legislation enforcing the Court's new interpretation of privacy. The Act required federal agents to secure a warrant prior to unconsented interception of wire or oral communications, that the warrant must be based on probable cause, and that the target of surveillance must be notified within ninety days, among other provisions. Notably, Title III does not account for other technologies for data or visual surveillance, and has various other enforcement loopholes regarding the attempt to halt the manufacturing of devices that are "primarily useful" for monitoring conversations. (Smith 2000) Therefore, it was a step back from *Katz*, where the court appears to have discarded particular consideration of the type of technology involved in the surveillance. Further, the Act allowed for wiretapping in cases of national security, which is a clear statement that legislators were cognizant of a tradeoff between privacy and national security. This is akin to viewing personal information as a public good, in the appropriate circumstances.

1.3.3. Recent Examples

In subsequent years, and partially in reaction to Watergate-era revelations about how the Nixon administration had disregarded privacy and the concurrent general loss of trust in government, there was an epidemic of Federal government regulations and loopholes, pertaining to data privacy. Most of these regulations are specific responses to particular perceived issues, often arising from distributed electronic databases containing personal information. A non-comprehensive list of these regulatory actions includes the Privacy Act of 1974, the Family Educational Right to Privacy Act of 1974 (also known as the Buckley Amendment), the Right to Financial Privacy Act of 1978, the Cable Communications Policy Act of 1984, Employee Polygraph Protection Act of 1988, the Video Privacy Protection Act

(VPPA) of 1988, the Telemarketing Protection Act of 1991, the Driver's Privacy Protection Act of 1994, and the National Do-Not-Call Registry, established in 2003.

The VPPA provides a good example of how these regulatory actions came to pass. The VPPA was enacted after the failed 1988 nomination of Judge Robert Bork to the US Supreme Court. At the time of the nomination, and presumably in an attempt to embarrass the nominee, a local paper, the Washington, DC City Paper, obtained and published Judge Bork's video rental records. As a result the Senate passed legislation designed to prevent the disclosure of personal rental records of "prerecorded video cassette tapes or similar audio visual material." (EPIC 2002) The major provisions of the act include a general ban on the disclosure of personally identifiable information unless a consumer consents in writing; disclosure of personally identifiable information to law enforcement requires a valid warrant or court order; exclusion of any evidence obtained in violation of the law; general preferences can be disclosed for marketing purposes but individuals can opt out; a requirement for a video store to destroy rental records within one year after an account is terminated; and civil remedies for violations are at least two thousand five hundred dollars. (EPIC 2002) However, the law does not explicitly deal with other customer records that a video store might possess, such as DVD or video game rental history, or purchases from the same store. As a result, although the VPPA is well intentioned and effective within a narrow scope, its excessively specific and reactive nature leaves it as one among many regulatory acts that don't combine to form a coherent whole. Many of the other recent regulatory actions mentioned above are similarly compromised. Regulations tend to be overly specific, and unable to keep up with evolving technology. Further, they either allow government or private organizations to still access the same private information that was being protected, make exceptions for

national security reasons, or have been weakened by subsequent government action. (Smith 2000)

1.4. RFID Technology and Applications

RFID is often viewed as a subset of a larger class of technology, known as automatic identification (Auto-ID), which also includes common technologies such as barcodes and smartcards, among others. RFID systems are unique in that they can be scanned at a distance, without overt physical interaction between the ID and the scanner. This distinctive property enables many possible applications, and gives rise to many perceived costs and benefits associated with using the technology, as discussed below.

1.4.1. RFID Technology Basics

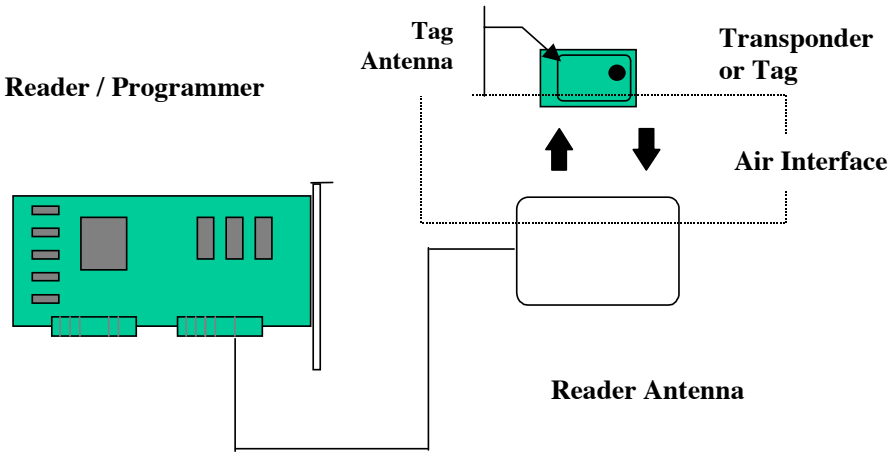


Figure 1-1: Typical RFID System Architecture (Balkovich, Bikson et al. 2005)

Although many specific architectures are possible, a generic RFID system consists of a tag (or transponder) and antenna, communicating via an air interface with a reader antenna. The tag is attached to an identifiable object, and the reader antenna is directly connected to a reader (sometimes referred to as a programmer or interrogator) that either maintains or

communicates with an information management system. A simple schematic is shown in Figure 1-1.

The RFID tag is always "listening" for a signal from the reader, and responds, when queried, by transmitting data back to the reader.[1] Data are transferred by one of three methods: amplitude shift, frequency shift, or phase shift keying. This modulation is typically done over three different basic frequency ranges: 100-500 kHz (low), 10-15 MHz (medium), and 2.4-5.8 GHz (high.) Other ranges are also used, and there is a current discussion ongoing to try and create agreed international standards. The choice of frequencies impacts both data rates and signal range. Typical performance characteristics of the common frequency bands are shown in Table 1-1, below.

Table 1-1: Typical RFID System Characteristics

Frequency Band	Characteristics	Typical Applications
Low 100-500 kHz	Short read range (<1 foot) Inexpensive low reading speed	Access control Animal identification Car immobilizer[2] Inventory control
High 10-15 MHz	Medium read range (<1 meter) potentially inexpensive medium reading speed	Access control Apparel item tracking Baggage tracking Pallet/container tracking
Ultra High (UHF) 850-950 MHz 2.4-5.8 GHz (Microwave)	Long read range (<10 meters passive, <100 meters active) High reading speed Expensive	Railroad car monitoring Supply chain management Toll collection systems

[1] Much of the following technical discussion is drawn from AIM Inc WP-98/002R2, "Radio Frequency Identification RFID: A Basic Primer"

[2] A car immobilizer provides vehicle theft deterrence. It is a device that must be within proximity of the car in order for a critical part, such as the fuel supply or transmission, to work properly.

A further distinction among tags is their power source. Tags can either be active, meaning that they are powered from a local source, or passive, meaning that they are powered by an inductive coupling when in the near field of a reader. Typically, passive tags store and transmit a fixed ID number, which has been pre-programmed at the point of manufacture, and is only useful when that number can be correlated with additional information in a database. In addition to transmitting an ID, active tags can often record information on the tag. As a result, they are sometimes integrated with additional sensors and electronics, allowing for enhanced signals and data.

Frequency, reader power, tag power (active vs. passive), and environmental conditions affect read range. As a result of their power source differences passive devices are usually smaller than active devices, have a shorter read range, and virtually unlimited operational lifetime, although they do require a more powerful reader. Active devices have a lifetime constrained by the local power supply, but can transmit over a long range, and can include onboard processing and read/write capability. An example of a state of the art passive device is the Hitachi μ-Chip, with a current version shown in Figure 1-2. It operates at 2.45 GHz, transmits a fixed 128-bit code, and can be read at a range up to 30 cm, with a typical reader. Hitachi has recently announced a newer μ-Chip; it has the same operating characteristics, but is about 85% smaller than the pictured device, and is 7.5 microns thick, as compared to typical paper thicknesses of 80 to 100 microns. (Hara 2006) Other recent developments include printers from Zebra Technologies that embed the RFID tag directly into a product label. (Garfinkel, Juels et al. 2005)

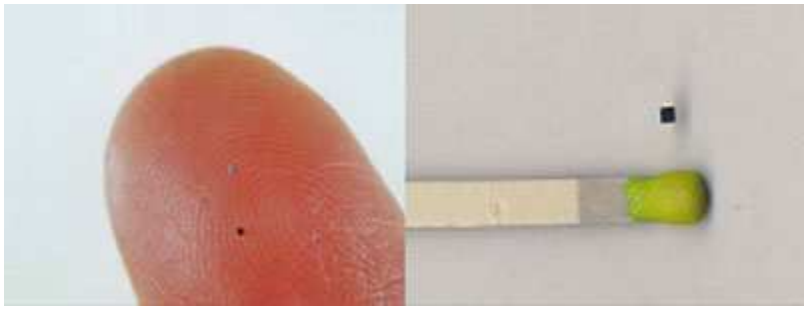


Figure 1-2: Hitachi μ-chip shown on a finger, and next to a matchstick.

An RFID tag can be programmed to store and transmit any information that fits within the tag's memory and power constraints. In practice, many RFID tags and systems follow a series of standards, known as the Electronic Product Code (EPC), which was developed by the Auto-ID Center in collaboration with universities including MIT. The EPC was explicitly developed with the intention of replacing the Universal Product Code (UPC) that is currently used within bar codes to identify many consumer products. The EPC Network is being promoted as an open worldwide standard that enables lower costs and easier adoption of the technology. An EPC tag is an RFID tag containing a serial number with a minimum of 96 bits in four partitions: a header identifying the EPC version, a manager number identifying the company associated with the product, an object class identifying the product type, and a unique serial number. Thus, an EPC tag code can uniquely identify a product, and provides a pointer to a possible database of detailed transaction history for any given product. The targeted high adoption rate and low cost means that EPC tags will be quite simple and unable to incorporate significant security features, such as encryption. The current standard, generation-2, does contain a kill feature, whereby a tag can be rendered permanently inoperable when it receives the appropriate command. (Garfinkel, Juels et al. 2005)

The wide range of product capabilities results in RFID tags that span a wide range of prices. The simplest tags, typically passive, high-frequency, short-range, and pre-

programmed by the manufacturers, are now available for about thirteen cents apiece in large quantities. Prices have been declining at a rate of about 40% in recent years, although this rate is expected to slow, and ten-cent tags are not now expected before 2008. (O'Connor 2005a) The ultimate goal of tag manufacturers is passive tags for less than five cents, which is seen as an enabling price-point for item-level tagging. Such tags are not now expected until after 2010. (Das 2005) Active tags, especially those integrated with sensors and memory, span a cost range from approximately $1/tag to as much as $100/tag. (Das 2005) Tags, especially those equipped with a battery and/or other complex components, might have additional costs, such as the need for proper environmental handling or disposal, although these issues haven't yet been well-quantified.

1.4.2. Applications overview

Although early research in areas similar to RFID dates at least back to the WWII era, as a part of IFF (Identification, Friend or Foe) systems on allied military aircraft, the first productive usage, such as the Electronic Article Surveillance anti-theft systems developed by Checkpoint and Sensormatic, occurred in the 1960s. (Landt 2001) Significant technical developments in the 1970s and 80s led to a widespread proliferation of RFID systems into applications such as animal tracking, remote keyless entry into cars, and highway toll collection. (Garfinkel, Juels et al. 2005) Today, the EPC global organization and other proponents of RFID technology have already demonstrated its capabilities in a wide range of applications. Familiar examples include employee identification badges and other access control systems, transportation systems such as E-Zpass electronic toll collection and ExxonMobil Speedpass™. (Federal Trade Commission 2005) In addition to these recognizable applications, RFID is already widely used or planned for a range of industry

sectors. For example, in healthcare the technology is being used to certify legitimate drugs and detect counterfeits, maintain a product pedigree if a recall is necessary, and monitor patients and procedures in hospitals. Pfizer has already announced plans to have all Viagra shipments labeled with RFID tags in 2006. (Smith 2006) Other businesses have also announced widespread plans for RFID, including baggage handling by airlines and airports, and monitoring the pedigree of cows or birds, in order to limit the possibility of mad cow disease or avian flu entry into the food chain. (EPCglobal 2004) RFID systems are also being used in a number of novel ways, including: in casino chips as both an anti-fraud measure and a way of tracking gambler behaviors, in smart washing machines that can detect and automate cleaning behavior in tagged clothes, and by a variety of school systems that monitor student attendance. (Weinberg 2005)

RFID systems are also already widely used in the public sector. At least thirteen federal agencies, including the Departments of Defense, Energy, Health and Human Services, Homeland Security, Labor, Sate, Transportation, Treasury, and Veterans Affairs, as well as the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration and Social Security Administration report that they use, or plan to use, RFID technology in applications including logistics and materials tracking, access control, and monitoring individuals. (GAO 2005) The Department of Defense mandate, which was finalized on July 30, 2004, is a well-known instance of government use of RFID technology. The mandate, issued by Acting Undersecretary of Defense Michael Wynne, specifies a multi-year phase-in, with tagging of certain products required on January 1, 2005, and building up to "all cases and pallets of all commodities shipped to all DOD locations" by January 1, 2007. (Roberti 2004) The State Department's plan, using RFID as a component of its next generation electronic passport, has also been

widely reported and has drawn a fair amount of controversy. Commentators have noted that the original plan called for a passport that would be continuously broadcasting information to anyone who wanted to read it, enabling surreptitious monitoring by anyone with a reader. (Schneier 2004) Although the State Department addressed some concerns in subsequent plans, a US RFID passport is now being issued, in spite of a number of unresolved issues.

1.4.3. RFID in the commercial retail sector

Although the above list includes some very high profile applications of RFID, the retail industry supply chain draws much of the interest in and debate over RFID technology and policy. Unlike most public sector uses, widespread deployment of RFID in these applications can have a large impact on varied types of stakeholders: individuals, firms, the government or other regulators, and society as a whole. The single most significant factor motivating this interest was the Wal-Mart mandate. In June 2003, Wal-Mart's logistics operations announced a mandatory RFID adoption plan for their top one hundred retail suppliers, beginning in January 2005. The mandate was expanded to their top three hundred suppliers by January 2006, and the top six hundred by 2007. (Roberti 2005) In the wake of this mandate, many competitors followed suit, including Target, Albertson's, and Best Buy in the United States, as well as Tesco and Metro AG in Europe. (Cavoukian 2004; Hardgrave, Waller et al. 2005; Wyld 2005)

Retail sector RFID proponents usually identify a series of potential benefits associated with implementing the technology throughout a supply chain. These generally include an increased efficiency of operations, reduced costs and improved customer satisfaction within the supply chain, (i.e., when another business is the likely customer). (Wyld 2005) These benefits derive from several properties of RFID technology, in contrast to existing bar codes,

including the unique identification of a particular product and rapid scanning of many products at once. (Kelly and Erickson 2005) Additional benefits not generally discussed arise from the privacy threats outlined above. Since RFID could enable a retailer to profile its customers, it would also enable the retailer to segregate those customers into different markets, and treat them differently. (Acquisti and Varian 2005) As a result, a retail firm with such capability could capture a substantial portion of existing consumer surplus (the difference between the maximum that consumers would be willing to pay for a good and what they actually do pay). An analytical approach for understanding cost and benefit issues, for each of the stakeholders in the policy debate, constitutes the bulk of this dissertation.

1.5. RFID Policy Debate

The review of the historic impact of technologies upon the privacy/security/efficiency debate highlights three primary groups of stakeholders: individuals, firms, and government/regulatory bodies. In addition, there are broader societal concerns raised by the commons-like nature of the data that can be collected by RFID information technology systems. As these concerns are frequently not addressed by any of the other actors in the debate, it is reasonable to include them under the auspices of society as an additional stakeholder in the current debate.

Many of the stakeholders have already made policy proposals, over the past several years. These encompass a wide range from purely technical solutions such as encryption and passwords, to purely policy solutions, such as the proposed "RFID Bill of Rights" that specifies a series of guiding principles for users of RFID systems. (Garfinkel, Juels et al. 2005) In between are alternatives such as offering customers the option of killing tags at the point of sale and various levels of consumer opt in/opt out. Each of these policies stands to

have a different impact on the costs and benefits of RFID to each stakeholder group. The substance of these policies and their impact will be explored in more detail in chapter four, but their presence highlights a fundamental paradox, which is the desire for stable rules governing a technology with so much uncertainty that it is virtually impossible to predict the evolutionary path of that technology. (Odlyzko 2006) This uncertainty is demonstrated by the decade-long cycle of claims that, for example, RFID will lead to "a new era of innovation and opportunity" (Auto-ID Labs 2000), followed by various policy responses. It is this uncertainty which highlights the need for an analytic framework that can be used on a continuous and evolving basis, by incorporating new information both from the marketplace and about the technology, as opposed to a "definitive" yet static analysis.

1.6. Organization of Dissertation

The remainder of this dissertation is organized as follows. Chapter two develops the methodology used during the course of research and provides a review of the key research literature in relevant areas. Chapter three develops a basic conceptual framework, elaborating on the stakeholder groups and their costs and benefits, which can be used for assessing the impact of technologies such as RFID. Chapter four provides an overview of the many policies that have been proposed in this area, and uses the Chapter three framework to explore several prominent options in greater detail. Chapter five develops an economic model that integrates many of the costs and benefits incorporated into the framework. Chapter six characterizes the results of the model, using the policy examples from chapter four, and extrapolates the model output into a scenario analysis considering all factors in the framework. Finally, chapter seven offers a series of conclusions, policy recommendations, and suggestions for additional research in this area.

2. Research background and methods

This research developed as a natural successor to earlier RAND Corporation work that examined the uses of RFID in corporate access control systems. (Balkovich, Bikson et al. 2005) That research used a replicated case study methodology to demonstrate that even in an apparently straightforward application, such as corporate access control, RFID systems and data were put to many uses, and that policies regarding those uses had not been clearly thought out. For example, in addition to the intended and overt uses of RFID (location entry and exit control), most of the participants used data these systems generated to monitor employee behavior for other reasons, such as security investigations triggered by suspected illicit activities, or workplace culture tracking in remote office locations. In most of these instances, the enterprise did not advertise that the RFID systems and data might be used for such purposes, did not articulate policies for or document its procedures for these additional uses, and did not keep clear records of when and how those "supplementary" uses were authorized and executed. Although private organizations in the US can legally operate in this manner, these findings highlight many of the issues associated with broader applications of RFID, such as the presence of multiple stakeholders, and the numerous costs and benefits associated with this type of technology, beyond the initial application objectives.

The appearance of these concerns in such a limited application of RFID led directly to interest in examining a broader set of technology and policy issues and to the first attempts to formulate the research questions and methods presented in this work. Initial surveys of published research showed that it is common to consider the interests of one group of stakeholders, across several literature domains, but that there are few instances of meaningful multi-stakeholder analysis, and none that attempt to assess policy options in a rigorous qualitative and quantitative way for all of the stakeholder groups. This need leads directly to

the research reported here, which establishes a framework outlining all of the interests of each stakeholder group and then develops a quantitative economic model whereby tradeoffs in those interests can be understood. The remainder of this chapter describes the literature relevant to this research, and links the findings from those works back to the research questions.

2.1. Literature Review

This research applies methods and concepts from across a range of academic and policy disciplines. RFID, individual privacy, and tradeoffs between privacy and security or economic efficiency are the primary foci of this research, and these literatures are reviewed here. This review differs from the background material presented in Chapter 1, in that it strictly focuses on research that is methodologically relevant to the qualitative and quantitative contributions presented in this work. The review starts from a large multi-disciplinary body of research into privacy, and the economics of privacy, and culminates with RFID-specific research publications. Privacy itself is a very expansive discipline, with active research conducted by legal scholars, sociologists, psychologists, historians, and economists among others. As a result, a broad review was conducted across a number of relevant topics, accompanied by a more detailed study of specific areas of interest, including theoretical economic models, empirical studies of individual behaviors with respect to privacy, and applications of the economic commons model to personal information and privacy.

There is also a large quantity of technical literature about RFID systems and their operation, but peer-reviewed policy-relevant RFID research has only recently begun to appear. Consequently, policy materials drawn from a variety of sources and methods are reviewed here, including cost-benefit research, policy analyses, and technical reviews of policy

options. Additionally, there is a substantial quantity of alternate source materials, such as news items, trade journals, publications from consultancies and advocacy groups, and government reports. These provide some useful background to the debate, and are referenced where appropriate, but given lower priority than reviewed sources.

In all of these cases, the same literature gathering approach, consisting of the selection of relevant keyword searches through targeted databases, was applied. The primary databases searched were Wilson Select Plus, Psycinfo, Econlit, and Google Scholar. In addition, both the RAND Library's TDNet service and the Google News service were used to create keyword alerts for new journal or news articles discussing RFID or privacy, thereby ensuring that the compiled literature remained current.

2.1.1. Privacy Literature

Academic dialogue on privacy has existed since at least the seminal "Right to Privacy" by Brandeis and Warren. (Brandeis and Warren 1890) Since that time, it has become a multi-disciplinary arena attracting research from domains including law, sociology, political science and psychology, and relying on analytic methods including legal analysis, behavioral models, and empirical research, among other approaches. The sensitive nature and high profile of privacy has even led to numerous thoughtful works of more popular literature. (Regan 1995; Brin 1998; Garfinkel 2000; Smith 2000; O'Harrow 2005) Legal scholars, for example, have made many attempts, since Brandeis and Warren published the original "Right to Privacy", to classify privacy, understand how it interacts with evolving technologies, or what it costs to society. (e.g., Kang 1998; Froomkin 2000; Post 2001; Cate and Litan 2002; Ku 2002; Simmons 2002; Slobogin 2002; Solove 2002b; Solove 2002a) Of more immediate relevance to this research is literature that addresses how individuals behave in situations where

technology can be used to profile them. Among social scientists, this is often known as personalization, which is the process of gathering personal information that enables a firm to target products or services to match a customer's tastes. The customer is often an unknowing participant, whose preferences are revealed through behavioral history. (Murthi and Sarkar 2002) One significant feature of the Internet is its ability to allow firms to engage in this activity, by linking customer behavior with various data mining tools and behavioral models. One of the best known examples of a firm engaging in this activity is the online retailer Amazon, which uses purchasing history, especially for items such as books and music, to offer recommendations, coupons and bundles to customers. In the past, as noted earlier, Amazon has apparently experimented with extending this system to differential pricing. (Weiss and Mehrotra 2001)

A result of both the Internet's potential for personalization, and activities by Amazon and others is that much, if not most, recent research on information privacy has focused on how individuals use the Internet. Some of this research takes as its antecedent a long series of public opinion research that repeatedly shows that there are individuals who care about information privacy. (Harris Interactive 1999; Westin 1999; Westin 2001; see Kumaraguru and Cranor 2005 for a summary of more than 30 surveys by Westin and associates, dating from 1990-2003) In this work, Westin has proposed and continues to advocate a tripartite segmentation of individuals: fundamentalists who are extremely concerned about the uses of personal information, and resistant to any further privacy erosion; an unconcerned group who do not consider privacy issues; and a group of pragmatists, typically the bulk of the survey respondents, who have some concerns about privacy but are willing to sacrifice personal information if there are tangible benefits. (Taylor 2003) Other similar research has reported different segmentations of individual concern (Sheehan 2002), or that levels of

privacy concern are dependent upon other factors, such as cultural values (Milberg, Smith et al. 2000), but has maintained support for the idea that at least some segment of any sampled population expresses concern for privacy.

A number of attempts have also been made to explore and quantify factors that affect individuals concerns. One of the earliest was the development of an instrument called the Concern for Information Privacy, which identified four factors: collection, errors, secondary use, and unauthorized access, as the primary dimensions of individual information concern. (Smith, Milberg et al. 1996) More recent research has argued that individual responses are sensitive to the types of information collected, and the ways that data are used. (Cranor, Reagle et al. 1999; Phelps, Nowak et al. 2000) In both cases, individuals were generally more resistant when asked to provide identifiable information, such as credit cards or social security numbers, as compared to personal demographics, such as race, gender and socioeconomic status. Research has also looked at the significance of other factors, including gender, age, income, and education, to privacy concerns. (e.g., Phelps, Nowak et al. 2000; O'Neil 2001; Graeff and Harmon 2002; Dommeyer and Gross 2003) In general these studies find conflicting results, with some reporting that income has an influence on privacy concerns, but education does not, while others show that age, education and gender are significant, and still another suggesting that women are more concerned than men about privacy, but men are more likely to take privacy protecting actions. (Boritz, No et al. 2005) Thus, it seems that while there is a widespread agreement that individuals are heterogeneous in their concerns over privacy, the dimensions of those dissimilarities are not clear.

Studies have also been conducted into the consequences of privacy concerns. Several researchers have shown that beliefs about privacy affect consumer behaviors. Sheehan and Hoy (2000) found that individuals are less likely to use web sites when their privacy concerns

are high, and further, that they are more likely to take defensive actions, such as providing incomplete information, or notifying their Internet Service Providers (ISPs) about spam. George (2002) found that beliefs about privacy and trustworthiness have a significant affect on purchasing intentions. He observed that the more an individual believes in information privacy (the property view, in his terminology), the more negative their attitude is toward Internet purchasing.

So, the body of this behavioral research shows that as enterprise-level use of RFID expands into the retail setting, individuals are liable to react to the effect of RFID on individual privacy. These reactions can take the form of altered consumption behavior or defensive actions. However, the lack of clear behavioral models suggests further empirical research in that domain would be valuable. In the meantime, alternative methods of analyzing the actual impact of RFID can be employed. A number of specific economic models, describing individual behaviors with regard to privacy or the interaction between firms and individuals, are a good starting point for developing these alternative methods.

2.1.2. Economics Literature

The basis for a comprehensive economic analysis of the costs and benefits of RIFD, to multiple stakeholders, is drawn from a relatively large body of economic literature. This literature, broadly defined, includes both the so-called "economics of privacy," which includes attempts to describe how consumption-minded individuals behave with regard to privacy of personal information, and "behavior-based price discrimination," which is the idea that when firms recognize customers, they can use information about the customers to offer different prices. (Fudenberg and Villas-Boas 2006) Both domains are primarily theoretical, but there is some limited relevant empirical data. Presented here is a brief review of the most

relevant works from these fields of literature. For a much more thorough analysis, the forthcoming Handbook of Economics and Information Systems (Hendershott 2006) provides several relevant chapters, including "The Economics of Privacy" (Hui and Png 2006) and "Behavior-Based Price Discrimination and Customer Recognition." (Fudenberg and Villas-Boas 2006)

The use of personal information as a basis for matching customized products and prices to individual tastes has been widely studied. (i.e., Varian and Shapiro 1999; Ulph and Vulcan 2000; Taylor 2002; Wathieu 2002; Odlyzko 2003; Taylor 2004b; Taylor 2004a; Acquisti and Varian 2005; Chellapa and Sin 2005; Hermalin and Katz 2005) Much of this analysis does offer a link between price discrimination and privacy. Odlyzko, for example, argues that much of the motivation to reduce privacy is, in fact, based on a private sector desire to price discriminate. (2003) More recently, Acquisti and Varian have proposed a set of conditions whereby sellers will "find it profitable to condition prices on purchase history." (2005) They initially show that customers are sophisticated, so they adopt technology to make themselves anonymous, thereby preventing the retail firm from establishing a purchase history. The result of this is that the firm does not benefit from differential pricing. However, the authors then go on to demonstrate that if technology is too costly to allow customer anonymity, or if enough consumers are myopic, then price conditioning will be profitable. Taylor (2004a) offers both a similar analysis and conditions whereby incentives to collect information are increased. These include increased ability to identify individuals (or segments), increased valuation for high consumers, or an increased proportion of high consumers. In addition to these conditions, Varian and Acquisti suggest that industries where customer anonymity is difficult and where the marginal cost of enhanced services is

low but those services offer advantage to those customers might undertake price discrimination.

Interestingly, much of this analysis finds some counterintuitive results. For example, privacy regulation that increases the cost of information collection will reduce the firm's collection activities, which will, in turn increase the production of information by individuals. In some circumstances, this could lead to more total information being produced and consumed, and a net increase in welfare. The converse case, of cheaper collection resulting in less production of information, has also been found. (Hui and Png 2006) Although theses examples have primarily considered straightforward monopoly models, the introduction of competition or regulation has been found to produce even more varied (and indeterminate) results. For example, if multiple sellers engage in price discrimination, then the increased competition could reduce profits. (Fudenberg and Villas-Boas 2006) Ulph and Vulcan found that with homogeneous customers in a duopoly model of firm behavior, increased competition dominates firm ability to capture consumer surplus, thereby reducing profits. (2000) A similar result was found by Dewan, et al., who used a game theoretic model to show that if only one firm customizes its products and price discriminates, that firm improves market share and profits, relative to a competitor, which results in the competitor also offering customized products and price discrimination, with reduced overall profits to the firms. (2000) One analysis of regulatory models (Tang, Hu et al. 2005) uses a series of strategic games to look at privacy intrusions as a direct cost to customers, under three different regimes: mandatory standards, *caveat emptor*, and seal-of-approval programs; it finds that social welfare is maximized with different policy choices, depending on consumer tastes for privacy and retailer costs to protect privacy.

Clearly, a significant outcome of these results is the need for a better understanding of how people value privacy. As discussed above, there are any number of opinion surveys which show individuals are concerned. Recently, there have been a small number of empirical or experimental analyses examining the degree of value individuals place on privacy, and how that might affect their behavior. One of the most interesting and useful findings is that individuals behave as rational economic actors when confronted with realistic situations involving the use of personal information. Further, they are sensitive to the context in which information will be used, responding differently when aware that a third party can use personal information collected in a database. (Freidman and Wathieu 2005) Recent research at Cambridge University has verified and extended this finding, using a model of a sealed second price auction to determine a compensation level sufficient to entice individuals to reveal their location, via cell phone tracking. The most valuable results are the wide variation in sufficient compensation, ranging from 0 up to £400 for one month of participation in the study, and an observed sensitivity to how location information would be used. In situations where participants were informed that commercial parties were interested in the data, bids shifted upwards by a statistically significant amount. (Danezis, Lewis et al. 2005) Other research has found that it should be possible to construct consumer-demand curves for privacy enhancing technologies and policies, based on observed behavioral variations in Internet environments with varying degrees of privacy risk. (Baumer, Earp et al. 2005)

The existence of these research results implies the feasibility of creating an economic model to examine the tradeoffs between firms and individuals, when considering RFID policies. However, the sensitivity of both the economic models and empirical results to individual characteristics, and the great uncertainty in those characteristics, suggests that it is

difficult to truly predict how a heterogeneous population will behave when privacy regulations are imposed, and that any model based analysis needs to be cognizant of heterogeneity. It also highlights the value implicit in understanding both the characteristics of the population, and the sensitivity of policy outcomes to the uncertainties, and trying to find policies, or aspects of policies that will reduce these sensitivities.

2.1.3. Information Commons

The economic and behavioral research reviewed above generally focuses on the perspective of a particular stakeholder group, either firms or individuals. A small number of the discussed works do consider the interaction between firms and individuals. However, none appear to take into account the potential that RFID, or other information systems that can aggregate large quantities of consumer identifiable information, offer for large positive and negative externalities. An example of a positive externality would be lowered costs of RFID systems enabling new and beneficial applications, such as preventing or controlling the spread of bovine spongiform encephalopathy ("mad cow disease") via improved ability to monitor and control livestock herds. (Sullivan 2004) An example of a negative externality is the possibility for private information to be used for purposes beyond the firm's original intent, resulting in extra costs to individuals. One potential case of this was a 2001 test by the Stop & Shop supermarket chain, which used a program called "Smartmouth" to create nutritional profiles based on customer purchases. Stop & Shop considered sharing this information with HMOs, although it appears that the firm ultimately did not. (Tucker 2006)

One approach that can provide an analytic framework for these types of externalities is an extension of the traditional idea of an economic commons into an information commons.

In economic terms, a common good is one that is competitive and non-exclusive. That is, there is competition (also referred to as rivalry) involved in obtaining a common good, but it is not possible to exclude a person from consumption of a given good. This is in contrast with a public good which is both non-competitive (non-rival) and non-exclusive (Nicholson 2002) The traditional examples of an economic commons are a fishery or a common grazing area in a small town.

The idea of an information commons has become quite popular recently. However, it is usually applied to intellectual property, such as the development of Linux, the use of Wiki collaborative tools (e.g., Wikipedia), the Public Library of Science, (Kranich 2004) or the MIT OpenCourseWare program, which electronically publishes and makes available core teaching materials through a Creative Commons license. (Carson 2005) The idea that information systems themselves, or the information within them, might comprise a commons has been discussed at times over the past few years, but it has received only little rigorous academic attention, primarily from Regan. (2002) She argued that cyberspace is a commons due to the existence of standards for the flow of information, open entry to some points on the Internet, the need for social protocols, and the limited carrying capacity (bandwidth) within cyberspace. As an extension of this, she also argues that personal information is a common pool resource, due to the interdependence of information appropriation, which affects the quality of data, i.e., data can be polluted through misuse.

In the broader context of information security, Anderson (2001) proposed and developed a number of interesting ideas. He suggested that the value of an information technology product, to an individual user, depends on how widely it is adopted, and that such products often have high fixed but low marginal costs. He also proposed a related scenario as a tragedy of the information commons, as an extension of Hardin's (1968)

original Tragedy of the Commons.[3] Adar and Huberman (2000) offered a specific example of free-riding, one of the characteristics that can lead to a tragedy of the commons, in an analysis of user traffic on the Gnutella file sharing system. Their study showed that nearly 70% of users do not share files, and they argued that this leads to a degraded system. A 2005 replication of the Adar and Huberman study found that free-riding rates had increased to 85% resulting in a further degradation in Gnutella's performance. (Hughes, Coulson et al. 2005) Neither study offers suggestions about acceptable levels of free-riding, or the implicit tradeoff between quality and quantity of file-sharers, but this newer study does provide a brief discussion of the factors motivating developers to ignore the free-riding problem, specifically noting that users are a common resource for developers, and since most users are free-riders, the developers are unlikely to produce incentives to decrease free-riding.

Ayres and Funk (2002) offer a pricing based model as a solution to telemarketing and spam, whereby a market would be created requiring telemarketers (and spammers, etc) to pay a small fee, in order to transfer external costs from individuals. Although they do not explicitly cite this as a commons model, it is implicit in their contention that the model they offer stands to benefit both individuals and the telemarketing firms.

2.1.4. RFID-Specific Literature

There are hundreds, if not thousands, of news articles about RFID, often published in the trade press, and similar numbers of peer-reviewed articles discussing technical and operational aspects of RFID; there are also publications by consultancies, and at least one scare-mongering book ("Spychips" by Albrecht and McIntyre). Only a small body of quality literature addresses policy issues, or provides empirical and quantitative behavioral or cost-

[3] This is the phenomenon resulting from a conflict for resources between individual interests and the larger societal or common good. It is discussed in detail, in Chapter 4.

benefit data, related to RFID. The technical analyses are outside the scope of this research, most of the consulting reports can be succinctly summarized as marketing or business development for the publisher, and the news reports are typically verbatim echoes of the perspective of particular advocates. The remaining relevant and useful literature about RFID is divisible into three areas: technical proposals designed to address policy issues, especially concerns over privacy; policy proposals, reviews or analyses; and cost-benefit analyses of actual or theoretical retail industry deployments. Each of these is discussed here.

Within the past two years, there has been a proliferation of proposed technical enhancements or modifications to the basic RFID system architectures with the intention of addressing perceived policy issues. The majority of this work, e.g. Karjoth and Moskowitz (2005), starts from the presumption of a poorly defined privacy problem, and offers a particular technical approach with little broader context. In contrast, Ari Juels and his colleagues at RSA Laboratories[4] have produced high-quality work, including both reviews of many of the proposed technical solutions, and new concepts such as the blocker tag.[5] (Juels, Rivest et al. 2003; Juels 2005) Although the focus of the work is technical in nature, Juels does make note of the many different potential users of RFID, the conflicts of interest that might exist among these users, and the potential for broad costs and benefits. He then goes on to give a relatively thorough, albeit non-specialist, review of technical approaches to RFID privacy and also discusses the need for technology and policy to act in concert. (Juels 2005) The technical approaches reviewed include killing tags, renaming tags, cryptographic methods, proxying, distance measurement, blocking tags, and authentication. Despite this

[4] RSA Labs is the research arm of RSA Security, a well-known private firm specializing in the protection of digital information, including identity.

[5] The blocker tag is a specially designed RFID tag. When one is in proximity to ordinary RFID tags, it shields those tags from being monitored; when the blocker tag is removed, ordinary RFID tags will operate normally.

excellent work, Juels' research is primarily technical; consequently it falls short of a thorough analysis in at least three areas. First, he does not recognize that individual privacy is heterogeneous, despite the sociological and behavioral research, discussed above. Second, despite mentioning the importance of policy, his analysis deems policy to have an inferior role to technology and privacy issues, and does not do justice to the effect that policies are sure to have on all of the costs and benefits to all stakeholders. Third, despite awareness of the conflicts between different potential users of RFID systems and data, Juels' analysis doesn't recognize that these conflicts represent potential externalities to other stakeholders, and that a comprehensive analysis of the situation therefore needs to incorporate these broader societal costs and benefits.

A number of broader overviews purport to address the full spectrum of issues, or at least recognize the inherent conflicts between different stakeholders, either in an analysis of the current situation, or as a means to offering a proposed solution. (e.g., Cavoukian 2004; Good, Han et al. 2004; Harper 2004; Hutto and Atkinson 2004; Shah and Kesan 2004; Campbell 2005; Data Protection Working Party 2005; Eckfeldt 2005; Federal Trade Commission 2005; GAO 2005; Garfinkel, Juels et al. 2005; Kelly and Erickson 2005; Perrin 2005; Spiekermann and Ziekow 2005; Weinberg 2005; Wyld 2005; Hildner 2006) Unfortunately, many of these publications betray the perspective of their origins. For example, one recent, legal policy analysis, titled "Defusing the Threat of RFID" argues for widespread state level legislation that would limit data collection, with no real regard for the larger costs of such action. (Hildner 2006) Conversely, Jim Harper of Privacilla.org and the Cato Institute, lays out the potential costs and benefits of RFID in a structure that allows him to argue that any regulation would impede the natural development of the technology, and that social forces will arise to constrain any abuses. (2004) Government analysts have

produced reports, such as those by the privacy commissioner of Ontario, Canada (Cavoukian 2004) and the European Commission Data Protection Working Party (2005) advocating continued support for their existing regimes of information privacy protection.

Some of this literature (Garfinkel, Juels et al. 2005; Spiekermann and Ziekow 2005) contains specific policy proposals related to RFID that are worthy of more detailed analyses. This are is presented in chapter four, using the multiple stakeholder framework first presented in chapter three. Unfortunately, these more rigorous studies still present analysis that heavily focuses on how RFID will affect privacy, with only minimal attention given to the broader issues. For example, Garfinkel, Juels, et al., devote the majority of their analysis to outlining privacy threats raised by RFID deployment, and then conclude with a policy proposal (the "RFID Bill of Rights") that is primarily a response to the threats, regardless of the views of other stakeholders or even the diversity of individual views about privacy. (2005)

Kelly and Erickson do a better job of analyzing in laying out a broader set of issues, with explicit recognition of some firm benefits, such as better inventory control and easier checkout procedures, and of the need to balance these with consumer concerns over privacy and security. However, they jump directly from laying out the issues to asserting that "given the tremendous potential for harm to society, the use of RFID technology should be legally regulated." (Kelly and Erickson 2005) While this view is widely held by advocates for privacy and civil liberties, their argument lacks all awareness of the likely impact of regulation, both in direct costs and lost benefits.

One publication, "RFID and the United States Regulatory Landscape" (Campbell 2005), stands out as excellent qualitative work. It recognizes the many stakeholders who are involved in the RFID policy debate and contains a presentation of the many interactions that exist between the interests of all of those parties. For example, Campbell specifically notes a

"Government versus individual context" where he suggests that there is a balance between government use of RFID for purposes such as law enforcement, and public willingness to accept consumer-level RFID. Campbell also provides an assessment of many of the possible policy options. His work is lacking primarily in that it presents all of the interactions and assessments as a laundry list, with no attempt to create an analytical framework whereby the tradeoffs can be assessed in a more concrete manner. However, the recognition that each policy proposal should be weighed against the interests of each stakeholder is a valuable step. It provides a logical starting point for the construction of the framework that I propose in Chapter three, apply to RFID policies in Chapter four, and extend to the economic analysis in Chapter five.

The still-developmental nature of most retail RFID systems does make it quite difficult to quantify any costs or benefits, and verify that they truly exist. Fortunately, at least three studies have recently been published, offering a first glimpse at the cost of implementing an RFID system and how it might enable cost reductions at the retail level. The first examines a limited RFID trial conducted by Sainsbury's, currently the third largest supermarket chain in the United Kingdom, which was designed to see whether RFID could improve efficiency for short shelf like products, such as ready meals and pre-packaged meat. (Käarkkäinen 2003) The second study, published in November 2005, investigates Wal-Mart's initial use of RFID, to see if that deployment impacted out of stock inventory levels. (Hardgrave, Waller et al. 2005) The third recently published investigation is a quantitative analysis of the printing industry in Taiwan that identified item-level tagging as the ideal approach. From some initial empirical data, the authors extrapolate a series of tables describing the costs and benefits of RFID deployment as a function of a number of parameters, such as enterprise size. (Hou and Huang 2006) The cost-benefit results reported by each are discussed in more

detail in Chapter three of this dissertation, but in assessing their contributions, it is relevant to note that all three of these use traditional methods that only assess firm costs and benefits. Käarkkäinen simply aggregates each operational cost and benefit that he observed in one application, while Hou and Huang essentially do the same, although they present a more generalized model. The study by Hargrave, et al., appears to use more sophisticated statistical methods to determine the impact of Wal-Mart's RFID system on cross-store inventory levels, but the exact methods are not well reported.[6] A few other recent publications (Jones, Clarke-Hill et al. 2005; Prater, Frazier et al. 2005) also usefully highlight specific areas where retailers might benefit from RFID, including better inventory management and control, reduced shrinkage, reduced labor and improved customer service, but do little to quantify these benefits other than pointing out the need for additional research. Further, they are also exclusively focused on understanding the enterprise perspective. Thus, while this literature can be useful as a baseline for understanding the firm side of an analysis, it represents only a small piece of the overall social impact liable to be introduced by RFID.

2.2. Research approach

The literature shows that there is an abundance of research, in multiple disciplines, that addresses aspects of the overall costs and benefits of deploying RFID. Behavioral research shows that individuals are quite heterogeneous with regard to privacy beliefs and actions based on those beliefs. Economic research shows similar heterogeneity, along with the idea that privacy can be treated as an economic good, when modeling individual behavior. The limited literature that is specific to RFID offers some guidance as to the likely costs and

[6] It should be noted that, thus far, these results have not been published in any peer-reviewed form. Instead they are presented as a working report of the Information Technology Research Institute, at the University of Arkansas.

benefits for a firm to implement an item-level RFID system. It also offers a number of ideas about possible policy options, which serve to highlight the interests of the key types of stakeholders.

The logical next step is to integrate these components into an analysis that reflects the key aspects of all three bodies of work, and takes into account the multi-stakeholder nature of the problem. This research provides a contribution to the existing literature by proposing both conceptual and economic frameworks that are multi-disciplinary and comprehensive across stakeholder groups, and by applying those frameworks to assess the impact of different policy options. The integrated conceptual framework, proposed in chapter three, develops a structure for assessing the cost and benefit issues seen by each key stakeholder group. The economic model constructed in chapter five uses microeconomic principles, guided by the research findings reviewed here, to enable quantitative assessment of the impact of various RFID policies.

3. Cost-Benefit Framework

The surge of RFID development in recent years has spurred an active policy debate. In a speech at given at Georgetown University Law School in 2004, Senator Patrick Leahy of Vermont, the ranking Democratic member of the Senate Judiciary Committee, described the issues arising from RFID technology as "the defining privacy challenge of the information age." He suggested the need to "encourage public dialogue in both the commercial and public sectors before the RFID genie is let fully out of its bottle." Numerous legislative bodies, including at least sixteen state legislatures and the US House of Representatives and US Senate, are debating a wide range of policies that might limit the uses of RFID technology in settings including the retail market. Simultaneously, consumer advocacy groups, in the US and elsewhere, are protesting retailer plans for RFID and have already organized boycotts against Wal-Mart in the US and Tesco in the UK. Unfortunately, much of the policy debate has been burdened with overheated advocacy, or purely technical analyses of RFID issues, with policy as an afterthought. A clear and comprehensive analysis of how various policy approaches take into account the impact of RFID technology on national security, economic efficiency, and individual privacy and civil liberties does not yet exist. As a first step toward that objective, this chapter defines the key stakeholders in the debate, and then elucidates the primary costs and benefits that motivate each.

3.1. Stakeholders

There are four types of primary actors who have interests at stake in the debate over RFID policies. These are individuals/consumers, private, for-profit firms[7], government

[7] Here the for-private firms are the key stakeholders among all private sector organizations, but non-profit organizations are conceivable, too.

agencies, and society as a whole. The relative interest of each varies according to the particular application area. This discussion focuses upon the retail sector, where the key applications have already been described. It defines each of the stakeholders more precisely, provides examples where appropriate, and elaborates on the issues each actor is likely to be concerned about.

Individual stakeholders are consumers and users of products that contain RFID tags, and specifically those who purchase retail products that are tagged with RFID chips. Also included are representatives of groups of individuals, including member organizations, advocacy groups, and unions. Stakeholder firms are considered to be all business operations that have an interest in the development and supply of RFID technology, the deployment of the technology, or the use of information collected by the technology, and associations of similar companies.

Technology developers as stakeholders include firms that produce RFID tags and related products, and those known as system integrators or value added retailers. The later firms provide technology often known as middleware, which enables the integration of the RFID technology with the remainder of a firm's resource management and planning systems. The anticipated growth of RFID technology has resulted in a proliferation of firms in these areas. The 2006 Buyer's guide for an industry trade magazine known as ID World lists more than one hundred fifty firms that fall into one of these categories. Examples of technology developers include many major semiconductor manufacturers, such as Hitachi, Texas Instruments, and Philips, as well as smaller firms such as Alien Technology and the aforementioned Zebra Technologies. Examples of system integrators include IBM, Accenture and many other smaller consulting organizations.

Retail sector firms that use RFID technology include companies that are focused on controlling production, supply chain, inventory and retail sale of products that are tagged with RFID. The most prominent examples are Wal-Mart and other big-box retail firms such as Target, Best Buy, Albertson's, Metro AG, and Tesco, and their suppliers such as Proctor and Gamble and Pfizer. In addition, there are indirect users of the technology, who are not directly involved in any transaction, but are interested in the information collected, such as financial services firms or credit agencies, advertising or marketing firms, and firms that sell data services including warehousing, mining and analysis. (Campbell 2005)

Government agencies and other regulatory bodies as stakeholders have a broad range of interests in RFID. They include government organizations that use or control their own RFID systems for internal purposes, those that want to make use of data collected elsewhere, and those that have regulatory responsibility to enforce current policies, to develop new policies, or to interact with other organizations such as standard-making bodies or international governance organizations. Government organizations that control their own RFID systems and policies are unlikely to be primary actors, but many others are, in fact, potential consumers of RFID-enabled products, who might have interest in how to manage their own logistics. If all of these various government actors were to consolidate their requirements, they would have substantial market power as consumers. In this, they are similar to individual consumers as stakeholders, but are identified separately here to illustrate the complexity of the government's role. There are many possible scenarios where government agents might be interested in capturing RFID data, or re-using it after it has been generated by another system. Examples of this might include law enforcement and first responders. Finally, RFID is a radio technology, and is such it could be subject to regulation, much as other wireless technologies, by the Federal Communications Commission. The

Federal Trade Commission has already held a series of hearings about applications of RFID and implications for consumers (Staff of the Federal Trade Commission 2005); other government bodies within the Department of Commerce and elsewhere will have to deal with export issues arising from the Privacy Directorate of the European Commission, and other international matters. (Campbell 2005)

In addition to these specific stakeholders, the issue of adoption of RFID can affect society as a whole, in line with the previous argument that personal information has value different from the costs and benefits to any particular individual or firm. Partially, this can be accounted for by an economic analysis that looks at changes in overall social welfare. But, changes in social welfare, arising solely from the specific economic market analyzed, ignore the possibility that the adoption of RFID could result in externalities in other markets, and therefore provide only a partial understanding of the impact of RFID, or similar technologies.

3.2. Stakeholder costs and benefits

Each stakeholder in this debate is presented with a unique set of potential costs and benefits, arising specifically from the use of RFID technology. In addition, each stakeholder faces costs and benefits that arise from data collection that is enabled by RFID technology, but independent of the technology, once the information has been collected. It is important to understand both aspects, and realize that policies may either address the specific technology, or the more general data collection problem. For example, the RFID system itself can provide location information about an individual, enabling surveillance or triggering a specific sales action, but the data collected by an RFID system can also be used to generate a profile that could then be sold to a data broker or credit agency which does not

need location specific information to benefit. Much of the existing public debate, including policy analyses and proposed legislation, has neglected one aspect of this problem, or the other.

Table 3-1: Summary of RFID Costs and Benefits in the Retail Market

Stakeholders			
Individuals/ Consumers	**Firms/Business**	**Government/Regulators**	**Society**
Cost/benefit of technology: change in consumer prices	Fixed Cost of deploying RFID technology	Method & cost of policy or standards development/ implementation/ regulation	Change in overall social welfare
Cost/benefit of information effect on privacy	Variable (operating) costs of data collection	Cost of protecting civil liberties (litigation)	Information commons
Benefit of information: Convenience, service, customization	Cost of Information Control: Protection; Liability	Cost of no regulation (market failures, etc.)	
	Benefit of technology: cost reduction through enhanced logistics	Benefit of technology: logistic improvements to government consumers (military, libraries, etc.)	
	Benefit of information: Market power allows price discrimination, customized products, selling data, etc.	Benefit of information: data access for law enforcement, regulation, emergency response, etc.	

This discussion of costs and benefits associated with RFID focuses on a retail market situation where a retailer is capable of tagging individual items and collecting and storing the data associated with each transaction for each tagged item. Currently, the majority of retail tagging occurs at an elevated level of inventory control, such as shipping pallets or cases, but some high-value products are already tagged at the item level. In addition, the majority of the debate is occurring over item level tagging and its likely impact on individuals and firms.

Many of the same costs and benefits pertain to other scenarios, if only in a more moderated form. A summary of costs and benefits for this item level retail-tagging scenario is presented in Table 3-1. The components of the table are explained further in subsequent sections of this chapter, along with a discussion of how to incorporate each unique stakeholder issue into a larger, coherent analysis.

3.2.1. Individuals/Consumers

Table 3-2: Summary of individual costs and benefits

Cost/benefit of technology: change in consumer prices
Cost/benefit of information effect on privacy
Benefit of information: Convenience, service, customization

A primary benefit to individuals of the adoption of RFID technology at the retail level will be reduced consumer prices. This follows directly from the expectation that RFID will improve supply chain efficiency for retail firms, resulting in lower costs. As a result, basic economic theory suggests that a market should expect lower price equilibrium, if all other things are held equal. (Nicholson 2002)

Individuals might also benefit in other fairly basic ways, such as consumer convenience, peace of mind, and improved service. (Eckfeldt 2005) Peace of mind is primarily a factor in the enhanced security that RFID can offer to applications such as access control or car anti-theft protection. However, it is also a factor in other areas such as improved security of prescription drugs, where an RFID tag can ensure that the received product is authentic and not yet expired, or quality of products where freshness and other handling factors are criteria. Consumers might be much more willing to buy meat, fish or milk in a grocery store if those

products had customer accessible RFID tags that established their lineage. (e.g., did the organic products truly come from an organic farm?)

The EZ-Pass toll-collection system, which links an active RFID tag attached to the interior of a car to a user's account, and the ExxonMobil Speedpass™ point-of-sale system, which links a passive RFID tag to a particular credit card, are examples, in applications similar to, albeit more limited than, the consumer retail environment. In both cases, the RFID system allows a user to complete a sales transaction with no additional human intervention. Even though EZ-Pass has been used to track individuals under criminal investigation, many customers have clearly perceived the benefits, in time savings and not needing to carry cash, to outweigh the costs. (Eckfeldt 2005)

An extension of the convenience benefit is enhanced customer service. In late 2001, Prada opened a flagship store in New York, designed by the well-known architect Rem Koolhaas to offer a new vision of the retail experience, substantially enhanced by item-level RFID tags. Prada issued customers a "convenience card" containing an RFID chip. The tag contained an ID linked to the customer's entire Prada shopping history, which was accessible to any sales associate. In addition, RFID readers were dispersed around the store, allowing customers or sales associates to scan an item, and call up additional information such as a designer collection portfolio, color choices, or details about the materials and construction of the product. As a final feature, the dressing rooms were equipped with "smart closets" that were linked to a touch screen LCD display. The closet would scan a clothing item that was placed in it, and offer the user accessory options or other details. (RFID Journal 2003) Unfortunately for Prada, they ultimately closed the store as a result of expenses, ending consumer concerns over the collection of sensitive information, such as the size of ladies dresses.

Some futurists have predicted additional long-term benefits from RFID. They envision homes with "smart" appliances that can read and react to RFID tags. For example, a refrigerator could report on expired food, a smart washing machine could select how to treat clothes (as already mentioned), and a smart drug cabinet could make sure that a patient is taking the correct medications. These are real at home possibilities, today, for Bill Gates, but are likely many years from being readily available to average consumers. Unfortunately, without any clear understanding of how individuals will respond to these types of benefits, it is difficult to incorporate them into any straightforward analysis. It is more appropriate to handle them in a scenario analysis, discussing how different strategies (including policies as well as the behavior of firms and individuals in reaction to those policies) will impact the likelihood of these benefits.

All of these potential benefits for individuals are balanced by costs, such as the possibility of being exposed to surveillance, profiling, or actions based on an RFID signature, as has already been discussed in Chapter one. Other authors have offered similar models of the costs to individuals, but there are no empirical or survey data that directly address RFID. Thus, it is difficult to quantify these costs or even specify a typical range of variation. A small number of recent empirical studies were described in chapter two. These studies show that individuals do behave rationally (in the economic sense, as utility maximizers) when facing privacy compromising situations, implying that demand curves responding to variations in the exposure of personal information are feasible, and that individual taste for privacy varies widely. These results, coupled with the many surveys (Harris Interactive 1999; Sheehan 2002; Berendt, Gunther et al. 2005) showing that individual preferences for privacy are a continuum ranging from the unconcerned to the "fundamentalists" (a finding supported by the variation in valuation reported in the Cambridge experiment), argue that individual costs

arising from lost control over personal information can be represented by a series of preference or demand curves that are dynamic in response to potential uses of collected RFID data. An added complication is that the costs of the potential uses of data vary in response to the cost of individual and firm compliance with any policies or regulations that are imposed. This representation, incorporating both the rational economic and individual variation aspects of privacy costs, is further developed in Chapter five.

3.2.2. Firms

Table 3-3: Summary of firm costs and benefits

Fixed Cost of deploying RFID technology
Variable (operating) costs of data collection
Cost of Information Control: Protection; Liability
Benefit of technology: cost reduction through enhanced logistics
Benefit of information: Market power allows price discrimination, customized products, selling data, etc.

The first order costs and benefits of RFID technology for large retail firms and their suppliers are based on the view that current supply chains are dated and inadequate for modern requirements. Information is static and often not up-to-date, systems are poor at dealing with dynamic demand, and error, inaccuracy and outright fraud abound. (Wyld 2005) Analysis shows the scope of many of the problems arising from inadequacies in the supply chain is substantial. Shrinkage (theft, expiry, loss or damage before the end customer) of consumer-packaged goods is estimated at up to (US) $60B annually and counterfeiting is estimated to be as high as $100B annually. (Noonan, Cheyne et al. 2004) Inefficiencies in the system lead to other substantial problems, as well. Retailer out of stocks are estimated to cost as much as 6% of sales, and over 50% of delivery trucks are empty or are returning unwanted or expired product. (Noonan, Cheyne et al. 2004)

Retail firms have identified a whole host of prospective opportunities to address these challenges using RFID. The majority relate to improved logistical efficiency that RFID can enable across the supply chain, from raw materials supply all the way up to the retail Point-Of-Sale (POS), and customer satisfaction even beyond the POS. Some of these benefits are specific to particular members of the supply chain, while others occur between elements of the chain, or across its entire breadth. As the process is optimized, the entire supply chain is likely to see benefits in areas including: counterfeit/fraud reduction through rapid identification and tracking of frauds and leaks, improved efficiency of shipment and delivery by way of real-time inventory control and demand management, labor cost reduction by reducing the amount of manual intervention required during the distribution process, shrinkage reduction by using RFID technology to quickly detect and respond to missing inventory, and improved retail stocking by better management of store-shelf inventory. (Wyld 2005) Retailers can also achieve some additional improvements from RFID. These include improved POS checkout through the elimination of the need to handle each product requiring a bar code scan, better sales support by automation of returned goods, and improved management of floor inventory (e.g., clothes that are taken to a fitting room). (Kurt Salmon Associates 2005) Finally, RFID is an enabling technology in the growing movement, by retailers, towards individually customized products.

Balancing these benefits are the large costs associated with developing and deploying appropriate RFID technology, managing the data that will be produced by a system that includes item-level tagging, integrating the RFID technology and data with other technologies and data, and complying with any government policy mandates. The costs can be partitioned into the fixed costs of installing an RFID system, and variable costs associated with collecting and managing the "avalanche of data" that an item-level tagging system will

product. The fixed startup costs include hardware such as readers, antennae, and appropriate networking capability, software (or middleware) to manage and integrate the RFID system with other corporate resource tools, possibly additional and customized material handling equipment to allow for automation of RFID processes, and the cost of installation, integration, and training. Variable costs include labor associated with the RFID system, the cost of tags, and, most substantially, the cost of managing data. As an example, it is estimated that Wal-Mart RFID systems deployed by the end of 2005 will generate more than 7 terabytes of data per day, and cause substantial challenges in sorting these data. It is expected that this volume will force a trend toward "edge computing," where most data are processed locally, and only select information is transmitted centrally, based on sophisticated event processing and decision agents. (Wyld 2005)

The still developmental nature of most retail RFID systems makes it quite difficult to quantify any of these costs or benefits, and verify that they truly exist. Fortunately, the three studies discussed briefly in chapter two provide an initial basis for understanding the costs associated with deploying an RFID system and how it might enable cost reductions at the retail level. As described previously, Käarkkäinen examined a Sainsbury's RFID trial that "started with one ready-meal supplier, a single depot, and a retail store. Later the trial was scaled up to encompass all chilled products going to the retails store." He further characterizes the trial process:

> The trial was based on applying RFID tags to recyclable plastic crates…
>
> Three pieces of information were needed to fulfill the goals of the trial, i.e. faster and better controlled stock rotation, especially in retail stores, and were programmed to the tag:
>
> (1) the description and quantity of products in the crate;
> (2) the use-by date of these products; and
> (3) the crate's own ID number

> …. [A]ll tags on crates with chilled goods produced at the one supplier were programmed with the description of the product and the use-by date of the products. The programming was completed with a reader at the end of the production line. Next, the goods were read at the depot's goods receipt with a portal reader. This reading method enables operational efficiency as all crates in a pallet or a roll cage can be read by a single movement through the reader. When delivering to the store the goods were again read with a portal reader that was located between the chilled storage and store areas. The goods were always moved through the reader, whether moving them in or out of stock.
>
> …. [A]ll products arriving to the test store were equipped with RFID tags, allowing easy access to product description, product quantity and use-by date information. This scaled-up test was run for three months to reveal the effects that the use of RFID may have on retail store operations. This was considered essential for accurate estimations of potential benefits. (Käarkkäinen 2003)

Sainsbury's calculated store level benefits using changes in labor standards, which are "work study timings for all key activities in store processes." From this, they determined that there were real savings in stock loss, stock/code check, replenishment productivity, store receiving, and depot inventory control. The total savings was estimated at £8.5 million/year, with nearly fifty percent coming from stock loss savings, and almost thirty percent from reductions in stock/code check costs due to increased inventory accuracy. This is balanced against an investment that was between £18 and £24 million, resulting in a payback period of between two and three years. Käarkkäinen also notes that suppliers did not participate in the program, and all work was done through Sainsbury's, so further savings should be possible, although Sainsbury's was not able to convince suppliers to implement RFID systems, due to uncertainty about the maturity of the technology. (2003)

More recently, The Wal-Mart study looked at a much broader trial, but only one area of cost savings, out of stock reduction. The study was commissioned by Wal-Mart, and consisted of a daily investigation, over a twenty-nine week period in 2005, of out of stock inventory at 24 Wal-Mart stores, 12 RFID-enabled and 12 control stores. The 12 RFID stores were selected out of 104 RFID-enabled stores and the control stores were then matched based on location, size, and annual sales. Each group included 6 supercenters, 3

neighborhood markets, and 3 traditional stores, located in Texas and southern Oklahoma. During the experiment, the data collectors monitored 4554 products containing RFID tags, from across almost all departments and in almost all sections of each store for out of stocks, defined as any empty shelf space, while attempting to control for time of day, route through the store and other possible measurement effects. With these data they performed two difference-of-differences calculations, looking at the change in out-of-stocks over time. One assessment was between tagged and non-tagged products within RFID-enabled stores, and the other was between the RFID-enabled stores and the control stores. Although the results are only preliminary, they conclude that the use of RFID enabled a 16% reduction in out of stock inventory. (Hardgrave, Waller et al. 2005) They did not report on more interesting results such as net benefits or payback period.

The third study, by Hou and Huang, provides a quantitative analysis of the costs and benefits of RFID in different logistics activities within the Taiwanese printing industry. (2006) The researchers surveyed the industry to determine six different supply chain scenarios, involving different sizes of publishers, distribution centers, and retail outlets. They estimate total costs and benefits for each of these scenarios, as well as other possible combinations, and present them in a series of lookup tables. Looking at the standard supply chain models and estimating the cost of tags, readers, middleware, and network infrastructure, for publishers with a range of revenues, Hou and Huang estimate costs. They identify the cost of tags to be the dominant factor, by far, especially for large publishers. (Oddly, they seem to expect little economy of scale in tag prices.) The savings are estimated by comparing the measured amount of labor involved in each current task, such as unloading a delivery truck, picking stock, or point-of-sale payment, with the measured amount of labor required when using an RFID system. Unfortunately, they fail to convert the labor savings

back to dollars, so this analysis is most useful in framing the system implementation costs for suppliers to the retail market, where tag costs will dominate.

In addition to the logistics impact of RFID, firms face other potential costs and benefits. The benefits arise from using information about individuals to gain additional market power, enabling activities such as targeted marketing, or price discrimination, which can be directly incorporated into an economic cost-benefit model. A number of existing analyses of price discrimination, employing a variety of different models and analytical techniques, were described in chapter two. Briefly, depending on the model assumptions, it is possible to describe conditions under which firms will benefit (or not) by employing price discrimination. Similarly, the overall welfare implications are also a function of analysis particulars. The model constructed in chapter five is able to replicate many of these sensitivities in outcomes, as a function of parametric choices.

Beyond the basic costs associated with installing an RFID system and collecting and analyzing data, firms will face costs to control those data, arising from the fact that a basic RFID tag can be read by many parties. This open nature of RFID, coupled with access to the EPC database allows a third party to scan and identify tagged objects, and gives rise to at least two direct threats. The first is that a firm might be subject to corporate espionage, whereby an agent of a competitor could monitor the first firm's inventory and supply chain data. The second is that customer preference information could be obtained and used to target certain desirable customers with particular marketing. This second threat also leads to possible liability issues (i.e., a customer holding a firm liable for revealing private information to another firm.) A third and final threat arising with RFID systems is more technical in nature. As logistics infrastructures become more dependent on easily jammed radio signals, the possibility exists of a malicious denial-of-service type attack. (Garfinkel, Juels et al. 2005)

The cost of any of these threats is unclear, as none has yet publicly come to pass. It is possible to understand each as added cost included in the design and installation of an RFID system. For example, tags can require a password, or data can be encrypted, to prevent the first two threats, at the cost of more expensive tags and more sophisticated infrastructure. Key points in the supply chain can be physically shielded to deal with the third threat, at the expense of added fixed cost of system installation. The cost of each of these threats can then be considered as the cost of prevention, as a function of policies, and be incorporated into economic analysis.

3.2.3. Government Interests

Table 3-4: Summary of Government costs and benefits

Method & cost of policy or standards development/ implementation/ regulation
Cost of protecting civil liberties
Cost of no regulation (market failures, etc.)
Benefit of technology: logistic improvements to government consumers (military, libraries, etc.)
Benefit of information: data access for law enforcement, regulation, emergency response, etc.

In the retail RFID sector, the government faces one broad direct cost, which will be imposed by whatever policy choices are ultimately made. This is the cost of developing, implementing and enforcing relevant policies and standards. Closely associated with this will be the cost of compliance on the part of firms and individuals. The cost of developing policies and standards also includes the need to integrate US domestic requirements with international preferences, policies and standards.

There are many indirect costs and benefits facing the government, which are largely a product of the rate and degree with which item-level RFID tagging will proliferate in the

retail industry. As shown in Table 3-1, there are other costs related to protecting civil liberties, and the cost of market failures that might occur in the absence of policies or in the presence of poor ones. These costs are potentially widespread and not easy to quantify, but generally speaking are related to the nebulous privacy right. In a series of possible precedent setting cases, the US Supreme Court has upheld an individual's right to anonymity using both first and fourth amendment grounds. (Samuelson 2005) Beyond the Constitution, there are questions about the relevance of the Electronic Communications Privacy Act and other similar laws that Congress has passed to provide individuals with a sufficient degree of privacy protection. (Campbell 2005) A more detailed discussion of currently relevant law, as well as proposed RFID specific legislation, is provided in Chapter four.

Government parties might also expect to accrue benefits related to the proliferation of RFID. Various government agencies are potential customers of products containing item-level tagging. There is the potential for these agencies to benefit from lower product prices if RFID is widely used. Further, many of those agencies, especially the Department of Defense (DoD), have their own substantial logistics operations. The Department of Defense has already embarked upon an RFID mandate, similar to Wal-Mart's, and they have chosen to allow suppliers to use the nascent standard EPC code for product identification purposes. (RFID Journal 2003) Widespread development and use of standard forms of RFID, such as EPC tags, stands to provide a direct benefit to the DoD in lower costs, higher quality, improved efficiency and generally easier deployment according to their own mandate. Other government agencies, including the Department of Energy, Department of Homeland Security, Department of Veterans Affairs, and the General Services Administration (GAO 2005) employing RFID for logistics might experience similar benefits. Although many of these benefits are essentially the same as those associated with the individual/ consumer

stakeholder, they are enumerated separately here to demonstrate the multi-faceted aspects of government involvement.

Government agents who are interested in collecting additional personal information for law enforcement or regulatory purposes stand to benefit more from wide-spread use of item-level RFID tagging. Possible examples include product authenticity investigations by the Food and Drug Administration or the Federal Trade Commission, and tax and fee levying and collection at various controlled locations (e.g. ports-of-entry.) (Campbell 2005)

3.2.4. Society, Economic Externalities and Tradeoffs

Understanding societal costs and benefits requires addressing both changes in overall social welfare arising from a new economic equilibrium, and the impact of the many indirect costs and benefits that can be interpreted as externalities. Changes in social welfare, as meant in the economic sense, can be determined directly out of an economic analysis; a new policy regime results in a new economic equilibrium with a different partitioning of overall welfare to individuals and firms. However, not all of the costs and benefits described in this chapter can be reduced to a single cost-benefit analysis, reflecting both the implicit tradeoffs in costs and benefits that are directly important to one stakeholder but represent an externality to another and the presence of additional markets where RFID might bring substantial costs or benefits. For example, imagine two policies where, all else being held equal, the first policy allows relatively cheaper data collection and use by firms than the second policy. A likely outcome of this, considering purely the economic cost-benefit tradeoff, would be that firm use of RFID and personal data would be more widespread, the equilibrium price would fall, and firms would have lower costs and higher profits, depending on the degree of price discrimination. However, if the same policy also allowed these data to be easily shared with

surveillance interests in the government, and if individuals perceived this as excessive government intrusion ("big brother" in action), a resulting consumer backlash might drive consumers away from firms collecting personal data altogether. Many other inter-related tradeoffs can be similarly imagined. The inter-related nature of these costs and benefits, and the fact that the marginal costs and benefits associated with any particular policy are certain to be different for each stakeholder, holds much in common with traditional definitions of a commons.

An information commons implies the need for policies that allow data to be generated and used, while ensuring that stakeholders are confident that the data are being used properly, so they do not need to engage in excessive competitive behavior. For example, if individuals know that their data are safe from excessive monitoring by other individuals, firms, or the government, they can make uninhibited use of whatever quantity of information they feel safe with. Firms can behave similarly, knowing that they are safe from industrial espionage, and so can the government during surveillance activities, knowing that they are collecting reliable information. Conversely, if stakeholders are concerned with overuse, they will take competitive steps, such as corruption, to protect data. The former case, where the commons is well managed, offers positive externalities, such as enabling new applications that rely upon RFID, e.g., smart home appliances or smart medicine cabinets. These will only develop when costs are low enough to result in a sufficiently large market opportunity. In the latter case, a tragedy of the commons might result in failure for such applications that require reduced system or tag costs before they can become effective.

If different policies lead to different levels of information collection (an assumption tested with the model of chapter five), then policies are ways of addressing the differing marginal costs/benefits to each stakeholder, and have implications for enabling the

commons. Policies will be most effective when they are adaptable to these differing marginal costs, whereas policies that impose a fixed cost to any or all stakeholders are unlikely to be effective, unless the fixed cost to each stakeholder fortuitously matches that stakeholder's share of the overall social cost.

The potential scenarios demonstrate that the outcome of a cost-benefit or economic analysis is necessary but not sufficient to understanding the actual impact of different policy choices on the overall societal costs and benefits. Returning to the summary of costs and benefits shown in Table 3-1, eight out of the fourteen issues can be directly incorporated into a cost-benefit or economic model. These are the cost or benefit to individuals of changing consumer prices, the cost or benefit to individuals of lost personal information (privacy), the fixed cost for a firm to deploy an RFID system, the firm's variable cost of operating an RFID system and collecting data, a firm's logistics benefits, a firm's market power (price discrimination) benefits, the government's cost to implement any regulatory actions, and the change in overall social welfare arising from the new economic equilibrium. The direct economic impact of the other stakeholder issues requires steps such as the exemplary hypothetical scenario analysis just presented. The scenarios can be assessed through their economic impact, and through qualitative assessments according to the framework presented here.

4. Framework applied to RFID policies

No current US law deals explicitly with RFID systems, but a number of existing laws and US judicial system rulings are generally relevant to the collection and use of private personal information, and could conceivably be adapted to RFID technology. Additionally, there are several international agreements and guidelines, proposed by organizations that the US participates in, that are more explicit with regard to handling personal information. Finally, a number of other countries have already taken, or are considering, specific regulatory steps to address RFID systems. This chapter provides a summary overview of these regulations, followed by a review of existing RFID specific policy proposals currently under consideration by a number of US states, and then an analysis of several types of RFID specific regulatory proposals, according to the cost-benefit matrix described previously in Chapter three.

4.1. Current US laws

There are a number of US federal and state statutory provisions, and numerous court rulings based either on those laws or attempts to reconcile the Fourth Amendment's protection against unreasonable searches and seizures with uses of new technology that are indirectly relevant to the policy issues surrounding RFID. None of these laws or court rulings make explicit reference to RFID technologies, but they do establish current rules regarding law enforcement's ability to conduct surveillance, wiretapping or tracking of individuals, and law enforcement or a private individual's ability to monitor records in computer databases. Thus, it is possible that these current laws could be extended to encompass RFID applications and concerns.

The most significant current laws governing federal surveillance behaviors are the Electronic Communications Privacy Act (ECPA) of 1986, the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994, and USA PATRIOT Act of 2001. The ECPA, sometimes used interchangeably with "federal wiretap law," is the successor to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. That act, usually known simply as Title III, was the original law establishing government wiretap procedures and was enacted by Congress in response to the 1967 Supreme Court ruling in *Katz v. United States*, which establish the "reasonable expectation of privacy" criteria as the basis for requiring a probable cause warrant. Katz revealed a Supreme Court which realized that information was becoming valuable as a commodity in its own right, that the Fourth Amendment must protect private speech and conversations and that "given the new technologies available in government investigations, a consideration of *how* the government agents (or their devices) carried out surveillance was no longer a meaningful factor." (Simmons 2002) Unfortunately, Title III had no provisions for the possibility of other (non-traditional wiretap) technologies for data or visual surveillance. Therefore, Title III was a step back from *Katz*, where the court appears to have discarded particular consideration of the type of technology involved in the surveillance. (Smith 2000)

These weaknesses in Title III ultimately led to the ECPA, which both provided updated wiretapping regulations in accordance with then current technology and sought to avoid restrictions on emerging communications technology. The ECPA contains three titles, respectively governing the interception of communications, stored communications, and the use of pen registers and trap and trace devices.[8] In brief, the act is the current source of the

[8] *18 U.S.C.* defines a pen register as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic

well-known provisions requiring a court order prior to use of a wiretap, with certain exceptions. The Act also established that while a wiretap warrant requires probable cause, pen registers and trap and trace devices must meet only a lower standard of relevance to an investigation. (Solove and Rotenberg 2003) The ECPA explicitly exempts "any communication from a tracking device" which is "[an] electronic or mechanical device which permits the tracking of the movement of a person or object." (Kobolev 2005)

Subsequently, and also in response to changing technology, Congress passed CALEA to augment policy authority to use newer still surveillance tools. CALEA (also known as the "Digital Telephony Act") requires "all telecommunications providers to be able to isolate and intercept electronic communications and be able to deliver them to law enforcement personnel." (Solove and Rotenberg 2003) However, CALEA also establishes a requirement to "protect the privacy and security of communications not authorized to be intercepted." (Solove and Rotenberg 2003) In addition, the USA PATRIOT Act and the Homeland Security Act of 2002 yet again expanded the government's authority. (Kobolev 2005) The USA PATRIOT Act altered the definition of both pen registers and trap-and-trace devices to include "Internet addresses, e-mail addressing information… and the routing information of a wide spectrum of communications." (Solove and Rotenberg 2003)

The actual applicability of this code to current means of tracking and surveillance is now under debate within the legal system. In *United States v. Knotts* (1983), a case where law

---

communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business."

18 U.S.C. defines a "trap and trace" as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."

enforcement officers tracked a suspect's vehicle by means of a device placed without warrant, the US Supreme Court held that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." Yet, in contemporary cases where the government has tracked individuals through their cell phones, five out of six recent appellate court rulings[9] have generally rejected the government claim that a broad interpretation of CALEA and the USA PATRIOT Act, in conjunction with ECPA and the generally lower standard required to authorize a trap and trace, establishes the legitimacy of tracking individuals via their cell phones prior to obtaining a probable cause warrant. One appellate court has upheld the Department of Justice position, and the broad uncertainty around the applicability of current laws led a number of the appellate courts to explicitly ask the Department of Justice to look to the Supreme Court for guidance, although this has not yet happened.

In short, US law is currently quite muddled with regard to the use of technology to track individuals without their consent or probable cause. This state of confusion is also perceptible in at least one recent and significant US Supreme Court ruling, *Kyllo v. United States*, where the Supreme Court held that the use of a thermal scanner to inspect the interior of a suspect's house required probable causes. Rather than establishing fourth amendment based general limits to technological surveillance, though, the court muddled matters

[9] Application for a Pen Register and Trap and Trace Device and Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F.Supp.2d 294 (E.D.N.Y. 2005); Application for Pen Register and Trap/Trace Device with Cell Site Location, 396 F.Supp.2d 747 (S.D.Texas 2005); In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and Production of Real Time Cell Site Information, 2005 WL 3160860 (D. Md. Nov. 29, 2005); In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 2005 WL 3471754 (S.D.N.Y. Dec. 20, 2005); In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, 2006 WL 41229 (D.D.C. Jan. 6, 2006); In Matter of Application of U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Information, 2006 WL 243017 (E.D.Wis. Jan 17, 2006).

significantly by holding that if "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'" (Slobogin 2002) Unfortunately, *Kyllo* does not define "general public use," and so it is entirely possible and reasonably to interpret this case as protecting Kyllo's rights in the short term, but enabling greater intrusion into all of our private lives, as technologies become commonplace. If this is in fact the case, then it implies that as RFID tags and readers become commonplace, and perhaps they already are given existing applications, the government will be free to monitor individuals through their tags, and without having to establish probable cause.

Laws regulating the monitoring of stored information provide less guidance than surveillance laws. Regulations governing public sector records, although covered by the Privacy Act of 1974, and the Freedom of Information Act, enacted in 1966, provide less insight than the private sector, where there are a number of specific records protection laws such as the Bank Secrecy Act, the Fair Credit Reporting Act, the Video Privacy Protection Act, the Health Insurance Portability and Accountability Act, and the Telephone Consumer Protection Act, each addressing a particular market segment, and narrowly tailored to particular types of business. (Solove and Rotenberg 2003) Many of these laws assume a basis in an implementation of Fair Information Practices (further discussed below), yet they do not represent a coherent approach to privacy, especially in the private sector aggregation of individual records. Detailed analysis of each regulation, while beyond the scope of this research, is provided by Solove and Rotenberg (2003). For now, it is sufficient to note that numerous legal analysts have critiqued the ad hoc collection of statutes as insufficient to meet today's challenges. They have identified problems including the lack of "a comprehensive set of rights or principles to address the acquisition, storage, transmission, use and disclosure of

personal information within the business community" (Reidenberg 1992) and the absence of "successful standards, legal or otherwise, … for limiting the collection and utilization of personal data in cyberspace." (Schwartz 1999)

4.2. Fair Information Practices and International Laws and Agreements

Beyond domestic laws, the US government and US based firms also need to consider international regulations that bear upon both the ability of US companies to conduct business abroad and of international firms to conduct business in the US. For example, the US is a member in several international organizations that have established policies or guidelines governing personal information, often in the form of Fair Information Practices. Although the earliest comprehensive Fair Information Practices were formulated in a 1973 report by the Department of Health, Education and Welfare, one of the most important instantiations is the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Information," published and promulgated by the Organization of Economic Cooperation and Development (OECD) since 1980. (Eschet 2005) The core of the guideline document is the eight principles describing limits on how data should be collected and used, as reproduced in Appendix A.

Many OECD member-states have gone further and established legislation to enforce these guidelines. A primary example is the entire European Union, which first negotiated the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and then, in an attempt to harmonize the many different national standards that arose, passed the 1995 Directive 95/46/EC of the European Parliament and of the Council, "On the Protection of Individuals with Regard to the Processing of Personal Data

and on the Free Movement of Such Data."(1995) This directive provides a broad definition of personal data, and specifies that such data should not be processed at all, except when specific conditions of transparency, legitimacy of purpose and proportionality are met. The first condition, transparency, means that the subject has the right to be informed when personal data are being processed. The (data) controller must provide a name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. A set of specific circumstances permitting data processing is defined, and the subject has the right to access all relevant data, and demand corrections to incomplete or inaccurate data.

Second, legitimacy means that personal data can only be processed for specified, explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes. Third, proportionality requires that personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data shouldn't be kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States need to lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. The basic definition of personal data has been updated, in Directive 2002/58/EC to include the concept of location data, defined as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service." (2002)

Among many other principles established within the Directive, the most important deal with each member state's requirement to establish an independent supervisory authority, and the requirement that data can only be transferred to third countries (non-EU member-states)

that provide an adequate level of protection. To manage these criteria, the European Commission established the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party." All EU member-states have now adopted requisite national legislation, including the establishment of a national Privacy Commissioner, or the equivalent. The Working Party has also negotiated with U.S. representatives about the protection of personal data, and ultimately a series of Safe Harbor Principles was agreed upon. The key elements of these principles, which have been approved by both the US Department of Commerce and the European Union, are shown in Appendix A.

Both the Article 29 working party and individual states within the EU have started to think about how Directive 95/46 applies to various RFID applications. In January of 2005, the Article 29 Data Protection Working Party issued a "Working document on data protection issues related to RFID technology." (Data Protection Working Party 2005) The document identifies three scenarios where RFID technology could have data protection implications that would require abiding by Directive 95/46 guidelines: RFID used to collect information linked to personal data, RFID used to store personal data on individual tags, and RFID used to track individuals. In these cases, and possibly others, the Working Party sees Directive 95/46 as applicable, and provides general guidelines for data controllers to use as the basis for managing individual data processing. Those specifically identified are the purpose, data quality and conservation principles, the legitimacy of processing requirements, and information requirements that data controllers must provide to data subjects. In the case of the last, an example is defined, where

> [T]he retailer store will have to provide data subjects at least with clear notice about the following:

i. The presence of tags on products or their packaging and the presence of readers;

ii. The consequences of such presence in terms of information gathering; in particular, data controllers should be very clear in informing individuals that the presence of such devices enables the tags to broadcast information without individual engaging in any active action;

iii. The purposes for which the information is intended to be used, including (a) the type of data with which RFID information will be associated and (b) whether the information will be made available to third parties and,

iv. The identity of the controller.

In addition, depending on the specific use of RFID, the data controller will also have to inform individuals about:

v. How to discard, disable or remove tags from the products, thus preventing them from disclosing further information and

vi. How to exercise the right of access to information. (Data Protection Working Party 2005)

As of today, the activities of the working party appear to be the most complete RFID specific policy proposal. So far, out of the EU member-states, at least Italy and Portugal have adapted these recommendations into their own guidelines (see, for example, the Italian guidelines, "The Garante Per La Protezione Dei Dati Personali," available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107). Other countries are exploring how and when to adapt their own data protection regimes.

4.3. Current US RFID Policy Proposals

In 2005, legislators in at least 15 states introduced bills considering various aspects of RFID technology. Many of the legislative actions deal with retail uses of RFID, and appear to be motivated by concerns of privacy advocates. The proposals cover a wide range of requirements, although labeling is the most common, as discussed below. Unfortunately, few seem to have been written with a thought to more general principles of data protection or

surveillance, as described in the OECD and EU Fair Information Practices guidelines and directives that affect individual rights, or with a clear understanding of the technology and how its use might actually benefit firms, government agencies and society as a whole. A summary of this legislation is presented in Appendix A. Even a quick review shows that most proposed actions are quite simple. Some of the listed legislation is targeted at non-retail applications of RFID, but is included because it highlights the potential for similar regulations in the retail regime.

The majority of these legislative actions restrict RFID in some way. Only the Wyoming, Maryland, Utah, and Illinois legislatures have adopted neutral or "pro-RFID"[10] views. Virginia, Texas, Tennessee, South Dakota, Rhode Island, New Mexico, New Hampshire, Nevada, Missouri, Massachusetts and California all considered actions to restrict RFID in some way. Five out of eleven restrictive proposals mandate disclosure of RFID tags on consumer-purchased retail products. Several of these five have additional provisions such as deactivating at the point-of-sale (also known as a "kill-switch,") and other proposals make explicit reference to prohibiting or restricting access to personal information. None of the legislation that explicitly restricts RFID has yet been enacted, although many of these bills are scheduled to reappear for debate during 2006.

4.4. Cost-Benefit Analysis of RFID Policies

As shown, a number of policies have already been proposed, regulating the use of RFID in certain applications. Beyond those discussed above by the states and the European Commission, a variety of other parties have put forth suggestions for market-based, statutory

[10] By Pro-RFID, I mean legislation that supports broader use of the technology, as opposed to legislation that places restrictions upon its use.

or technical approaches. A lengthy but non-exhaustive list of these proposals is included in Table 4-1, below, where the policies are described in brief, and classified by the type of solution they contain and who has proposed them.

Table 4-1: Summary of Key RFID Policy Proposals

Policy	Advocate	Type	Overview
No regulation	Various	Market	Legislation, especially on the state level will result in confusion and added costs, and detract from the potential benefits. (Hutto and Atkinson 2004)
Industry self-regulation	EPCglobal, et al.	Market	Consumer notice via a label or identifier Consumer choice to discard, remove or disable tags from products they acquire Consumer education and access to information about EPC tags Companies publish information on data retention policies, and maintain all data in ways consistent with applicable laws (EPCglobal Public Policy Steering Committee 2005)
Encryption	Microsoft, RSA, et al.	Technical	Encryption of data between readers and tags to protect privacy. (Juels 2005)
Configurable antenna	IBM	Technical	Consumers can detach antenna, and reduce read range by up to 2 orders of magnitude. (O'Connor 2005b)
"Kill switch"	Auto-ID Center	Technical	Tags come with a disablement feature that can be activated at point-of-sale, based on consumer choice. (Auto-ID Center 2003)
Blocker tags	Juels, et al. (RSA Security)	Technical	An extra tag, carried by individuals, to prevent unauthorized scanning of a tag. (Juels, Rivest et al. 2003)
Data use restrictions	EPIC, et al.	Regulatory	RFID should not be used to track individuals w/o informed and written consent. RFID should not be used to reduce anonymity.
Individual opt-in	Various	Regulatory	Individuals must give explicit consent for RFID data collection.
Individual opt-out	Various	Regulatory	Individual are included in RFID data collection by default, but offered the option of removing themselves.
Banned on individual products	Various	Regulatory	No tagging of individual items allowed. Enforcement via government regulatory agencies.
Fair Information Practices: RFID Bill of Rights	Garfinkel, et al.	Regulatory	Users have the right to: 1) Be informed of the presence of a tag in a product, 2) Have embedded tags removed, deactivated or destroyed at purchase, 3) Comparable alternative services if they opt out of RFID, 4) Know what information is stored on their tags, and a way to amend incorrect information, 5) Know when, where, and why a tag is being read. (Garfinkel, Juels et al. 2005)

Policy	Advocate	Type	Overview
Best Practices	Center for Democracy & Technology	Self-regulatory	A company with a direct consumer relationship should provide consumers with clear, conspicuous and concise notice when linkable information is collected through an RFID system. Consumers should be notified when entering a commercial or public environment where RFID technology is in use. Wherever practicable, individual RFID readers should be identified as such. Companies should engage in annual internal assessments to confirm that the posted notices accurately reflect their information practices related to RFID systems. Consumers should be clearly notified, before the conclusion of a transaction, if possible, when there is an opportunity to exercise choice with respect to the use of the RFID technology or with respect to the use of linked information collected on the RFID tag or associated with the RFID number. Where cost effective, consumers should have efficient, reasonable access to personally identifiable information collected using RFID technology. Companies should exercise reasonable and appropriate efforts to secure RFID tags, readers and, whenever applicable, any corollary linked information from unauthorized reading, logging and tracking, including any network or database transmitting or containing that information and radio transmissions between readers and tags. In addition, companies should exercise reasonable and appropriate efforts to secure the linked information from unauthorized access, loss or tampering. (Center for Democracy & Technology Working Group on RFID 2006)
POS notification	Various	Regulatory	Consumers must be informed of specific information about the presence of tags. Details vary according to specific proposal.
EU Data Protection Policy	Working Party 29	Regulatory	The general guidelines of Directive 95/46/EC, particularly: -Consent from individuals -Clear notice about the presence of RFID tags on packaging, the presence of readers, the purpose of collecting the information, and the consequences -How to discard, disable, or remove tags -How to exercise the right to access information (Data Protection Working Party 2005)
7-Point Framework	Spiekermann	Technical/ Regulatory	1) Default killing or password protection of RFID tags 2) No sharing of local tracking data beyond logistics 3) Limited timestamp information 4) Only partial saving of a full serial number 5) Rigorous controls and transparency for Network access 6) Time-sensitive deletion of object data 7) Owner control over personal information (Spiekermann and Ziekow 2005)

The technical options presented are meant to be representative, not exhaustive. Other possible technologies have been proposed, including protective shielding, authentication,

encryption, and proxies, and research into these and other methods is ongoing. (Eschet 2005) An excellent review by Juels (2005) provides a summary description of at least ten different theoretically plausible and contemporary technical approaches.

The policy options defined as regulatory would require a level of government enforcement. In a case such as required POS notification, this could be accomplished by a straightforward audit or monitoring program, at representative retailers points-of-sale, but in policies where data usage is mandated in some way, regulatory oversight would need to be considerably more extensive.

The policies are not exclusive of each other. For example, Fair Information Practices policies such as the RFID Bill of Rights incorporate versions of the point-of-sale (POS) notification policy, data restriction policy, and the opt-out policy. Technical solutions such as the RFID blocker tag can exist in conjunction with regulatory or market solutions such as opt-in or industry self-regulation.

4.5. Detailed Policy Assessment

One or more advocates have seriously proposed many of these policies, but it is not necessary to analyze all of them in depth. A subset, representing the key policy options, is sufficient for further analysis, in order to evaluate the stakeholder framework, and provide a basis for subsequent economic analysis. Three options that are well representative of the different types of proposals are industry self-regulation, currently advocated by EPCglobal and other leading industry organizations; the RFID blocker tag, as a reasonably developed and supported example of a proposed technical solution; and the "RFID Bill of Rights," which is a widely promoted (in the United States) attempt to use Fair Information Practices,

such as those generally advocated by the OECD, as the basis for RFID policy-making.[11] Industry self-regulation is the current de facto policy choice in the United States.

Each of these policies is described in detail, below, along with likely costs and benefits, which are summarized in Table 4-2, Table 4-3, and Table 4-4. The costs and benefits are provided in a relative sense, with today's current situation as the baseline. The current situation is a low level of actual deployment of RFID technology at the retail level. If RFID were to proliferate, unimpeded by any policy changes, it would likely lead to lower costs for firms, an easier ability for firms to collect individual information, and lower equilibrium prices for consumers, but a loss of privacy. More specific numeric values are introduced during the detailed economic analysis. In all three tables, cells are shaded to provide a quick reference. An orange cell indicates a relatively worse situation: higher costs or reduced benefits. A light green cell highlights the opposite: reduced costs or increased benefits. A yellow cell shows that costs or benefits can be expected to be the same. Light blue indicates a cost or benefit that will be assessed by using outputs of the economic model in conjunction with scenario analyses described in chapters five and six.

4.5.1. Industry Self-Regulation

EPCglobal is a joint venture between GS1 (who describe themselves as "a leading global organization dedicated to the design and implementation of global standards and solutions to improve efficiency and visibility in supply and demand chains globally and across sectors") and GS1 US, an organization formerly known as the Uniform Code Council, which is now

[11] The Best Practices proposal is a very comprehensive attempt at developing self-regulatory practices based on fair information practices, and addressing many of the weaknesses in previous industry self-regulatory proposals as well as the FIP-based RFID Bill of Rights. The CDT working group that produced this proposal included a range of RFID industry leaders and consumer activists. Unfortunately, the proposal was not released until May 2006, which was after the completion of most of this research.

the US member of GS1. EPCglobal is charged to "establish and support the Electronic Product Code (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." In this role, they work closely with the International Standards Organization (ISO), international trade organizations such as the Association for Automatic Identification and Mobility (known as AIM Global), and many end-user firms. Current members of the EPCglobal Board of Governors include senior representatives from Proctor & Gamble, Sony, Lockheed Martin, and Wal-Mart, US Office of the Secretary of Defense, DHL, Hewlett-Packard, Metro AG, Cisco, Novartis, and Johnson & Johnson. Considering its mission statement and oversight, it is clear that EPCglobal acts in the interest of all types of firms that want to adopt RFID technology, and despite the technical challenges, they intend to develop technology allowing for widespread item-level tagging.

As a result of this interest, it is no surprise that EPCglobal has shown some sensitivity to the privacy tradeoffs that RFID entails. They attempt to address this with a series of four guidelines for consumer products. These are:

> - Consumers will be given clear notice, through a unique logo, of the presence of EPC on products or their packaging and will be informed of the use of EPC technology.
>
> - Consumers will be informed of choices to discard, remove or disable EPC tags in products they acquire.
>
> - Consumers will be able to easily obtain accurate information about EPC, applications, and technology advances. Companies using EPC will work to familiarize customers with the technology.
>
> - EPC data will be collected, used, maintained, stored and protected in compliance with applicable laws. Companies will publish information on their retention and use policies. (EPCglobal Public Policy Steering Committee 2005)

In the absence of any government regulatory actions, this policy allows firms to employ widespread item-level tagging, collect individual information, and use that information to gain market power, in such a way that optimizes firm profitability, with some basic provisions for consumer notice. It does not address what happens to tags after the point-of-sale, where many of the consumer benefits and costs are likely to be incurred.

Given the lack of direct and explicit protection of individual interests, the actual outcome of this policy will depend on exact consumer preferences for privacy, and other economic parameters, as explored in detail in Chapters five and six. A likely result for price-sensitive consumers is a widely deployed RFID system that drives down costs, resulting in lower price equilibrium, and greater consumption quantities. The widespread adoption of industry standards will result in minimal firm costs associated with deploying the technology and collecting and using information (relative to no regulation.) All firms are likely to see similar deployment costs, such as joining the standards organizations, and abiding by those guidelines. Individuals who benefit from RFID tags in general will similarly receive greater benefit from the adoption of standards. Conversely, the presence of standard tags, without any clear thought given to protecting data means that individual privacy will be worse off: it will be easier to collect personal information. Given these assumptions, the change in overall costs and benefits is summarized in Table 4-2.

Table 4-2: Stakeholder Costs and Benefits for an Industry Self-Regulation Policy

Individuals/ Consumers	Firms/Business	Government/Regulators	Society
Cost/benefit of technology: change in consumer prices	Fixed Cost of deploying RFID technology	Method & cost of policy or standards development/ implementation/ regulation	Change in overall social welfare
Cost/benefit of information effect on privacy	Variable (operating) costs of data collection	Cost of protecting civil liberties	Information commons
Benefit of information: Convenience, service	Cost of Information Control: Protection; Liability	Cost of no regulation (market failures, etc.)	
	Benefit of technology: cost reduction through enhanced logistics	Benefit of technology: logistics benefits to government consumers (military, libraries, etc.)	
	Benefit of information: Market power allows price discrimination, selling data, etc.	Benefit of information: data access for law enforcement, or regulation	

Increased costs/ Reduced benefits
Reduced Costs/ Increased Benefits
No expected change
Outcome of economic model

4.5.2. RFID Bill of Rights

The basis for the "RFID Bill of Rights" lies in codes of Fair Information Practices, which have propagated over the past thirty years. (Garfinkel, Juels et al. 2005) The "RFID Bill of Rights" distills the eight principles of the OECD guidelines down into the five that are summarized in Table 4-1, and presented here in full:

> Users of RFID systems and purchasers of products containing RFID tags have:
>
> 1. The right to know if a product contains an RFID tag.
> 2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
> 3. The right to first-class RFID alternatives. Consumers should not lose other rights (such as the right to return a product or travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag's kill feature.

4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
5. The right to know when, where, and why an RFID tag is being read. (Garfinkel, Juels et al. 2005)

These "rights" are a mapping of most of the key points from the OECD's Fair Information guidelines into recommendations that are relevant to RFID use. However, they do not address post point-of-sale issues well, so firms could still use any data collected in accordance with this policy, as long as they notified individuals why the data were being collected. Thus, firms can still gain market power, although it is likely to be at a lower level than under a self-regulatory or unregulated regime.

Further, it is evident this policy will add substantial cost to firms, who will need to maintain comparable RFID and non-RFID based systems, in order to abide by item number 3, and will also need to develop an infrastructure to alert customers to read activity. This cost is liable to be greater for a large firm, due to the extra infrastructure requirements related to the firm's size. Finally, enforcing the Bill of Rights guidelines would require the establishment of a government authority, perhaps similar to the privacy commissioner position that exists throughout the EU and in many other OECD nations. These increased costs, as shown by the preponderance of orange colored cells (compared to green) in Table 4-3 shows the result of a policy that is constructed with one set of stakeholder's interests paramount. As with the other policies, the indirect costs and benefits, highlighted in blue, will be addressed using the outcome of the economic analysis and related scenarios presented in chapters five and six.

Table 4-3: Stakeholder Costs and Benefits for the "RFID Bill of Rights" Policy

Individuals/ Consumers	Firms/Business	Government/Regulators	Society
Cost/benefit of technology: change in consumer prices	Fixed Cost of deploying RFID technology	Method & cost of policy or standards development/ implementation/ regulation	Change in overall social welfare
Cost/benefit of information effect on privacy	Variable (operating) costs of data collection	Cost of protecting civil liberties	Information commons
Benefit of information: Convenience, service	Cost of Information Control: Protection; Liability	Cost of no regulation (market failures, etc.)	
	Benefit of technology: cost reduction through enhanced logistics	Benefit of technology: logistics benefits to government consumers (military, libraries, etc.)	
	Benefit of information: Market power allows price discrimination, selling data, etc.	Benefit of information: data access for law enforcement, or regulation	

Increased costs/ Reduced benefits
Reduced Costs/ Increased Benefits
No expected change
Outcome of economic model

4.5.3. RFID Blocker Tags

The RFID blocker tag was first proposed in 2003 by researchers from RSA Laboratories, including the well-known security expert, Professor Ron Rivest. The blocker tag is designed to allow consumers who possess live RFID tags to selectively use them, while preventing arbitrary scanning. In doing so, it addresses the concerns that many of the proposed technical solutions do not offer this option, or have other technical drawbacks that are at least as large as their benefits. For example, one of the most common suggestions, killing tags at the POS, does not allow selective use post-sale, so it eliminates the possibility of taking advantage of post-POS benefits such as automatic processing of returned or recycled goods and home inventorying by smart appliances. Other technical proposals, such as encryption or hashing,

require a smart RFID tag. The actual technical merits of these solutions are still under debate, but it is clear that they will be computationally resource intensive for both tags and readers. While this is not a concern for readers, which are directly connected to power and can easily have sufficient local processing power, it is a concern for tags. In order to incorporate the ability to do encryption operations, passive RFID tags will need to be designed with substantially more processing power, and correspondingly more power. The cost of these modifications will likely prohibit their widespread retail use in the near term.[12] (Juels, Rivest et al. 2003)

The blocker tag works by being placed in proximity to ordinary tags. When present during an unauthorized scan, the blocker essentially "spams" the reader. More explicitly, the blocker tag takes advantage of the protocol that a tag reader uses to learn a tag's ID to make an unauthorized reader think that all possible serial numbers are present. For a basic standard tag, the number of possible serial numbers is at least 2^{64}, and for EPC tags it is at least 2^{96}, forcing the reader to stall in short order. When removed from the vicinity of a blocker tag, the reader and standard RFID tags resume normal operating behavior. Since a blocker tag can be manufactured by slight modifications to already existing tags, the developer's estimate is that the cost of a blocker tag will be only slightly more than the cost of a regular passive RFID tag. (Juels, Rivest et al. 2003)

In summary, the blocker tag appears to offer individuals the opportunity to protect themselves when desired, yet still obtain benefits from the use of RFID when they deem appropriate. Firms face slightly greater costs in developing tags and an operating protocol

[12] Although the exact cost implications of encryption are unclear, relevant data can be obtained from the Smart card market, where a common product, the Mifare® Ultralight (using Philips components) is available for $.70 in small quantities, $.59 for 50k quantities, and $.45 in 200k bulk orders. The corresponding product, with encryption, the Mifare® DESFire retails for $2.50 in small quantities, and $1.70 in a quantity of 50k. (Data are from www.idcardmarket.com/smartcard.html, accessed on Feb. 14, 2006.)

that integrates with the blocker concept. Once this is in place, the operating costs to the firm will be similar to those for any other RFID tag, so firms stand to still capture large logistic benefits, albeit less than in the self-regulation scenario.

Table 4-4: Stakeholder Costs and Benefits for the Blocker Tag Policy

Individuals/ Consumers	Firms/Business	Government/Regulators	Society
Cost/benefit of technology: change in consumer prices	Fixed Cost of deploying RFID technology	Method & cost of policy or standards development/ implementation/ regulation	Change in overall social welfare
Cost/benefit of information effect on privacy	Variable (operating) costs of data collection	Cost of protecting civil liberties	Information commons
Benefit of information: Convenience, service	Cost of Information Control: Protection; Liability	Cost of no regulation (market failures, etc.)	
	Benefit of technology: cost reduction through enhanced logistics	Benefit of technology: logistics benefits to government consumers (military, libraries, etc.)	
	Benefit of information: Market power allows price discrimination, selling data, etc.	Benefit of information: data access for law enforcement, or regulation	

Increased costs/ Reduced benefits
Reduced Costs/ Increased Benefits
No expected change
Outcome of economic model

Table 4-2 and Table 4-3 clearly highlight that much of the debate over RFID is between advocates of individual privacy and business users who see the logistics benefits first and foremost. These tables do not yet answer the question of how these costs and benefits, which represent fundamentally different interests, can be balanced. The economic model developed and explored in Chapters five and six is a first attempt at such an analysis.

5. Economic model

The economic model constructed here provides a tool for analyzing the impact of different policies upon the choices faced by producers and consumers of products that might reveal personal information due to the use of RFID. This model integrates four ideas previously discussed. First is the notion that private information can be treated as an economic good. The second idea is individuals are heterogeneous with respect to the value that they place on privacy. The third key aspect of the model is that firms can collect private information, by individually tagging items with RFID, and use this information to gain market power in the form of both reduced costs and price discrimination. Finally, the fourth fundamental facet of the model is that policies can be understood and implemented by their costs to both firms and individuals. The incorporation of each basic component is outlined below, as an overview of the whole model, and then subsequently described in detail.

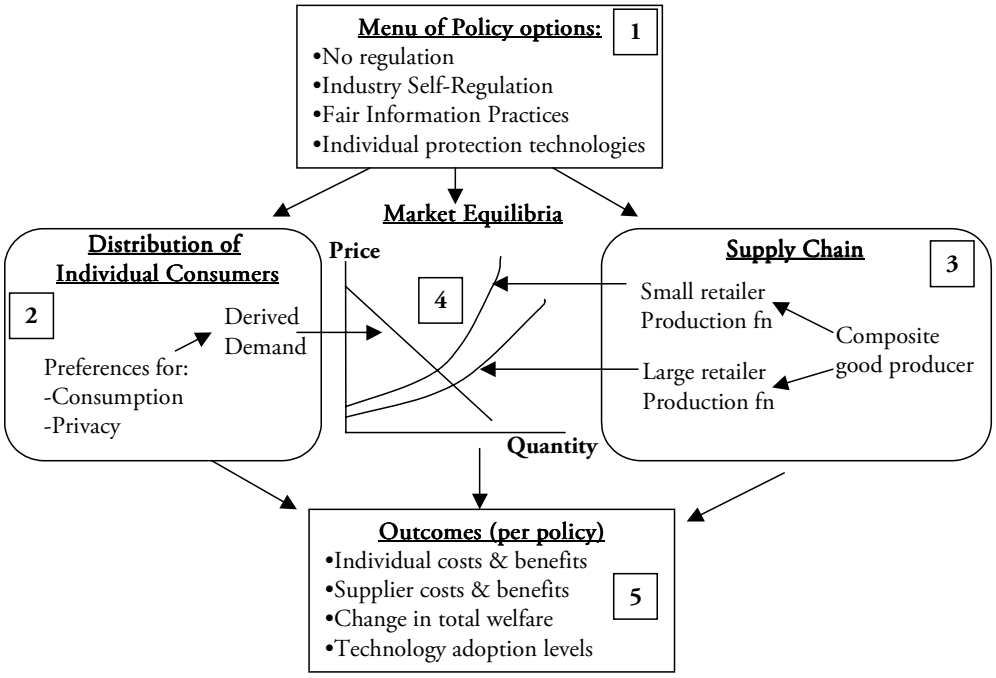
5.1. Model Overview and Assumptions

Figure 5-1 is a simple pictorial representation of the key components of the model, how they interact, and how model outcomes are produced in order to assess the various policy options. The model consists of producers, individuals, policies, and a calculated market equilibrium that leads to outcomes that are the basis for evaluation. The producer side of the model consists of a composite good, supplied through a competitive market to both a large retailer (such as Wal-Mart), and a small retailer. A large and competitive market means that the retailers are both price-takers. Costs for the two retailers are the summation of fixed costs, a constant variable cost to acquire the composite good, and another variable cost due to managing inventory. Currently the two retailers are in a strategic equilibrium, but the large retailer is in the process of implementing item-level RFID tagging, in order to reduce

the cost of inventory management. Although there are fixed and variable costs to this implementation, it will ultimately drive down the large retailer's costs, resulting in a lower priced composite good. In addition, once the large retailer deploys RFID, it will collect personal information, and use this to price discriminate. The large retailer can then choose a quantity of information that maximizes profits. In response, the small retailer can choose both a price strategy and an RFID implementation plan, given their own possible production gains from using RFID, and a similar option to price discriminate.

Figure 5-1: Economic model overview

For individuals, the model is constructed around heterogeneous preferences for privacy



versus consumption of the composite commodity. The privacy preference is modeled as a threshold effect, where if a firm collects a quantity of information below an individual's threshold, that individual will purely maximize consumption at the lowest price. If the quantity of information collected is above the threshold, then individuals will protect themselves. Protection occurs by either choosing the fringe retailer, assuming that retailer is

not collecting personal information, by taking defensive actions to guard privacy during consumption, or by a mixed strategy. Individuals have information about the firm's actions, so they can make the choice that maximizes consumption, subject to protecting privacy up to the threshold level.

The cost of individual privacy protection, cost of implementation of item-level RFID tracking, and benefit from market power are all functions of governing policies. As a result, outcomes such as firm profits, production quantities, quantity of information collected, and changes in consumer welfare will vary according to policy, and this might have substantial impact on the ultimate costs and benefits at all levels. These outcomes are determined through numeric calculation of the equilibrium conditions for each policy, each firm strategy choice (adopting RFID or not, fringe firm price strategy), and several different models of firm strategic interaction. In addition to these variations, outcomes are explored for many additional parametric variations, such as changes in individual preferences or heterogeneity, and different maximum levels of price discrimination. Details for each of these steps are described below. First, I present Table 5-1, a summary of the terminology used in the analysis.

Table 5-1: Descriptions of parameters and model terminology

Parameter	Description
Individual and Individual Distribution Characteristics	
I	Individual income
I_a	Individual income adjusted after privacy protection
N_L	Individual threshold for acceptable quantity of personal information disclosed
N_0	Starting quantity of personal information
R	Correlation coefficient between I and N_L
% N_L=0, % N_L=max	% of distribution with $N_L = 0$ and with $N_L = N_{max}$
N_{min}, N_{max}	Minimum and maximum possible values of N_L
σ_I	Standard deviation of I

Parameter	Description
σ_{NL}	Standard deviation of N_L
Firm Characteristics	
A_d, A_f	Fixed cost to dominant (d) and fringe (f) firms
B_d, B_f	Linear variable cost coefficient to dominant (d) and fringe (f) firms
D_d, D_f	Quadratic variable cost coefficient to dominant (d) and fringe (f) firms
C_d, C_f	Total cost to dominant (d) and fringe (f) firms
D_s	Cost benefit from implementing RFID
P_s	Commodity supplier price to retailers
S_p	% of consumer surplus that can be collected through price discrimination
N	Target quantity of information to collect from individuals
Policy Characteristics	
Y	Policy choice
D_{dm}, D_{fm}	Realizable % of theoretical cost benefit (D_s) for each firm
P_N	Price of individual protection
P_{tag}	Price of an RFID tag
Model and Simulation Characteristics and Terminology	
P_c	Equilibrium price
Q_c	Equilibrium quantity of commodity good
Q_d, Q_f	Quantity of composite good provided by dominant and fringe firms
α	Demand curve slope parameter
β	Demand curve exponential parameter
π_d, π_f	Profit for dominant and fringe firms
CS	Consumer Surplus
N1	Normal distribution basis of N_L
N2	Normal distribution basis of uncorrelated Income
N3	Weighted distribution combining N1 and N2 using R, to generate correlated Income
Nact	Actual quantity of information collected by firm(s)
Scenario	A set, consisting of a unique value for all non-policy parameters, forming the basis for each simulation run
Strategic Model/ Strategy	The economic interaction between firms, primarily fringe firm choices about RFID adoption and price

5.2. Policy Options

In the model, several policies are evaluated. Each policy, Y, is enumerated according to appropriate model parameters. These parameters are the price for individuals to protect themselves, per unit of information, P_N, the price of an RFID tag, the benefit to firms in cost reduction from the use of RFID, and the fixed and variable cost of a firm's implementation of the policy. The policies explicitly tested are the three elaborated in chapter four, the RFID blocker tag, industry self-regulation, and the RFID bill of rights, along with an estimation of what would happen if there was no governing policy. Parametric values chosen for each of these are discussed below.

5.3. Individuals

Individuals are described by preferences for consumption or privacy protection, expressed through a varying demand curve. Each individual has a unique demand curve that is a function of both income and the taste for privacy. The same initial level of personal information, N_o, exists for all individuals. The taste for privacy is expressed as a random draw out of a normal distribution[13], representing the amount of personal information that an individual wants to protect, N_L, which is a value less than or equal to the initial quantity, N_o. N_L can be negative, indicating an individual who is willing to sell personal information. A second random draw from a normal distribution is used to create a nominal income value. Nominal income and privacy taste (N_L) are correlated over [-1,1], according to user

[13] The population is divided into 3 groups according to the Westin model discussed in chapter 2: those who will not allow any information collection, those who are unconcerned and will allow any amount of information to be collected with no defensive action, and those in the middle. A random uniform draw is used to segment the population into these three groups. A random normal draw is then used to distribute the middle group of individuals.

specification, to produce a real income, I. The real income is spent to purchase a quantity, Q_c, of composite commodity product c, at price P_c.

Consumption of c is subject to two constraints, where N is actual amount of information a firm intends to collect for all individuals:

1) $N_o - N \geq N_L$, i.e., the firm can't collect more information than any individual is willing to give up. This is not applicable in a baseline case where no information is collected by either firm, but otherwise applies in all situations where one or both firms can collect information. If the firm's desired quantity of information, N, exceeds the threshold, individuals will protect themselves by reducing consumption in favor of privacy. For those individuals, the firm can only collect information up to the threshold value.

2) Demand:

For the purposes of this analysis, demand for the j^{th} individual in a distribution is assumed to be a function of the form:

$$P_c = I_j - P_N(N_{L,j} - N_o + N) - \alpha Q_{c,j}^{\beta} \quad (1)$$

In the case where $N_L \geq N_o - N$ then the firm collects less than the individual is willing to freely give up, and demand reduces to a simpler form:

$$P_c = I_j - \alpha Q_{c,j}^{\beta} \quad (2)$$

When $N_o - N \geq N_L$, individual demand will depend on the firm choices, which are explained in more detail as a part of the equilibrium analysis. If both firms collect information, then equation (1) holds as the demand. If the fringe does not collect information, but matches the dominant firm price, then individuals can consume some goods according to equation (2), up to the fringe equilibrium (profit maximizing) limit. Above that limit, they will consume according to equation (1). However, if the fringe does

not collect information, and the price difference between equation (1) and equation (2) is great enough, then individuals will sort into three groups, according to privacy taste:

- Individuals with $N_L \geq N_o - N$ will maximize consumption at the lower price, according to the demand in equation (2).
- Individuals with $N_o - N \geq N_L$ and a cost of protecting information that is less than the retailer price differential will spend some money to protect privacy, and the remainder on consumption, according to equation (1). This case will occur if either the cost of protection is low, or the quantity of information to be protected is small.
- Individuals with $N_o - N \geq N_L$ and a cost of protecting information that is more than the retailer price differential will consume from the higher priced retailer according to the demand specified by equation (2). This occurs if either the cost of protection is high, or the quantity of information to be protected is large.

5.4. Supply Chain

The supply chain consists of 3 firms: firm d, a dominant retail firm, firm f, a representative fringe retail firm, and a wholesale supplier, firm s. The wholesale supplier is assumed to exist in a competitive market, so it is not a significant contributor to the model and analysis. The respective cost functions for the dominant and fringe firms are:

$$C_d = A_d(y) + B_d Q_d + D_d(y, N) Q_d^2 \quad (3)$$

$$C_f = A_f(y) + B_f Q_f + D_f(y, N) Q_f^2 \quad (4)$$

where

$$B_d = B_f = P_{tag}(y) + P_s \quad (5)$$

That is, each firm has a fixed cost, A, a linear cost component, B, and a second order cost component D. The fixed cost, A, is specified as a function of policy. That is, each policy has a constant cost associated with implementing RFID, such as placing signs advertising the presence of RFID tags. The linear cost component, B, is equal to the retailer's purchase price for the composite commodity, P_s, which is taken as exogenous, plus the price of the tags, P_{tag}, which is a function of policy, when there is item-level tagging is ongoing, and quantity. (As volume increases, tag price decreases.) The higher order cost component, D, accounts for logistic complexities such as shipping and warehousing that increase at a rate greater than linear. For simplicity, it is here assumed to be second order. D is also a function of the policy and of the quantity of information firm w or f collects. Because the policy can dictate how information is collected, stored and used, it affects the potential for cost savings. Independently, the more information a firm collects and uses, the greater the cost savings, in improved inventory efficiencies. Generally, the dominant supplier has lower production costs than the fringe, due to economies of scale, and this is captured in the values for A and D. Final market prices and quantities are resolved through several distinct models of firm strategic interaction detailed below in the equilibrium analysis.

5.4.1. Price Discrimination

In addition to inventory efficiency, the use of RFID offers opportunities for firms to collect information and profile individuals in order to price discriminate, as previously discussed. This is implemented in the model by allowing the firm to capture some of the consumer surplus that exists. The firm does this by identifying those customers who are willing to pay a higher price, and offering pricing schemes that collect that additional revenue. In this analysis, the amount of price discrimination is proportional to both the

amount of information collected, and a user specified maximum amount to be captured. Each simulation run specifies an amount, S_P, assuming all available information is collected. During analysis, the total consumer surplus is calculated, and a linear proportion is applied as extra firm revenue, as a function of the amount of information collected. S_P weights this value, to arrive at a final profit based on the transfer of some consumer surplus to the firm.

This is shown graphically in Figure 5-2, where Q_e and P_e represent the market equilibrium price and quantity, respectively.

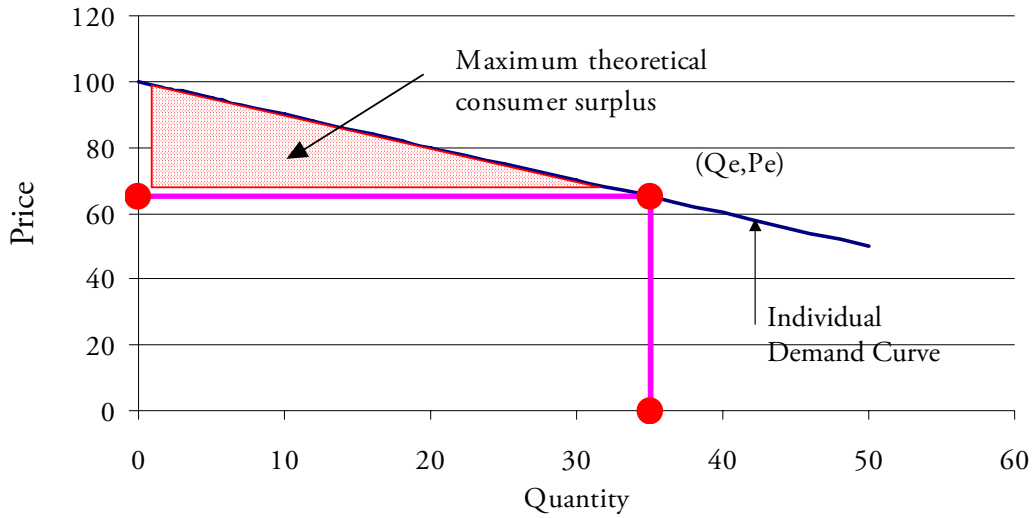


Figure 5-2: Consumer Surplus

With no price discrimination, revenue is simply the rectangular area defined by Qe*Pe, but the triangular area above P=Pe is consumer surplus. The amount of surplus can be calculated in a direct manner, by integrating the whole area under the demand curve, and subtracting off the revenue already collected by the firm. In this analysis, the integration is:

$$CS = \int_0^{Q_w} \left(I_j - P_N (N_{L,j} - N_o + N) - \alpha Q_c^{\beta} \right) \partial Q_c - Q_d * P_e \qquad (6)$$

Letting

$$I - P_N (N_L - N_o + N) = I_a \qquad (7)$$

Then

$$CS = \int_0^{Q_w} \left(I_a - \alpha Q_c^{\beta} \right) \partial Q_c - Q_d P_e \tag{8}$$

$$CS = I_a Q_d - \frac{a Q_d^{\beta+1}}{\beta+1} - Q_d P_e \tag{9}$$

Thus, the actual total revenue collected is:

$$S_p\left(N / N_0 \right)\left(I_a Q_d - \frac{a Q_d^{\beta+1}}{\beta+1} - Q_d P_e \right) + Q_d P_e \tag{10}$$

In equation 10, N/N_0 is the percentage of total information that the firm actually collects.

5.5. Equilibrium Analysis

The final supply and demand curves result in market equilibrium. This equilibrium is calculated for each of the strategic options that the firms have, for each parametric scenario, and is a function of the policy parameters. As a result, under different policies, firm revenues and profits will vary, and so will consumer surplus. In addition, the overall amount of information collected is a factor in subsequent analysis of the information commons.

Three different models of strategic interaction are developed. In all three models, individuals will consume according to the specified demand curves, which will adjust according to the amount of information the firms intend to collect, as already described. The first model is a monopoly, where the fringe firm is excluded. In the initial implementation, the monopolist does not collect information, and merely sets quantity and price to maximize profit. (This is simply the quantity where MR=MC, and then price is set according to the demand curve.) In the second implementation, the monopolist collects personal information

and uses that to price discriminate. The monopolist then can set both price and quantity of information to maximize profit. This is numerically solved, as detailed below.

The second interaction model is the so-called dominant and fringe model. In this case the retail price is set at P_c = marginal cost for the fringe firms. (If price exceeds marginal cost, then fringe firms will enter, driving price down. Similarly, if price is less than marginal cost, fringe firms will exit the market, reducing supply, and driving price up.) Once the fringe firm absorbs demand at this price, the dominant firm selects their quantity, to maximize profit. In the initial case, as with the monopoly, no information is collected. In the three subsequent strategic choices, information is collected by either the dominant firm, or by both firms, as shown in Table 5-2. Additionally, the fringe firm can choose to either match the new price, or maintain the old, higher price. In either case the dominant firm can select both a quantity of information and a price, in order to profit maximize. These solutions are resolved numerically.

The third interaction model is the Cournot duopoly, which is developed by determining appropriate constraints describing the interplay between the two firms. That is, each firm takes the other firm's quantity as exogenous, and maximizes their own quantity accordingly. The first order conditions for each firm's profit maximization equation give what are called the reaction functions, as derived here for the dominant firm.

$$\pi_d = P_c Q_d + CS - \left(A_d(y) + B_d Q_d + D_d(y,N) Q_d^{\,2}\right) \tag{11}$$

Letting

$$I - P_N(N_L - N_o + N) = I_a \tag{12}$$

then

$$\pi_d = \left(I_a - \alpha Q_c{}^{\beta}\right)Q_d + S_p \frac{N}{N_0}\left(I_a Q_d - \frac{aQ_d{}^{\beta+1}}{\beta+1} - Q_w P_e\right) - \left(A_d + B_d Q_d + D_d Q_d{}^2\right) \qquad (13)$$

Expanding terms:

$$\pi_d = \left(I_a - \alpha\left(Q_d + Q_f\right)^{\beta}\right)Q_d + S_p \frac{N}{N_0}\left(I_a Q_d - \frac{aQ_d{}^{\beta+1}}{\beta+1} - Q_d P_e\right) - \left(A_d + B_d Q_d + D_d Q_d{}^2\right) \qquad (14)$$

The final form of the reaction function is then:

$$\frac{\partial \pi_d}{\partial Q_d} = \left(I_a - \alpha\left(Q_d + Q_f\right)^{\beta}\right) - \alpha\beta Q_d\left(Q_d + Q_f\right)^{\beta-1} + S_p \frac{N}{N_0}\left(I_a - Q_d\right) - B_d - 2D_d Q_d = 0 \qquad (15)$$

The fringe firm reaction function is symmetric to the dominant firm function:

$$\frac{\partial \pi_f}{\partial Q_f} = \left(I_a - \alpha\left(Q_d + Q_f\right)^{\beta}\right) - \alpha\beta Q_f\left(Q_d + Q_f\right)^{\beta-1} + S_p \frac{N}{N_0}\left(I_a - Q_f\right) - B_f - 2D_f Q_f = 0 \qquad (16)$$

The Cournot model is applied to the same four model schemes as the dominant-fringe model, as shown in Table 5-2.

Table 5-2: Summary of behaviors analyzed in model

Strategic Model	Market Interaction
Monopoly 1	Monopoly retailer maximizes profit by setting price.
Monopoly 2	Monopoly retailer maximizes profit by setting price and quantity of information collected. Individual income and consumption is reduced by information protection.
Dominant-Fringe 1	No information collection. Fringe firm sets price at marginal cost (p=mc), Dominant firm chooses quantity to maximize profit.
Dominant-Fringe 2	Dominant firm has item-level tagging, and chooses quantity of information to collect, and price, to maximize profit. Fringe firm maintains price from model Dominant-Fringe 1. Individuals sort between firms, according to taste for privacy.
Dominant-Fringe 3	Fringe firm matches price of dominant firm, selling the quantity where p=mc. At that price, dominant firm chooses quantity of units and information, to maximize profit. Individuals consume from the fringe, up to fringe profit maximizing quantity, then consume from dominant firm, protecting information if necessary.
Dominant-Fringe 4	Fringe firm adopts RFID and matches price of dominant firm, setting p=mc again. Dominant firm chooses quantity of good and information, to maximize profit. Individual income and consumption is reduced by information protection
Cournot 1	No information collection. Both firms maximize profits subject to Cournot reaction constraints.
Cournot 2	Dominant firm adds RFID to products, chooses amount of information to collect, and price, to max profit. Fringe firm maintains price from Cournot 1. Individuals sort between firms, according to taste for privacy.
Cournot 3	Both firms maximize profits subject to Cournot reaction constraints. Individuals consume from the fringe, up to fringe profit maximizing quantity, then consume from dominant firm, protecting information if necessary.
Cournot 4	Fringe firm adopts RFID and matches price of dominant firm. Both firms maximize profits subject to Cournot reaction constraints. Individual income and consumption is reduced by information protection

5.6. Outcomes

The model can be used to explore the effect of policies on many different outcomes, which are representative of the interests of many of the key stakeholders. For firms, the model can be used to calculate firm production quantities and profits, and changes in the relative market power of the two participant firms. Individual interest can be assessed by changes in consumer surplus, as well as consumption quantities. The broader interests, represented by the government and society, can be partially assessed by total changes in welfare. However, the amount of information that is collected and used is also an important contributor to the broader information commons issues of interest to society, and the relative impact of different policies on that quantity can also be observed.

In all cases, although the model is ultimately run with specific parameters, and sensitivity analysis is performed on many of those parameters, as discussed in Chapter six, no credence can be given to actual numerical results. Instead, the primary value comes from being able to relatively rank the different evaluated policies, using the different interaction models, for the different outcomes. Results are reported in this way, for each of the key outputs. In addition, parametric sensitivities in the relative rankings are examined. Finally, the model can also be used to assess firm strategy choices, especially for the fringe firm. Assuming that the fringe has good information about consumer preferences, they will choose the instance of strategy 2, 3, or 4 that offers maximum profit. The sensitivity of this choice to policy choices and parametric sensitivity is also reported.

5.7. Model implementation

The model described above is realized with Microsoft Excel and the included Solver package, which can be used to find optimum solutions for numerical systems such as those

developed here. As discussed above, a demand function is created for each individual, assuming that individuals are heterogeneous in income I, and I can have any degree of correlation with N_L over the range of [-1,1]. The distribution of N_L is assumed to have 3 parts: a percentage of individuals with $N_L = N_{min}$ (i.e., they either don't care about controlling their information at all, or if $N_{min}<0$, they are willing to sell personal information), a percentage of individuals with $N_L = N_{max}$ (they will always choose to protect personal information), and a remaining (most likely predominant) group who are distributed in between the extremes. For now, we assume that this group is normally distributed, with a user specified mean and variance. The partitioning into the three groups is user-defined, and can be varied during different simulation runs.

The population consists of one thousand individuals, each represented by a demand curve. $I_{,j}$ and $N_{L,j}$ are created for each member of the distribution using draws from three 1000-element distributions of random numbers. The first distribution is U(0,1), and is used to partition the individuals into the three components of N_L described above, and according to the user specification. The second and third distributions, N1 and N2, are both defined as N(0,1). The N1 distribution is used to create $N_{L,j}$ according to $N_{L,j} = N_L + N1_j * \sigma_{NL}$, where N_L and σ_{NL} are the user specified mean and standard deviation for the normally distributed central group. All three distributions are generated using the built-in Excel random number generator, which can produce draws of standard distributions. While this random number generator is not ideal, results were tested and found to be adequate for this simulation.[14]

[14] Statistical characteristics of the 3 distributions are:

- The U(0,1) has mean of .4937 and standard deviation of .295. A perfect U(0,1) distribution would have mean .5, and standard deviation = 0.2887.
- N1=N(0,1) has mean of 0.017 and standard deviation of 0.981.
- N2=N(0,1) has mean of –0.032 and standard deviation of 1.01.

The correlation between N_L and I is produced by creating a new number that is a combination of the second and third random distributions, according to:

$$N3_j = R * N1_j + N2_j * \left(1 - R^2\right)^{0.5} \quad (17)$$

Here R is the user specified correlation factor, varying over [-1,1]. N3 is used to create the actual income for each individual, I_j, according to:

$$I_j = I + N3_j * \sigma_I \quad (18)$$

Equation 18 produces an income that is normally distributed with a user specified values for mean income, I, and standard deviation, σ_I. It is possible, for large values of σ_I or σ_{NL}, or for a skewed distribution, that the calculated value of $N_{L,j}$ will exceed the user specified upper or lower limits. In these cases, $N_{L,j}$ is fixed to the appropriate limit value (max or min), and I_j is normally distributed, using N3, around the correlated endpoint value.[15] Individuals already randomly drawn to be at one of the limits are also normally distributed around the same endpoint values, using N3. The effect of the correlation between and the variance within N_L and I is shown in Figure 5-3 below.

[15] For example, if mean N_L is 2 standard deviations from the maximum value (endpoint), then the correlated endpoint value for I is $I + 2*R*\sigma_I$, i.e, if R=1, it is exactly 2 standard deviations above the mean I. If R = .5, then it is one standard deviation greater than I.

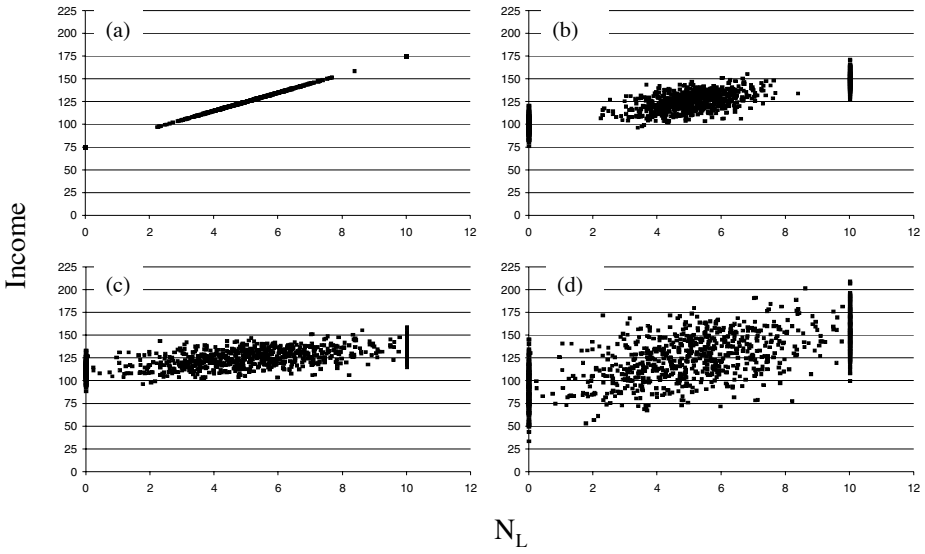


Figure 5-3: Effect of correlation between and variance within N_L and I.

Figure (a) shows perfect correlation (R=1) and small variances (σ_{NL}= 1, σ_I =10). Figure (b) has R=0.5 with the same variances. Figure (c) has R=0.5, σ_{NL}= 2 and σ_I =10. Figure (d) has R=0.5, σ_{NL}= 2 and σ_I =25.

A nominal series of model parameters are specified as baseline characteristics of firm and individual behavior (i.e., coefficients in the firm cost functions, and for policy cost to individuals), and then modified according to the policy selected, and the amount of information collected. These parameters, and the type of modifications for each are described in Table 5-3, below. These assumptions are based on the RFID characterization reported in chapter three, and the policy assessments of chapter four. The specific values are the result of experimental characterization of an initial model, and the selection of parametric values that produce reasonable outputs. The quadratic cost coefficients, D_d and D_f, are described by a decreasing function that varies with policy, quantity of item-level tagging the firm employs, and a user specified limit, D_s, on the cost benefits expected from implementing RFID. D_s is experimentally varied during simulation runs. The specific values for D_d, D_f, A_d, and A_f were empirically determined to match the characterization of RFID technology reported in chapter three, where a 2-3 year payback period can be expected, along with a 10-20% annual

cost savings, using industry self-regulation as the baseline policy in this case, and adjusting the other policy costs and benefits according to the analysis of chapter four.

Table 5-3: Variation in Model Coefficients

Parameter	Initial Value	Policy specific modification	
P_N	0	8	No regulation
		2	Blocker tag
		6	Industry self-regulation
		4	RFID bill of rights
P_S	10	No change – competitive commodity price	
P_{tag}	1	=1/N (price falls as volume increases)	
		=1.5/N for Blocker tag policy	
A_f	0	15	Blocker tag
		10	Industry self-regulation
		30	RFID bill of rights
D_f	2	$2-D_s*D_{fa}(Y)*(N/N_0)$ where D_s is experimentally varied and $D_{fa}(Y)$ is listed below	
		0.5	No regulation
		0.3	Blocker tag
		0.4	Industry self-regulation
		0.2	RFID bill of rights
A_d	0	20	Blocker tag
		10	Industry self-regulation
		50	RFID bill of rights
D_d	1	$1-D_s*D_{da}(Y)*(N/N_0)$ where D_s is experimentally varied and $D_{da}(Y)$ is listed below	
		1	No regulation
		0.4	Blocker tag
		0.8	Industry self-regulation
		0.4	RFID bill of rights

These scenario specific parameters, and the 1000-element distribution of individuals are then used to calculate equilibrium conditions for each scenario, using the Excel solver package to guess price, P, and information quantity, N, that maximize the profit of the dominant firm. The Solver is not good at finding global solutions to non-linear systems of equations, such as those developed here; it is very sensitive to initial conditions, and is only reliably able to find local extrema. To address this problem, an Excel program was written to

pick proper initial conditions for the solver. The program creates a 100-element data table, reporting the dominant firm profit for all combinations of 10 levels of both P and N. These levels are automatically scaled at even steps between the minimum and maximum of each. For N, those are user-defined; for P, the maximum is set as the mean income, and the minimum as half of the mean income, during the 1st case of each firm interaction model (Monopoly 1, Dominant-fringe 1, and Cournot 1.) In subsequent interaction models, the maximum is set as the optimum price eventually calculated in model 1, and the minimum is set as half of that price. Once these levels are established, the data table is populated with dominant firm profit for each combination, the maximum profit is identified, and the values of P and N associated with that profit are used to initialize the Excel Solver.

Once these initial conditions are specified, another program runs the solver through each of the scenarios for each of the strategic interaction models. The solution basis for each of these calculations is shown in Table 5-4, below. These solution methods are employed for each of more than six hundred simulation runs that examine variations in many of the key parameters, including R, D_s, S_p, σ_I, σ_{NL}, N_L=0 and N_L=max, for each of four policies: no regulation, industry self-regulation, RFID blocker tag and RFID bill of rights, as discussed at the beginning of Chapter six.

Table 5-4: Equilibrium model calculations

Strategic Model	Solution Method
Monopoly 1	Guess price to maximize firm profit.
Monopoly 2	Guess price and N to maximize firm profit.
Dominant-Fringe 1 (Baseline)	Guess price; calculate total quantity for each consumer; set fringe quantity at p = mc, and dominant firm at (Total-Fringe quantity). Dominant firm chooses price to maximize profit.
Dominant-Fringe 2	Fringe firm maintains price from Dominant-Fringe 1. Individuals spend either I at old price at fringe firm, or Ia (reduced by information protection) at new price at dominant firm, and choose whichever leads to maximum consumption. Dominant firm chooses new price, and N, to maximize profit, including price discrimination.
Dominant-Fringe 3	Dominant firm chooses P, N to maximize profit with price discrimination. Fringe matches dominant firm price; Fringe quantity is set at p = mc. After fringe quantity is determined, income is adjusted according to N, and remaining income is spent at the dominant firm.
Dominant-Fringe 4	Dominant firm chooses P, N to maximize profit, with the same model setup as in the baseline. For all consumption, income is reduced according to the amount of information collected. Both firms can price discriminate.
Cournot 1 (Baseline)	Guess Q_f, P to maximize dominant firm profits, constrained by reaction functions.
Cournot 2	Fringe firm maintains price from Cournot 1. Individuals spend either I at old price at fringe firm, or Ia (Income reduced by information protection) at new price at dominant firm, and choose whichever leads to maximum consumption. Dominant firm chooses new price and N to maximize profit, including price discrimination.
Cournot 3	Guess Q_f, N, P to maximize dominant firm profit, with price discrimination, and reaction function constraints. Income is adjusted according to information collection and fringe quantity, and remaining income is spent at the dominant firm.
Cournot 4	Guess Q_f, N, P to maximize dominant firm profit, with price discrimination, and reaction function constraints. Demand curve is reduced according to information collection. Both firm profits include price discrimination.

6. Results and Discussion

This chapter reports simulation results for the parametric and policy variations described at the end of chapter five. Many dependent variable outputs are observed, as a function of variation in many independent input parameters. The large quantity of simulations makes analyzing individual runs difficult, so parametric sensitivities are investigated by performing ordinary least squares linear regressions for each output, in order to identify significant parameters. Identifying the significant factors allows the parameter estimates for each policy to be used as the method of sorting policies, and reporting the relative effect of each of the different policies for each output of interest, as discussed in chapter five. An initial sensitivity analysis is reported first, followed by a more detailed graphical analysis of select parameters, policies, and outputs; then a discussion of the key results is presented along with how they link back into the stakeholder framework analysis of chapters three and four. The linkage to the framework is provided by means of three hypothetical scenarios that are used as the basis for predicted parametric and qualitative outcomes.

6.1. Initial results and analysis of simulation outputs

A total of 168 different sets of parametric permutations were modeled. These runs primarily explored all possible permutations for the parameters shown in Table 6-1, for each of the four explored policies, and for each of the three models of firm strategic interaction. These runs were augmented by an extension designed specifically to investigate the effect of heterogeneity in individual preferences, which other economic research has identified as critical. (Ulph and Vulcan 2000; Tang, Hu et al. 2005) This extension is shown in Table 6-2 below. In total, there were 2016 (168*3*4) simulation runs.

Table 6-1: Completely explored parameter space.
Simulations were performed using all possible combination of parameter values shown in this table.

Parameter	Simulation values
R (Income-Privacy correlation)	0.75, 0, -0.5
D_s (Cost savings)	0.6, 0.3
S_p (Price discrimination)	0.75, 0.25
I (Income)	100, 125, 150
% N_L=0	0.3, 0.15
% N_L=max	0.3, 0.15

Table 6-2: Extended parameter space exploring heterogeneity

Parameter	Simulation values
R (Income-Privacy correlation)	0.75, 0, -0.5
D_s (Cost savings)	0.6, 0.3
S_p (Price discrimination)	0.75, 0.25
I (Income)	125
% N_L=0	0
% N_L=max	0
σ_I	5, 25
σ_{NL}	1.5, 0.3

Although N_L did not explicitly deviate in these simulation runs, the variations in the three segments of the constructed population (% N_L=0, % N_L=max, and the remaining population) similarly affect the mean limit value. With the chosen parameters, the calculated theoretical mean N_L varies over the range of 4.25-5.75. Other model parameters, such as demand slope, and demand exponent were only explored in simple one-off experiments to verify that the model is not uniquely sensitive to the linear structure employed.

Each of the four policies is described by firm costs and benefits, and individual protection costs, as set out in Chapter five. Table 6-3 shows the summary of chosen parameters. (An alternative explanation is to consider that one policy is being evaluated, and the different options represent some uncertainty in the relative costs and benefits of the

single policy. The simulation runs are exploring that uncertainty, and the names given to each set of parameters are indicative of how the uncertainty varies in that particular case.) Trial runs of the simulation model were used to determine a range of generally feasible values (i.e., where reasonable numeric solutions would be observed.) Specific values were then chosen according to the qualitative policy analysis presented in Chapter four (in reality, none of the policies are well enough specified at this point to merit any more detailed investigation of their true costs). Two additional assumptions were made:

- For any given policy, fringe firms gain half the cost benefit of the dominant firms. This is due to the general ability of the large firm to take advantage of existing logistic superiority to a greater extent than any small firm would be able.
- Parameters should spread out over a large range of the possible space, in order to explore a wide range in parametric uncertainty in policy costs and benefits.

Table 6-3: Policy parameters employed in simulation runs

Policy	P_N	P_{Tag}	A_d	A_f	D_{dm}	D_{fm}
No Regulation	8	1	0	0	1	.5
Blocker Tag	2	1.5	20	15	.4	.2
Industry Self-regulation	6	1	10	10	.8	.4
RFID Bill of Rights	4	1	50	30	.4	.2

In Table 6-3, the parameters P_N, P_{tag}, A_w and A_f each have the same definition as those provided in Chapter five. The parameters D_{wm} and D_{fm} represent the fraction of the simulation run specific D_s that each firm can realize. That is, with no regulation, the dominant firm (firm w) can obtain 100 percent of the theoretical maximum cost savings, but the fringe firm can only receive half of the theoretical maximum.

A total of 76 different output measures were calculated for each simulation run. These are listed in Table 6-4 below, organized by the firm interaction models described in chapter

five. Each in the series of parameters described as Deltas (e.g., Delta Price) are the difference between each parameter's result in the chosen scenario with the same parameter's result in the baseline (scenario 1) case. The final category, fringe firm optimum, represents the strategic choice by the fringe firm; assuming that they have complete information about their profit under each choice, they choose among 2, 3, or 4, by selecting their RFID and price strategy to maximize profit. Once that choice is made, the output parameters in that scenario are equivalent to those in the chosen strategy. This set of simulations was run in Excel, as described in Chapter five. For the chosen range of parameters, nearly all outcomes are possible by selecting the appropriate combination of values. This is demonstrated in Table 6-5 below, which shows a summary of the rank ordering of policies for several of the key outputs in the Fringe firm optimum scenario. The table was produced by rank ordering each of the listed outputs from highest to lowest (represented by 1-5 in the table) and then counting the number of occurrences of each policy at each rank. The summations in Table 6-5 are conducted across the Cournot, Dominant-Fringe and Monopoly models, resulting in 504 total simulation cases. The exception to this is for fringe firm profit, which is not included in the monopoly model, and has 336 total cases.[16] In addition to the four policies parametrically described in Table 6-3, a fifth option is included in the ranking, which is the pre-RFID value of the output parameter, denoted as "Pre-regulation" in Table 6-5, and subsequently. With this option, there is no information collected. Tables summarizing the ranked outcomes for these same parameters for each of the other individual interaction scenarios are presented in Appendix B. They show similar patterns to those presented in Table 6-5.

[16] Note that the summation of rankings does not always equal 504, because policies occasionally are tied, and both receive the higher rank.

Table 6-4: List of simulation calculated output parameters

Strategic Model (# of outputs)	Parameters
1 (7)	Price (P_Sc1), Quantity (Q_Sc1), Fringe Firm Quantity (Qf_Sc1), Dominant Firm Quantity (Qd_Sc1), Fringe Profit (πf_Sc1), Dominant Firm Profit (πd_Sc1), Consumer Surplus (CS_Sc1), Total Surplus (TS_Sc1)
2 (17)	Price (P_Sc2), Quantity (Q_Sc2), Fringe Firm Quantity (Qf_Sc2), Dominant Firm Quantity (Qd_Sc2), Fringe Profit (πf_Sc2), Dominant Firm Profit (πd_Sc2), Consumer Surplus (CS_Sc1), Firm Target Information Quantity (N_Sc2), Firm Actual Collected Information (Nact_Sc2), Delta Price (ΔP_Sc2), Delta Quantity (ΔQ_Sc2), Delta Fringe Firm Quantity (ΔQf_Sc2), Delta Dominant Firm Quantity (ΔQd_Sc2), Delta Fringe Profit (Δπf_Sc2), Delta Dominant Firm Profit (Δπd_Sc2), Delta Consumer Surplus (ΔCS_Sc2), Total Surplus (TS_Sc2)
3 (17)	Price (P_Sc3), Quantity (Q_Sc3), Fringe Firm Quantity (Qf_Sc3), Dominant Firm Quantity (Qd_Sc3), Fringe Profit (πf_Sc3), Dominant Firm Profit (πd_Sc3), Consumer Surplus (CS_Sc1), Firm Target Information Quantity (N_Sc3), Firm Actual Collected Information (Nact_Sc3), Delta Price (ΔP_Sc3), Delta Quantity (ΔQ_Sc3), Delta Fringe Firm Quantity (ΔQf_Sc3), Delta Dominant Firm Quantity (ΔQd_Sc3), Delta Fringe Profit (Δπf_Sc3), Delta Dominant Firm Profit (Δπd_Sc3), Delta Consumer Surplus (ΔCS_Sc3), Total Surplus (TS_Sc3)
4 (17)	Price (P_Sc4), Quantity (Q_Sc4), Fringe Firm Quantity (Qf_Sc4), Dominant Firm Quantity (Qd_Sc4), Fringe Profit (πf_Sc4), Dominant Firm Profit (πd_Sc4), Consumer Surplus (CS_Sc1), Firm Target Information Quantity (N_Sc4), Firm Actual Collected Information (Nact_Sc4), Delta Price (ΔP_Sc4), Delta Quantity (ΔQ_Sc4), Delta Fringe Firm Quantity (ΔQf_Sc4), Delta Dominant Firm Quantity (ΔQd_Sc4), Delta Fringe Profit (Δπf_Sc4), Delta Dominant Firm Profit (Δπd_Sc4), Delta Consumer Surplus (ΔCS_Sc4), Total Surplus (TS_Sc4)
Fringe firm optimum (18)	Fringe Optimum Scenario # (Fringe_o), Price (P_o), Quantity (Q_o), Fringe Firm Quantity (Qf_o), Dominant Firm Quantity (Qd_o), Fringe Profit (πf_o), Dominant Firm Profit (πd_o), Consumer Surplus (CS_o), Firm Target Information Quantity (N_o), Firm Actual Collected Information (Nact_O), Delta Price (ΔP_o), Delta Quantity (ΔQ_o), Delta Fringe Firm Quantity (ΔQf_o), Delta Dominant Firm Quantity (ΔQd_o), Delta Fringe Profit (Δπf_o), Delta Dominant Firm Profit (Δπd_o), Delta Consumer Surplus (ΔCS_o), Total Surplus (TS_o)

Analysis of Table 6-5 shows that no policy is dominant, or even generally prevalent across the many outputs. However, a number of interesting results appear:

- The introduction of RFID, under any policy regime, generally increases dominant firm profit (π_d), and quantity (Q). This can be seen in the first set of output rankings, for π_d, where Pre-Regulation profit is ranked last, in more than 80% (412/504) of all simulation cases. Blocker tag and no regulation policies are the most likely to result in maximum dominant firm profit, but there is no single dominant strategy.
- The blocker tag is a nearly dominant policy for maximizing information collection, ranking first in 472/504 simulation cases. Pre-regulation always ranks last because there is no information collected at that point.
- Fringe firm profits are nearly dominated by the pre-RFID case, which is the best choice in 248/336 simulations. Second best is evenly distributed across almost all policy choices. In the rare cases where fringe firm profit increases, it is most common under no regulation or industry Self-Regulation policies.
- Total quantity increases in all simulations, for at least one policy, and almost always for all policies, as shown by Pre-Regulation resulting in the lowest quantity in 473/504 simulation cases. The quantity maximizing choice is distributed across all four policies, although No Regulation (151) is most frequently the leader.
- Consumer surplus decreases, relative to Pre-Regulation in more than half of all simulations run (272/504). In cases where it increases, the largest increase occurs most often when there is no regulation (173/504).
- Total surplus is maximized under the No Regulation policy in about 50% of cases, but no policy is dominant, or dominated by any other.

Table 6-5: Rank ordering of policies for key outputs in all simulations; Fringe optimum strategy

Parameter	Rank	Blocker Tag	Self-regulation	Bill of Rights	No Regulation	Pre-Regulation
π_d	1	192	21	45	204	42
	2	67	228	93	87	30
	3	160	172	107	52	12
	4	75	72	250	99	8
	5	10	11	9	62	412
π_f	1	4	25	6	53	248
	2	55	57	94	96	34
	3	85	75	77	68	31
	4	84	94	75	68	15
	5	108	85	84	51	8
Nact	1	472	29	38	20	0
	2	17	158	292	32	0
	3	9	282	79	121	0
	4	6	35	95	331	0
	5	0	0	0	0	504
Q	1	157	58	37	252	4
	2	53	300	64	82	6
	3	211	101	90	91	12
	4	75	35	312	68	9
	5	8	10	1	11	473
Consumer Surplus	1	25	22	13	173	272
	2	52	167	47	186	56
	3	81	192	116	43	68
	4	78	82	255	44	45
	5	268	41	73	58	63
Total Surplus	1	73	35	119	254	23
	2	57	280	55	44	68
	3	118	82	195	47	62
	4	171	79	109	71	74
	5	85	28	26	88	277

One final and important observation is that a more detailed and thorough analysis is necessary, in order to understand the sensitivity of each output to market structure, policies, and the distribution of individual characteristics.

6.2. Parametric Sensitivity

Detailed statistical analysis was performed using two analysis packages: R for automated analysis of the many different parametric outputs, and JMP to create the graphical figures shown below. (R is an open source software package that is designed to be compatible with the widely used S and S-plus. See www.r-project.org for details. JMP is a GUI-based package developed by the SAS Institute to assist in data visualization. See www.jmp.com for details.) Once the entire set of simulations was completed in Excel, the data were organized into a large table, and exported into R. Within R, a basic analysis of variance (ANOVA) was performed, looking at a variety of models, in order to determine the basic significance of each independent parameter, and to examine the possibility of parametric interactions. Significance was determined using the F-statistic reported for each component of the ANOVA, for each output model. After this initial exploration did not identify significant higher order or interaction terms, a straightforward linear model, determined using the ordinary least squares (OLS) method and containing each parameter, was chosen for detailed analysis of parametric significance. In this analysis, most of the independent variables are treated as continuous, but the choices of both firm economic interaction model and policy are categorical, and are treated as such. For each output, j, listed in Table 6-4, the model has the structure:

$$\begin{aligned} Output_j = {} & \alpha_j + \beta_{1,j} R + \beta_{2,j} D_s + \beta_{3,j} S_p + \beta_{4,j} I + \beta_{5,j} (\%N_L = 0) + \beta_{6,j} (\%N_L = \max) \\ & + \beta_{7,j} \sigma_I + \beta_{8,j} \sigma_{NL} + \beta_{9,j} DF + \beta_{10,j} Mono + \beta_{11,j} BofR + \beta_{12,j} BT + \beta_{13,j} ISR \end{aligned} \quad (1)$$

In equation (1), each β_j is a parameter estimate derived through the linear regression. To account for the categorical nature of the economic model and policy choices, *DF* and *Mono* are dummy variables representing the use of the dominant-fringe or monopoly firm models, respectively, and *BofR*, *BT*, and *ISR* are dummy variables respectively indicating the RFID

Bill of Rights Policy, the Blocker Tag Policy, and the Industry Self-regulation policy. Each of the dummy variables takes on a value of 0 when it is not chosen and a value of 1 when it is chosen. These estimates are relative to a baseline case, which contains the Cournot model of interaction and the no regulation policy option. Those two levels are absorbed into the intercept (α_j), so each of the β_j coefficients represents the relative effect of that choice as compared to the baseline case.

As is typical with OLS models, the resultant model reports the parameter estimates, associated standard errors, the t-statistic resulting from these values (simply the parameter estimate divided by the standard error), and the probability (p-value) associated with the calculated t-statistic. A sample report containing one model and associated diagnostics (standard error, t-statistic, and probability) is included in Appendix B. Parameter estimates for each significant predictor of output, and for the fringe optimum strategic interaction model, are shown in Table 6-6. The remaining parameter estimates are shown in tables in Appendix B. In all cases a conservative p-value of .01 was used as a threshold for significance. A blank field indicates that the parameter is not significant in the final fitted model. Also shown in each table is the adjusted R^2 coefficient for each model, which is useful for determining the overall correlation between each output and the set of independent parameters in the model.[17]

[17] The adjusted R^2, denoted here as $\underline{R}^2$, is useful as a guard against adding excess parameters into the model. It penalizes excess parameters, as opposed to the non-adjusted R^2, and is calculated by:

$$\underline{R}^2 = 1 - \frac{SS_E/(n-p)}{SS_y/(n-1)} = 1 - \frac{n-1}{n-p}\left(1-R^2\right)$$ where n = number of observations, p = number of independent model parameters, SS_E is the sum of squares of the residuals, and SS_y is the total sum of squares.

Table 6-6: Estimates for significant parameters for Fringe optimum strategy

Parameter estimate	Price	Quantity	Fringe Quantity	Dominant Quantity	Fringe Profit	Dominant profit	Consumer Surplus	Target Info.	Actual Info.
$\underline{R}^2$	0.86	0.87	0.50	0.76	0.85	0.86	0.83	0.64	0.76
R	7.04	-0.52	1.52	-1.84	98.99	-104.50	236.80	-2.66	-1.29
Ds	-8.25	3.77		4.92	-68.09	224.62	76.49	1.55	0.87
S_p	-6.80	2.54	-4.72	6.49	-75.25	481.21	-405.25	2.29	0.67
I	0.54	0.40	0.14	0.26	10.03	25.56	13.81	0.01	0.01
%NL=0	-5.49	-4.95	-2.95		103.58	485.44		5.35	1.03
%NL=max	21.59	-9.00		-8.81	361.46		593.40	-5.57	-6.93
σ_I						4.37	9.25		0.01
σ_{NL}	1.35	-2.44	-1.66	-0.75	30.02			-0.27	-0.72
BoR	2.67	-1.46	-1.03	-0.77		-80.20	-40.68	0.35	0.17
BT	1.46	-0.58			-18.39		-72.17	1.38	0.69
ISR									0.11
DF		-1.20		-1.24		94.48	-109.02	0.83	0.64
Monopoly	16.36					519.23	-616.34	0.41	0.68

Table 6-6 shows that each output in the fringe optimum scenario is well predicted by a combination of parameters. For example, Quantity can be predicted by the linear formula: Quantity = $-0.52R + 3.77D_s + 2.54S_p + 0.4I - 4.95(\%N_L=0) - 9.0(\%N_L=max) - 2.44\sigma_{NL} - 1.46BoR - 0.58BT - 1.20DF$, with an adjusted R^2 of 0.87. For all outputs, the adjusted R^2 is at least 0.5, meaning that each model explains at least half of the variance, and most explain more than 75% of the output variance.[18]

Results from the regressions shown in Table 6-6 and in Appendix B produce some expected results. For example, the Monopoly model produces a substantially higher equilibrium price and profit for the dominant (monopoly in this case) firm, and reduced consumer surplus. Some other results from Table 6-6 are also worth highlighting:

- Some policies have noticeable effects across many outputs. The Blocker Tag (BT) policy is significant across a number of outcomes, with a large positive effect on information collection, and smaller but significant effects on price,

[18] Since these are simulation results, it should be possible to identify a more sophisticated functional form that explains all of the variance. However, that was not examined in detail.

quantity, and consumer surplus. The Bill of Rights (BoR) policy also has small but significant effects, most noticeably in reducing dominant firm profits. The Industry Self Regulation (ISR) policy is not significant across any output with the exception of Nact. This means that, as modeled, it does not result in significant differences from the No Regulation policy.

- The market structure (Monopoly, Cournot, or Dominant-Fringe) has statistically significant effects for most of the outputs. Other market parameters, such as Income, and Income-N_L correlation are also significant for most outputs.
- Individual heterogeneity affects all outputs. This is seen through σ_{NL}, σ_I, %NL=0, and %NL=max, several of which are significant for all outputs.

However, it can also be seen that many outputs are affected by most, if not all parameters, and it is difficult to draw easy conclusions from these models, without additional and more sophisticated analysis. This analysis was performed through the development of logistic regression models to predict several key outcomes: the probability of each fringe optimum strategy (a choice between strategy 2, 3, or 4), and the probability that a given policy will result in the top-ranked outcome (as shown in Table 6-5) for Total Surplus, Consumer Surplus, and Information Collected.

Determination of the fringe firm optimum choice assumes that the fringe firm operates as a profit-maximizing firm, and that it is able to acquire complete information about the effect of each option it faces. In this case, the fringe firm is then able to pick a

strategy that maximizes its profit.[19] This choice is a discrete dependent variable, so it cannot be modeled by the linear regression techniques used for other outputs. A simple analysis of the fringe firm's strategic choices, shown in Figure 6-1 below, indicates that policy has a substantial impact on the fringe optimum choice.

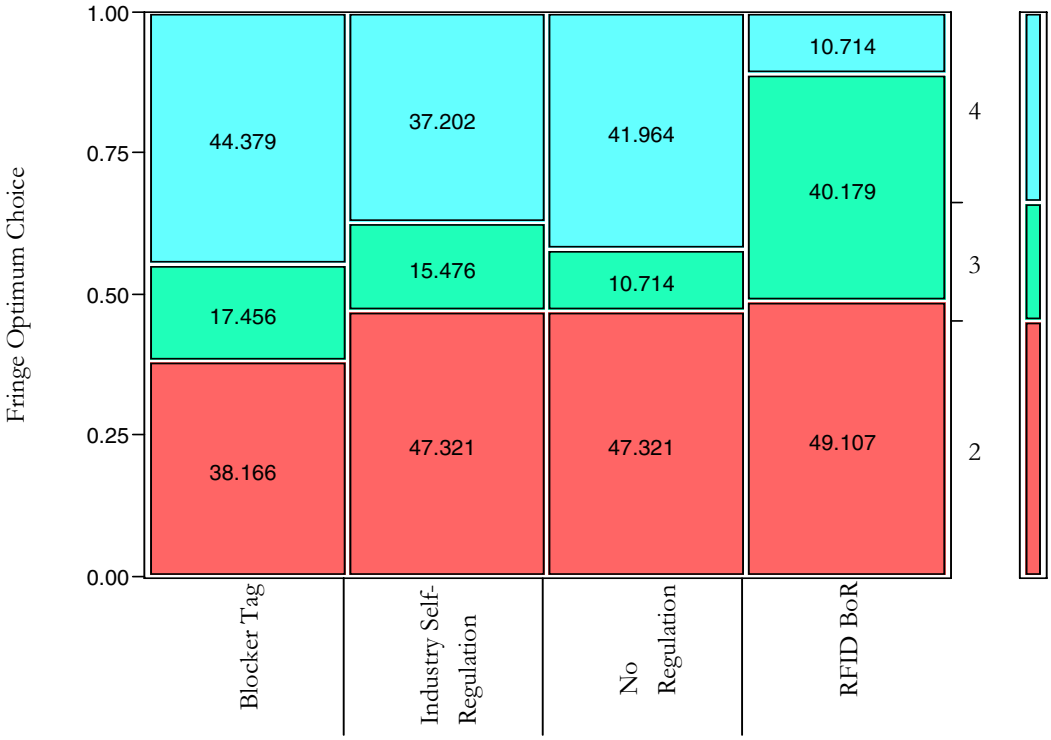


Figure 6-1: Contingency analysis of fringe optimum choice by policy.
Strategy choices are shown in the color-coded legend at the right; the numbers in each cell are percent of total, per policy. For example, with the Blocker Tag policy, the fringe firm chose strategy 2 in 38.166% of scenarios.

Figure 6-1 is a simple graphical representation of a percentage tabulation of the strategic choice made by the fringe firm, for each policy, and over all simulation runs. This analysis shows that the RFID Bill of Rights (labeled as RFID BoR in the figure) policy is likely to result in the fringe not using RFID or matching price in 49% of scenarios, and matching price but still not using RFID in 40% of scenarios. As a result, the fringe firm

[19] Note that this fringe choice suggests the use of a game-theoretic model as a method for analysis. That technique was considered here, but ultimately the microeconomic model appeared to offer greater richness of analysis.

adopts RFID in approximately 11% of all scenarios, compared with at least 37% for other policies. The other apparent differences in outcomes between policies are smaller, and require a more detailed investigation to assess their significance.

A logistic regression model that accounts for the three-level choice of fringe optimum takes the form:

$$\log it(p_j) = \log\left(\frac{p_j}{1-p_j}\right) = \alpha_j + \beta_{1,j}R + \beta_{2,j}D_s + \beta_{3,j}S_p + \beta_{4,j}I + \beta_{5,j}(\%N_L = 0) + \beta_{6,j}(\%N_L = \max)$$
$$+ \beta_{7,j}\sigma_I + \beta_{8,j}\sigma_{NL} + \beta_{9,j}DF + \beta_{10,j}Mono + \beta_{11,j}BofR + \beta_{12,j}BT + \beta_{13,j}ISR \qquad (2)$$

In equation (2), p_j is the probability that the fringe firm will choose either scenario 2 (j=1) or scenario 3 (j=2) as the profit maximizing scenario. The probability of scenario 4 is then simply the remainder. The term log (p/(1-p)) is the log of the odds ratio (sometimes called log odds), and each β_j has a multiplicative effect on the odds ratio. Errors are binomially distributed, and parametric significance can be determined according to the Wald chi-square test, which evaluates the probability of the (estimate/SE)^2 against the chi-square distribution. Table 6-7 shows the parameters that are significant predictors of the log odds of the firm optimum choice, again using a p-value of .01 as the threshold for statistical significance.

Table 6-7: Log odds of significant parameters in fringe optimum strategy

Parameter estimate	Scenario 2	Scenario 3
Intercept	-3.04	4.82
R		0.78
Ds		-3.62
S_p	5.10	1.78
I		-0.03
%NL=0		-0.06
%NL=max	0.05	0.06
σ_I	-0.08	
σ_{NL}	2.17	-0.72
ISR		-.46
BT	-0.77	-0.55
No Regulation		-1.07
Cournot		-0.40

The parameters, in the second and third columns of Table 6-7 are, respectively, estimates of the log odds of choosing strategy 2 compared to strategy 4, and choosing strategy 3 over strategy 4. The categorical nature of the policy and economic model choices means that one of the four policies and one of the two models are each absorbed into the intercept term. In these results, the Bill of Rights policy and the dominant-fringe economic model are embedded in the intercept.

As the tabulation in Figure 6-1 shows, among policies, only the Blocker Tag is a significant contributor to the likelihood of the fringe firm opting for strategy 2, whereas all policies have significant effects on the likelihood of the fringe opting for strategy 3. The primary controls over whether the fringe opts for strategy 2 are individual heterogeneity, and the ability to price discriminate. The negative log odds for each shown policy is equivalent to a significant positive affect of the Bill of Rights policy on the likelihood of a fringe firm opting for strategy 3, as compared to all other policies. This, too, is a confirmation of the tabular results in Figure 6-1. σ_{NL}, S_p, and %NL=max also have a significant role across all three choices, and other parameters significantly affect the choice between strategy 3 and strategy 4. That is, a relatively small set of factors significantly affect the first decision by the fringe, which is whether it should match the new dominant firm price; but more factors are involved in the fringe decision to use RFID, once it has matched price.

Figure 6-2 provides an example of how policy, σ_{NL}, and S_p, interact in the fringe firm's decision. The figure is a 3x3 matrix of 9 graphs, which represent all of the possible interactions between the three inputs (policy, σ_{NL}, and $S_{p)}$ and the probability that the fringe will choose strategy 2, 3, or 4. The solid line represents the relationship between the input and the probability of that fringe choice, given the other parameters are held constant. The red dotted lines and red values at the bottom are the current plot choices, and the red value

at the left is the modeled probability of that outcome. For example, in Figure 6-2 where the policy is the Blocker Tag, σ_{NL} = 1.5, and S_p = 0.25, the most likely fringe optimum is strategy 4 at 63%. However, by changing only the policy, to RFID Bill of Rights, strategy 2 becomes the likely best choice, at 61%.

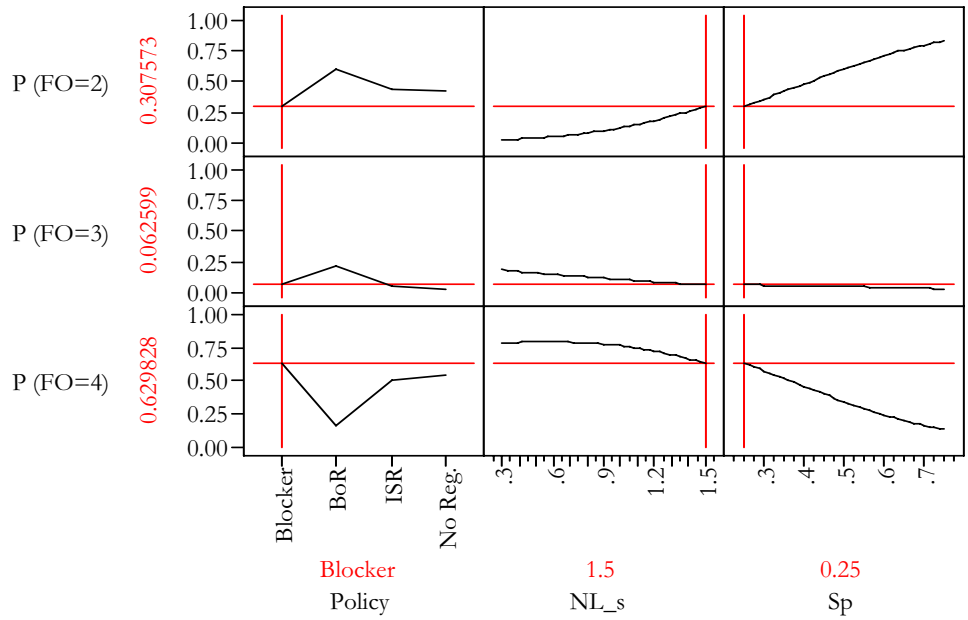


Figure 6-2: Example of parametric interactions in fringe optimum strategy. Independent inputs are shown in red at the bottom and probabilities of each outcome are shown in red on the left. (FO = Fringe optimum choice)

The probability of a policy resulting in the highest ranked Total Surplus, highest ranked Consumer Surplus or highest ranked Information Collected is determined with a similar logistic model that is extended to include interactions between each policy and each market model, between policy and each other covariate, and between economic model and covariate. A generic form of the model is shown here:

$$\log it(p_j) = \alpha_j + \beta_{z,j}Z + \beta_{x,j}X + \beta_{m,j}M + \beta_{mx,j}M \bullet X + \beta_{mz,j}M \bullet Z + \beta_{xz,j}X \bullet Z \qquad (3)$$

In equation (3), p_j is the probability that, for output j, a set of parameters will result in an output that is ranked highest. Since the rankings are for the set of policies, with all other parameters held constant, p_j is the probability that any given policy will produce the highest

rank in a scenario. Z is a vector of all parameters (eight) except for the policy and economic model choices, X is a vector of dummy variables selecting each of the five policy choices, and M is a vector of dummy variables selecting each of the three economic market models. M • X is a vector of all possible interactions between each policy choice and each market model, X • Z is the vector of interactions between policy and other model parameters, and M • Z is a similar vector for economic market model and other model parameters. The *j* subscript represents each of the three outputs (total surplus, consumer surplus, and actual information collected) that are being modeled. Each β is a vector containing the estimated effect of each parameter on the log odds of the output, so $\beta_{x,j}$ contains 4 unique estimates for each output, representing the relative effect of each policy on the j^{th} output, as compared to a dropped baseline policy. The other β parameters are similar, differing only in the length of the vector. In all subsequent logistic models, the whole model described by equation (3) was tested, and a final model created by removing non-significant parameters. The exception is for parameters without a statistically significant independent linear component, but with a significant contribution through interaction with another parameter.

The data used in this analysis is based on the results reported in Table 6-5. The distribution of highest policies for each output (consumer surplus, total surplus, and information collected) is graphed, by policy, in Figure 6-3, which shows that consumer surplus is highest prior to adopting RFID in slightly more than 50% of all scenarios, total surplus is maximized by the no regulation policy in about 50% of cases, and the blocker tag maximizes information collected more than 90% of the time.

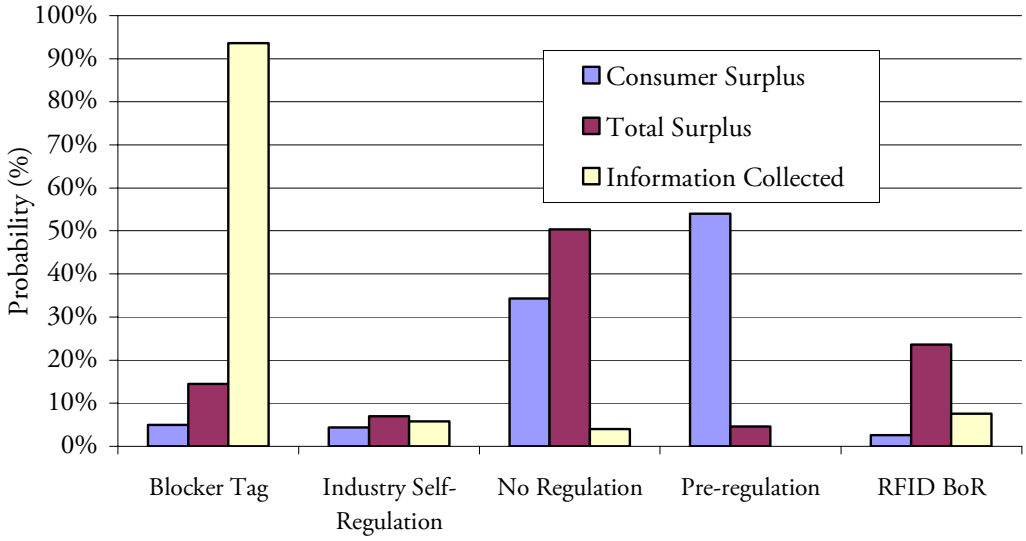


Figure 6-3: Probability of each policy producing the highest ranked output

Table 6-8 shows the results of fitting a logistic model, specified in equation (3), to the consumer surplus ranking data shown in Figure 6-3. The model, while not perfect, has substantial explanatory power. Actual parameter estimates for all significant parameters are shown in Table 6-9, below. Two tests of significance, Wald Probability and Maximum Likelihood Ratio Probability are reported. The former can be used to test the estimates for each parameter, however, when those values are large, estimated Standard Errors are also large, and the estimated probability is small. In this case, it is better to use the Maximum Likelihood Ratio, which tests the final model with, and without each parameter. (Menard 2002) Thus, it can only be used for significance, and not for parameter estimates for each level of a nominal variable.

Table 6-8: Summary of logistic model predicting highest ranked consumer surplus

Model	Log Likelihood	DF	ChiSquare	Prob>ChiSq
Difference	668.0380	51	1336.076	<.0001
Full	594.3612			
Reduced	1262.3992			
RSquare (U)		0.5292		
Observations (or Sum Wgts)		2520		

Table 6-9: Parameter estimates for model predicting highest rank consumer surplus

Term	Estimate	Std Error	Prob>ChiSq	Likelihood Ratio Prob
Intercept	5.02	16.83	0.7654	
Econ Model[Cournot]	-2.29	5.56	0.6798	<.0001
Econ Model[DF]	-1.70	5.56	0.7603	
Policy[Blocker Tag]	2.71	13.83	0.8446	
Policy[No regulati]	-4.20	6.19	0.4977	<.0001
Policy[Pre-regulat]	-5.56	6.19	0.3689	
Policy[RFID BoR]	3.77	13.13	0.7739	
NL s	-1.24	10.58	0.9070	.4433
Income mean	0.01	0.01	0.0908	.0788
% NL = N0	-3.05	1.40	0.0289	.0206
% NL = 0	-2.88	1.39	0.0382	.0280
Income-NL correlation	-1.02	0.24	<.0001	<.0001
Dw (quadratic cost savings)	0.59	0.69	0.3943	.3910
Price Discrimination scaling	2.27	0.57	<.0001	<.0001
Policy[Blocker Tag]*(NL s)	1.52	10.59	0.8859	
Policy[No regulati]*(NL s)	1.61	10.58	0.8790	.0105
Policy[Pre-regulat]*(NL s)	0.97	10.58	0.9273	
Policy[RFID BoR]*(NL s)	2.96	10.61	0.7803	
Policy[Blocker Tag]*(Income mean)	-0.02	0.01	0.1089	
Policy[No regulati]*(Income mean)	-0.03	0.01	<.0001	<.0001
Policy[Pre-regulat]*(Income mean)	0.00	0.01	0.8622	
Policy[RFID BoR]*(Income mean)	0.05	0.02	0.0099	
Policy[Blocker Tag]*(% NL = N0)	-4.58	2.72	0.0917	
Policy[No regulati]*(% NL = N0)	8.22	1.82	<.0001	<.0001
Policy[Pre-regulat]*(% NL = N0)	0.52	1.78	0.7715	
Policy[RFID BoR]*(% NL = N0)	-6.02	4.40	0.1713	
Policy[Blocker Tag]*(% NL = 0)	-0.72	2.77	0.7946	
Policy[No regulati]*(% NL = 0)	5.14	1.79	0.0041	.0414
Policy[Pre-regulat]*(% NL = 0)	2.11	1.77	0.2334	
Policy[RFID BoR]*(% NL = 0)	-8.22	4.34	0.0582	
Policy[Blocker Tag]*(Income-NL correlation)	-2.32	0.55	<.0001	
Policy[No regulati]]*(Income-NL correlation)	1.68	0.30	<.0001	<.0001
Policy[Pre-regulat]]*(Income-NL correlation)	1.34	0.30	<.0001	
Policy[RFID BoR]]*(Income-NL correlation)	-1.25	0.61	0.0382	
Policy[Blocker Tag]*(Dw (quadratic cost savings))	-0.99	1.45	0.4937	
Policy[No regulati] *(Dw (quadratic cost savings))	-4.44	0.94	<.0001	<.0001
Policy[Pre-regulat]*(Dw (quadratic cost savings))	3.01	0.94	0.0014	
Policy[RFID BoR]*(Dw (quadratic cost savings))	3.01	1.91	0.1164	
Policy[Blocker Tag]*(Price Discrimination scaling)	-0.04	0.99	0.9642	
Policy[No regulati]*(Price Discrimination scaling)	3.61	0.72	<.0001	<.0001
Policy[Pre-regulat]*(Price Discrimination scaling)	-8.84	0.71	<.0001	
Policy[RFID BoR]*(Price Discrimination scaling)	3.53	1.78	0.0478	
Econ Model[Cournot]* (Income-NL correlation)	0.57	0.22	0.0082	.0212
Econ Model[DF]*(Income-NL correlation)	-0.08	0.21	0.7125	
Econ Model[Cournot]*Policy[Blocker Tag]	-2.86	13.56	0.8326	
Econ Model[Cournot]*Policy[No regulati]	2.51	5.56	0.6515	
Econ Model[Cournot]*Policy[Pre-regulat]	2.92	5.56	0.5996	
Econ Model[Cournot]*Policy[RFID BoR]	-1.55	12.83	0.9039	<.0001
Econ Model[DF]*Policy[Blocker Tag]	-0.10	13.56	0.9943	
Econ Model[DF]*Policy[No regulati]	1.71	5.56	0.7577	
Econ Model[DF]*Policy[Pre-regulat]	1.68	5.56	0.7623	
Econ Model[DF]*Policy[RFID BoR]	-1.29	12.83	0.9202	

Table 6-9 shows the substantial contribution of interactions to the final model ranking consumer surplus. Especially significant are the interactions between policy choice and market model, including both the strategic interaction choice and price discrimination, and between policy choice and individual heterogeneity.

Table 6-10 shows model summary statistics for a logistic model, specified as in equation (3), and describing the probability of a scenario producing the highest ranked total surplus. Again, the model is significant, and explains a substantial portion of the total variance. Table 6-12 contains the estimates for all significant parameters in this model. As with Table 6-9, two tests of significance, Wald Probability and Maximum Likelihood Ratio Probability are reported.

Table 6-11 shows model summary statistics for a logistic model, specified as in equation (3), and describing the probability of a scenario producing the highest ranked total information collected. In this case, the model is very significant, and explains almost 80% of the total variance.

Table 6-13 contains the estimates for all significant parameters in this model. As previously, both Wald Probability and Maximum Likelihood Ratio Probability are reported. Table 6-12 and Table 6-13 also show the importance of interactions between policies and market structure, and policies and individual heterogeneity, in the final models ranking total surplus and total information collected.

Table 6-10: Summary of logistic model predicting highest ranked total surplus

Model	Log Likelihood	DF	ChiSquare	Prob>ChiSq
Difference	524.2726	43	1048.545	<.0001
Full	736.7415			
Reduced	1261.0141			
RSquare (U)		0.4158		
Observations (or Sum Wgts)		2520		

Table 6-11: Parameter estimates for model predicting highest rank total surplus

Term	Estimate	Std Error	Prob>ChiSq	Likelihood Ratio Prob
Intercept	3.71	1.38	0.0072	
Econ Model[Cournot]	-0.65	1.32	0.6203	.0345
Econ Model[DF]	-0.47	1.32	0.7214	
Policy[Blocker Tag]	0.12	1.35	0.9322	
Policy[No regulati]	-3.52	1.33	0.0082	<.0001
Policy[Pre-regulat]	2.47	1.52	0.1046	
Policy[RFID BoR]	0.86	5.24	0.8701	
% NL = N0	-2.74	0.97	0.0049	.0037
% NL = 0	-1.58	1.01	0.1176	.1114
Income-NL correlation	-1.02	0.29	0.0005	<.0001
Dw (quadratic cost savings)	0.91	0.52	0.0796	.0779
Price Discrimination scaling	0.09	0.31	0.7760	.7758
Econ Model[Cournot]*Policy[Blocker Tag]	1.73	1.34	0.1991	
Econ Model[Cournot]*Policy[No regulati]	1.65	1.32	0.2126	
Econ Model[Cournot]*Policy[Pre-regulat]	0.32	1.34	0.8134	
Econ Model[Cournot]*Policy[RFID BoR]	-3.74	5.24	0.4753	<.0001
Econ Model[DF]*Policy[Blocker Tag]	2.20	1.35	0.1039	
Econ Model[DF]*Policy[No regulati]	0.05	1.32	0.9703	
Econ Model[DF]*Policy[Pre-regulat]	1.21	1.35	0.3707	
Econ Model[DF]*Policy[RFID BoR]	-2.29	5.24	0.6617	
Econ Model[Cournot]*(% NL = 0)	-1.29	1.02	0.2030	.0082
Econ Model[DF]*(% NL = 0)	-2.63	1.04	0.0112	
Econ Model[Cournot]*(Income-NL correlation)	-0.24	0.21	0.2603	.0142
Econ Model[DF]*(Income-NL correlation)	-0.51	0.21	0.0153	
Policy[Blocker Tag]*(% NL = N0)	-2.55	1.74	0.1420	
Policy[No regulati]*(% NL = N0)	9.49	1.40	<.0001	<.0001
Policy[Pre-regulat]*(% NL = N0)	-8.30	2.77	0.0028	
Policy[RFID BoR]*(% NL = N0)	-2.81	1.48	0.0584	
Policy[Blocker Tag]*(% NL = 0)	-7.96	2.00	<.0001	
Policy[No regulati]*(% NL = 0)	3.62	1.37	0.0083	<.0001
Policy[Pre-regulat]*(% NL = 0)	-5.11	2.95	0.0830	
Policy[RFID BoR]*(% NL = 0)	4.29	1.61	0.0077	
Policy[Blocker Tag]*(Income-NL correlation)	-1.40	0.46	0.0023	
Policy[No regulati]*(Income-NL correlation)	2.52	0.34	<.0001	<.0001
Policy[Pre-regulat]*(Income-NL correlation)	-3.78	1.07	0.0004	
Policy[RFID BoR]*(Income-NL correlation)	1.33	0.37	0.0004	
Policy[Blocker Tag]*(Dw (quadratic cost savings))	1.31	0.99	0.1864	
Policy[No regulati]*(Dw (quadratic cost savings))	-4.46	0.77	<.0001	<.0001
Policy[Pre-regulat]*(Dw (quadratic cost savings))	-0.52	1.35	0.6993	
Policy[RFID BoR]*(Dw (quadratic cost savings))	1.11	0.84	0.1852	
Policy[Blocker Tag]*(Price Discrimination scaling)	0.22	0.59	0.7077	
Policy[No regulati]*(Price Discrimination scaling)	0.81	0.45	0.0731	.0015
Policy[Pre-regulat]*(Price Discrimination scaling)	1.56	0.83	0.0617	
Policy[RFID BoR]*(Price Discrimination scaling)	-1.56	0.50	0.0020	

Table 6-12: Summary of logistic model predicting highest ranked information collected

Model	Log Likelihood	DF	ChiSquare	Prob>ChiSq
Difference	945.0212	39	1890.042	0.0000
Full	245.1600			
Reduced	1190.1812			
RSquare (U)		0.7940		
Observations (or Sum Wgts)		2016		

Table 6-13: Parameter estimates for model predicting highest rank information collected

Term	Estimate	Std Error	Prob>ChiSq	Likelihood Ratio Prob
Intercept	112.19	399.17	0.7787	
Econ Model[Cournot]	-23.38	91.78	0.7989	.3374
Econ Model[DF]	-22.61	91.78	0.8054	
Policy[Blocker Tag]	-106.46	354.92	0.7642	
Policy[No regulati]	38.62	128.52	0.7638	<.0001
Policy[RFID BoR]	36.37	125.74	0.7724	
NL s	-0.21	0.29	0.4724	.4702
Income mean	-0.21	1.01	0.8338	.0628
% NL = 0	-194.44	690.64	0.7783	<.0001
Income-NL correlation	45.11	164.87	0.7844	<.0001
Dw (quadratic cost savings)	-19.58	106.10	0.8536	.0566
Price Discrimination scaling	-56.23	229.34	0.8063	<.0001
Econ Model[Cournot]*Policy[Blocker Tag]	102.64	354.92	0.7724	
Econ Model[Cournot]*Policy[No regulati]	-36.62	128.52	0.7757	
Econ Model[Cournot]*Policy[RFID BoR]	-35.64	125.74	0.7768	<.0001
Econ Model[DF]*Policy[Blocker Tag]	97.77	354.92	0.7829	
Econ Model[DF]*Policy[No regulati]	-33.67	128.52	0.7933	
Econ Model[DF]*Policy[RFID BoR]	-34.86	125.74	0.7816	
Econ Model[Cournot]*(Income mean)	0.23	1.01	0.8175	.0211
Econ Model[DF]*(Income mean)	0.20	1.01	0.8411	
Econ Model[Cournot]*(% NL = 0)	191.49	690.64	0.7816	<.0001
Econ Model[DF]*(% NL = 0)	184.45	690.64	0.7894	
Econ Model[Cournot]*(Income-NL correlation)	-46.27	164.87	0.7790	<.0001
Econ Model[DF]*(Income-NL correlation)	-43.34	164.87	0.7927	
Econ Model[Cournot]*(Dw (quadratic cost savings))	20.73	106.10	0.8451	.0071
Econ Model[DF]*(Dw (quadratic cost savings))	14.55	106.10	0.8909	
Econ Model[Cournot]*(Price Discrimination scaling)	59.43	229.35	0.7955	<.0001
Econ Model[DF]*(Price Discrimination scaling factor)	57.50	229.35	0.8020	
Policy[Blocker Tag]*(Income mean)	-0.04	0.01	0.0010	
Policy[No regulati]*(Income mean)	0.01	0.01	0.5252	.0072
Policy[RFID BoR]*(Income mean)	0.02	0.01	0.0869	
Policy[Blocker Tag]*(% NL = 0)	3.46	1.94	0.0738	
Policy[No regulati]*(% NL = 0)	-6.78	2.84	0.0169	.0213
Policy[RFID BoR]*(% NL = 0)	4.08	2.01	0.0419	
Policy[Blocker Tag]*(Dw (quadratic cost savings))	-2.95	1.36	0.0300	
Policy[No regulati]*(Dw (quadratic cost savings))	-0.66	1.75	0.7080	.0083
Policy[RFID BoR]*(Dw (quadratic cost savings))	4.14	1.43	0.0037	
Policy[Blocker Tag]*(Price Discrimination scaling)	-6.69	1.05	<.0001	
Policy[No regulati]*(Price Discrimination scaling)	2.93	1.70	0.0847	<.0001
Policy[RFID BoR]*(Price Discrimination scaling)	2.15	1.11	0.0530	

The models reported in Table 6-9, Table 6-11 and Table 6-13 can be used to predict the conditions under which each policy is most likely to result in the highest rank consumer surplus, total surplus, and information collected, respectively. This is done by creating a

baseline scenario of parameters and a probability prediction for each policy. The policy with the greatest probability for the baseline set of parameters is assigned to be the policy with the maximum output (consumer surplus, total surplus or information collected) for that scenario. The baseline parameter scenario for each output is then varied, and transition points to other policy regimes can be identified.

For example, using maximum consumer surplus as the output of interest, five sets of parameters, and the resulting probability for each policy, are shown in Table 6-14. In the first case, scenario 1, it can be seen that the No Regulation policy, with a predicted likelihood of 55%, is the most likely to produce the maximum consumer surplus. However, in scenario 2, which differs only by allowing a high degree of price discrimination, as opposed to the low level in scenario 1, Pre-Regulation becomes the most likely policy to maximize consumer surplus, with an 82% probability. The other three scenarios shown in Table 6-14 demonstrate parameter sets that result in each of the other policies being the most likely to maximize consumer surplus. Further analysis of similar variations allows transitions to each of the policies to be identified:

- Pre-Regulation is most likely to maximize consumer surplus in all market models when price discrimination is high. As price discrimination drops, Pre-Regulation continues to be the best choice, as long as the Income-N_L correlation is low, or negative, until price discrimination becomes quite low.
- No Regulation becomes most likely to maximize consumer surplus when there is low price discrimination. In the Cournot or Dominant-Fringe market models, the likelihood of No Regulation maximizing consumer surplus increases as the population becomes more homogeneous, especially as $\%N_L=0$ declines.

- The RFID Bill of Rights policy is most likely to maximize consumer surplus in the Cournot and Dominant-Fringe market models, when price discrimination is low, and $\%N_L=0$ or $\%N_L=N0$ is high.

Table 6-14: Scenarios where each policy maximizes consumer surplus

Parameter	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Economic market model	Cournot	Cournot	Cournot	Cournot	Dominant-Fringe
N_L σ	0.3	0.3	.3	1.5	1.5
Mean Income	100	100	100	150	100
$\%N_L=N0$	0	0	30%	30%	30%
$\%N_L=0$	0	0	30%	30%	15%
Income-N_L correlation	0	0	0	0.75	0.75
D_w (cost savings factor)	0.3	0.3	0.3	0.6	0.6
S_p (price discrimination factor)	0.3	.75	0.3	0.3	0.25
Pre-regulation	18.8%	**82.0%**	39.0%	7.8%	22.1%
No Regulation	**55%**	8.0%	11.4%	25.5%	27.1%
RFID Bill of Rights	3.3%	0.2%	**93.4%**	10.7%	27.4%
Blocker Tag	1.5%	0.5%	30.2%	**81.3%**	8.9%
Self-regulation	0.0%	0.0%	0.0%	8.6%	**31.7%**

- The Blocker Tag maximizes consumer surplus in the Cournot market model, when the population is very heterogeneous (N_L σ, $\%N_L=0$, $\%N_L=N0$ are all high), Income and correlation between Income and N_L are high, price savings is high, and price discrimination is low.
- Self Regulation maximizes consumer surplus in the Dominant-Fringe model, with low Income and price discrimination, high Income-N_L correlation, $\%N_L=N0$ and N_L σ, and intermediate $\%N_L=0$.

A similar analysis was performed for total surplus. Typical scenarios where each policy maximizes total surplus are shown in Table 6-15.

Table 6-15: Scenarios where each policy maximizes total surplus

Parameter	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Economic market model	Monopoly	Dominant-Fringe	Cournot	Cournot	Cournot
$\%N_L$=N0	30%	0%	0%	0%	30%
$\%N_L$=0	30%	0%	30%	30%	30%
Income-N_L correlation	0.75	0.75	0.75	.75	.75
D_w (cost savings factor)	0.1	0.1	0.3	0.6	0.6
S_p (price discrimination factor)	0.25	0.6	0.6	0.3	0.3
Pre-regulation	47.9%	0.2%	6.8%	9.7%	**74.5%**
No Regulation	1.9%	33.9%	16.9%	**43.6%**	9.2%
RFID Bill of Rights	0.00%	20.7%	**36.9%**	17.0%	51.8%
Blocker Tag	**94.9%**	0.6%	17.0%	10.3%	36%
Self-regulation	0.0%	**46.2%**	7.1%	2.0%	1.3%

As with consumer surplus, further analysis of similar variations allows transitions to each of the policies to be identified:

- The Blocker Tag maximizes total surplus in the monopoly market model with low cost savings benefit, high income-N_L correlation or with lower income-N_L correlation, and heterogeneous population (high $\%N_L$=0 and $\%N_L$=N0)
- The RFID Bill of Rights has the highest probability of maximizing total surplus in most scenarios of the Cournot market model, unless price discrimination is low, cost savings is high, and the population is homogeneous.

- Total surplus is maximized when there is No Regulation, under either the Cournot or Dominant-Fringe market model, when there is low price discrimination, and the population is homogeneous. In the monopoly market model, similar conditions hold, without the constraint of low price discrimination.
- Total surplus is most likely to be maximized pre-regulation when there is a heterogeneous population with a strong income-N_L correlation and low price discrimination, in either the Cournot or Dominant-Fringe market model.
- Finally, Self-regulation has the highest probability of maximizing total surplus in a very specific set of conditions: the Dominant-Fringe market model, with very low cost savings, a high amount of price discrimination, maximum income-N_L correlation, and a very homogeneous population.

The same analysis was performed for total information collected. Typical scenarios where each policy maximizes total surplus are shown below, in Table 6-16. Again, analysis of these scenario predictions allows key transitions between each of the policies to be identified:

- No Regulation and the Self-regulation policy are very similar in the scenarios where their respective probabilities maximize information collected. This is most likely to occur in the Cournot market model with low price discrimination, high cost savings, low income, and a heterogeneous population.
- The RFID Bill of Rights maximizes information collected in the Cournot market model, when there is low price discrimination, low cost savings, and a somewhat homogeneous population.

- The Blocker Tag policy is most likely to maximize information collected in all other scenarios. This is expected from the high number of top-ranked outputs for the Blocker Tag, as reported in Table 6-5.

Table 6-16: Scenarios where each policy maximizes information collected

Parameter	Scenario 1	Scenario 2	Scenario 3
Economic market model	Cournot	Cournot	Cournot
N_L σ	1	2	2
Mean Income	100	60	100
$\%N_L=0$	0	30%	0
Income-N_L correlation	1	1	1
D_w (cost savings factor)	0	0.6	0.6
S_P (price discrimination factor)	0.3	0	0.3
No Regulation	11.5%	**98.0%**	11.0%
RFID Bill of Rights	**95.5%**	95.4%	52.8%
Blocker Tag	74.2%	59.8%	**91.2%**
Self-regulation	38.4%	96.1%	35.2%

Comparing these results for all three of the major outputs, it is evident that it is not generally possible to find any conditions where a single policy is the most likely optimal strategy for all three outputs. For example, consumer surplus is maximized Pre-Regulation when price discrimination is high, but total surplus is maximized Pre-Regulation when price discrimination is low. Another example is that the Blocker Tag maximizes consumer surplus when there is substantial cost savings from RFID, but maximizes total surplus when the cost savings benefit is low. One interesting exception is the No Regulation policy, which maximizes both total and consumer surplus when there is low price discrimination and a

homogeneous population, in the Cournot or Dominant-Fringe market structure. However, this scenario does not result in the No Regulation policy maximizing information collected.

6.3. Analysis and discussion of results

Examining results across each all of these analytic approaches highlights several interesting results:[20]

- As modeled, policies do matter, but none are either dominant or dominated by another. Further, there is significant interaction between policies and the market model and characteristics, and between policies and individual characteristics.
- For the specified range of parameters, individual heterogeneity matters as much as or more than policy choice in many cases. Particularly important is the shape of the distribution of individual preferences, since the tails have opposite effects. This is seen from the opposite signs in many parametric estimates of % N_L=0 and % N_L=max. Further, the degree of heterogeneity is a clear factor in modeling which policy has the highest probability of maximizing any of the analyzed outputs.
- Fringe firms are best off with no RFID at all in most cases. Once the dominant firm adopts RFID, the fringe is most often best served by not adopting RFID, and allowing customers to sort themselves out. This is a logical outcome from the model setup assumptions, where the fringe is assumed to benefit less from the addition of RFID. As a result, they are at a competitive disadvantage. This disadvantage can be made up through policies that make RFID expensive (to

[20] Note that all of these conclusions are a function of model and parametric assumptions. Conclusions such as the relative significance of different policies and parameters are likely to be sensitive to these assumptions.

firms or consumers) or if the population is strongly inclined to value privacy. These outcomes mean that policies can change the overall rate of adoption of RFID across the retail sector applications considered here, and the viability of an information commons.

- Heterogeneity interacts with firm decisions about how much information to collect. If the population is already very heterogeneous, then it will sort itself out between firms, based on the price and information strategies of the firms, and collecting information has less benefit. If the population is more homogeneous, then it is less likely to separate itself out in a useful manner, and so it is more beneficial for a firm to collect information that can be used to capture consumer surplus. This suggests that a large information commons is more likely to exist when the population is homogenous, rather than heterogeneous, and policies to manage the commons and enable greater use of RFID systems are more necessary in that case.

6.4. Model Predictions and Framework

As seen, detailed analysis of all of these outputs across all possible parametric variations is a complicated task, and it is difficult to draw conclusions about many parameters or outputs, partly because a careful selection of parameters allows virtually any possible output to be produced. One method of simplifying this step and allowing a more thorough consideration of the implications of possible outcomes is scenario planning, which is a tool for creating flexible long-term plans. This tool defines several possible future worlds, including particular parameter sets (scenarios), a path by which those situations might evolve, and the expected outcomes. The creation of these "worlds" allows decision-makers to

understanding the driving forces involved with a particular problem, and create adaptive plans that are sensitive to various signposts identified as characteristics of each scenario. In this case, three scenarios are described: Status Quo, Big Brother and Social Paranoia. For each of these worlds, this section of analysis describes that hypothetical future and then provides both a set of parameters and predictions using the models previously discussed in this chapter, as well as a qualitative assessment using the framework of chapter 3. The integration of the quantitative analysis on top of these scenarios can allow for policy planning that is sensitive to both quantitative and qualitative issues.

The Status Quo scenario is simply an extrapolation of the current situation with regard to the deployment of RFID, and individual preferences about privacy. That is, RFID and associated data management technologies continue to develop under the auspices of the various private and cooperative enterprises that are currently engaged in these activities. The US federal government (and other relevant bodies, such as state legislatures) takes no explicit role in these developments, except as a customer in applications such as those already discussed in Chapter 3. The public debate about the use of RFID continues without any real consensus being reached, and there are no events that lead to overwhelming social pressure in any direction. Economic simulation parameters describing this future world, shown in the second column of Table 6-17 are the best estimates for current values: there are small segments of the population with the extreme views about RFID and privacy and everyone else occupies a wide normal distribution, that distribution is positively correlated with income (wealthy individuals are more likely to see the need and value in protecting their personal information at the expense of luxury consumption), and a reasonable amount of both price discrimination and cost reduction will take place.

Social Paranoia is a scenario where information collection is strongly resisted by a significant portion of the population. This future could evolve for reasons related to government or firm-level misuse of personal information, such as recent negligence by the Department of Veterans Affairs. This mismanagement will inevitably lead to additional costs to individuals, such as recovering from identity theft, and in the extreme case will lead the government to institute protective actions. Both of these factors contribute to reduced individual income. The general climate of distrust in surveillance results in less standardized RFID and data management technologies. Consequently, price discrimination and cost benefits are both lower than in the status quo scenario. The obvious cost of lost personal information means that a strong plurality of individuals will resist all information collection, while only a very small minority will continue to support unimpeded collection. Additionally, the taste for privacy will become more strongly correlated with income, as wealthier individuals will perceive a greater risk. Finally, there will be more variance in income; firms that already collect information about employees will be forced to pay higher wages in order to satisfy employee privacy concerns, while firms that don't collect information, or manage it properly, will offer less compensation in return. Simulation parameters describing these scenario characteristics are shown in the third column of Table 6-17.

Big Brother is a scenario where the government has taken wide steps to enhance its ability to collect and use personal information, with little or no resistance from individuals. A presumptive cause of this scenario is additional acts of terrorism against the US, followed by evidence and claims that enhanced surveillance and information collection would have minimized (or eliminated) the likelihood of successful terror acts. As a result of this demonstration, individual beliefs swing strongly in favor of allowing personal information to

be collected, to the point where a majority of individuals express no concern at all over information collection, and only a very small minority objects to it altogether. Those individuals with an intermediate taste for privacy are tightly grouped around a threshold level that they believe is sufficient for the government's counterterrorism activities. There is no correlation between income levels and the desire for privacy, as individuals at all income levels are accepting of the government's surveillance needs. The government responds to this shift by greatly expanding its surveillance programs, which are paid for by a tax increase. In addition, the government establishes standards for all surveillance and information collection technologies, including RFID, and encourages private corporations to participate in programs whereby they can collect and use information for their own purposes, as long as they also share that information with the government. These firms are both able to see greater logistic benefits, and increased ability to price discriminate. Parameters describing this future world are shown in the fourth column of Table 6-17.

Table 6-17: Prediction parameters for 3 future scenarios

Parameter	Status Quo	Social Paranoia	Big Brother
R	0.5	.75	0
Ds	0.5	.25	0.75
S_p	0.5	0.33	0.66
I	125	120	120
%NL=0	15%	5%	50%
%NL=max	15%	50%	5%
σ_I	10	15	10
σ_{NL}	1	0.1	0.1

These scenarios can be analyzed in two ways. The first is the outcome of the prediction models developed earlier in this chapter, and these results are shown in Table 6-18 below. The second is a qualitative assessment of the non-explicit economic impacts in each scenario, according to the stakeholder framework of chapter 3. Two of these are presented in Table

6-19 and Table 6-20 below, comparing the Social Paranoia and Big Brother scenarios to the Status Quo. Table 6-18 shows values predicted by the linear forecasting models, for each of the scenarios parametrically described in Table 6-17. The 1st row of results is the baseline case, and the predicted parameters are for scenario 1 of the Status Quo future scenarios, so they are the expected outcome before any RFID systems are deployed.

Table 6-18: Scenario economic outcomes predicted by linear models

Scenario	Policy	Fringe Opt.	Price	Nact	Q	Qf	Qw	π_f	π_w	CS
Status Quo: Pre-RFID	All (avg.)	1	85.0		43.4	17.3	26.2	695	1296	1261
Status Quo	All (avg.)	2	80.5	2.5	45.7	16.1	29.8	663	1411	1194
Paranoia	All (avg.)	3	89.5	0.1	42.5	19.2	23.5	751	1114	1510
Big Brother	No reg., Self-reg, BT)	4	65.0	5.3	47.6	14.7	33.3	500	1684	951
Big Brother	BofR	2	67.0	5.2	46.4	13.9	32.7	496	1620	941

The subsequent four rows of Table 6-18 represent the predicted fringe optimum strategy and parametric outcomes, given the optimum choice of the fringe, for each of the future scenarios. In each scenario, predictions were made using each of the four policy options, and each of the two economic models of strategic interaction. In the Status Quo and Social Paranoia scenarios, the predicted outcomes for each of these cases were very similar, so they are each reported by a single row of Table 6-18 that contains the average of 8 predictions (4 policies * 2 economic models) for each outcome.[21] The Big Brother scenario is divided into 2 rows, because the RFID Bill of Rights policy results in a different fringe strategic choice. As a result, the first row of Big Brother results represents the average of 6

[21] Actual parametric differences are on the order of those shown in the results tables above. So, for example, the different economic models cause Nact to vary by about 0.5, while the policy choice has a similar effect.

predictions, while the second row contains the average of only the 2 Bill of Rights predictions. It can be seen, however, that the quantitative predictions are quite similar for each of the other parameters, especially when compared to the baseline, again implying that while policy choice is significant, its effect is relatively small when compared with heterogeneity.

The importance of heterogeneity, as opposed to variations in other systemic parameters was confirmed by predicting outputs for two alternative sets of scenarios. In the first set of alternatives, the heterogeneity parameters (R, %NL=0, %NL=max, σ_I and σ_{NL}) for the Social Paranoia and Big Brother scenarios were held equivalent to those values shown in Table 6-17 while the other parameters were reset to the same values as used for the Status Quo scenario. In this case, the fringe optimum strategies were the same in all cases, other outputs were similar in magnitude, and policies were ordered the same. The second alternative set of scenarios was the inverse of the first set; it reverted all of the heterogeneity parameters to status quo values, while the other terms (Ds, I, S_p) were kept at the original scenario levels. In this case, the prediction outputs were significantly different. In nearly all cases, the fringe optimum was found to be scenario 2, meaning that the fringe firms would never adopt RFID nor match prices with the dominant firm. This result held for all policies in the Big Brother Scenario, and even for both the Self-regulation and No Regulation policies under the Social Paranoia Scenario. The Blocker Tag still led to the fringe choosing strategy 4 (adopting RFID and matching price), but the Bill of Rights Policy resulted in a choice of strategy 3 for the fringe. Thus, the non-heterogeneity parameters led to a different fringe strategic outcome in nearly all cases, while the heterogeneity parameters produced identical strategic choices in all cases. This supports the contention that individual heterogeneity has the most substantial impact on the final predicted results for the scenarios.

Table 6-19 and Table 6-20 Table 6-18 below are the summaries of stakeholder costs and benefits, relative to the Status Quo scenarios, for the Social Paranoia, and Big Brother scenarios, respectively. In both, cells are shaded to provide a quick reference, with the same color-coding previously used in chapter four. An orange cell indicates a relatively worse situation: higher costs or reduced benefits. A light green cell highlights the opposite: reduced costs or increased benefits. A yellow cell shows that costs or benefits can be expected to be the same. Due to the similarities reported in Table 6-18, these summaries are policy independent.

Table 6-19: Stakeholder framework analysis for social paranoia scenario

Stakeholders			
Individuals/ Consumers	**Firms/Business**	**Government/Regulators**	**Society**
Cost/benefit of technology: change in consumer prices	Fixed Cost of deploying RFID technology	Method & cost of policy or standards development/ implementation/ regulation	Change in overall social welfare
Cost/benefit of information effect on privacy	Variable (operating) costs of data collection	Cost of protecting civil liberties	Information commons
Benefit of information: Convenience, service	Cost of Information Control: Protection; Liability	Cost of no regulation (market failures, etc.)	
	Benefit of technology: cost reduction through enhanced logistics	Benefit of technology: logistic improvements to government consumers (military, libraries, etc.)	
	Benefit of information: Market power allows price discrimination, selling data, etc.	Benefit of information: data access for law enforcement, regulation, emergency response, etc.	

Increased costs/ Reduced benefits
Reduced Costs/ Increased Benefits
No expected change

As expected, the outcome of the scenarios is inverted in many, but not all respects. For example, all benefits of using information decrease in the Social Paranoia scenario, but

increase in Big Brother. This logically leads to the better-managed information commons in the Big Brother case. One interpretation of this is that the majority of the stakeholders (individuals and firms) are much less likely to compete for information, either in self-protection or to gain an advantage over others, due to the perceived societal cost of this competition. As a result, there is more information widely available for all stakeholders to use, without concerns about it being degraded. This leads to several other tradeoffs, most notably, firm profits increase markedly, but consumer surplus declines more rapidly, resulting in a fall in overall social welfare. This is possibly compensated by the extra information benefits that are not captured in the economic model or predictions.

Table 6-20: Stakeholder framework analysis for big brother scenario

Stakeholders			
Individuals/ Consumers	**Firms/Business**	**Government/Regulators**	**Society**
Cost/benefit of technology: change in consumer prices	Fixed Cost of deploying RFID technology	Method & cost of policy or standards development/ implementation/ regulation	Change in overall social welfare
Cost/benefit of information effect on privacy	Variable (operating) costs of data collection	Cost of protecting civil liberties	Information commons
Benefit of information: Convenience, service	Cost of Information Control: Protection; Liability	Cost of no regulation (market failures, etc.)	
	Benefit of technology: cost reduction through enhanced logistics	Benefit of technology: logistic improvements to government consumers (military, libraries, etc.)	
	Benefit of information: Market power allows price discrimination, selling data, etc.	Benefit of information: data access for law enforcement, regulation, emergency response, etc.	

Increased costs/ Reduced benefits
Reduced Costs/ Increased Benefits
No expected change

7. Conclusions and Policy Recommendations

This research has applied qualitative and quantitative methods that enable consideration of the broad implications of how new technologies and associated policies affect the balance between individual privacy, economic efficiency, and security. Currently, most policy research and proposals consider only one on these issues, and frequently only from the perspective of one stakeholder in the debate. The framework laid out here offers a broad view of all of the issues facing each of the stakeholders, and therefore provides a novel perspective on a policy debate that often consists primarily of issue advocacy on all sides. Further, the quantitative economic model that is developed offers specific measures for evaluating many of the outcomes, and illustrates the many tradeoffs that are implicit in all policy proposals. The model was used on a number of simulations, enabling some exploration of a range of parameters that might affect the many outcomes. Although, like all models, it is an imperfect representation of a real world problem, it is useful in identifying a number of interesting conclusions.

The first significant conclusion from the economic analysis is that policies do matter, but in the face of substantial uncertainties in market structure and individual preferences, it is not possible to identify a "best" policy. That is, there is not any single policy that ensures positive outcomes across the many outputs that stakeholders are interested in, and across the range of policy, market, and individual parameters that were modeled. For example, the policy that is modeled to offer individuals low-cost methods of protecting personal information often leads to the most information collection by firms, and the largest decrease in consumer surplus, but the highest ranked total surplus. These uncertainties mean that

there is a strong need to understand the real nature of the relevant markets, and true individual tastes for privacy.

Independent of policy choices, individual taste for privacy has a clear impact, especially on the competitive behavior of firms. If individual preferences are widely distributed, then individuals sort themselves so that their privacy tastes become aligned with the firm practices. In this case, a fringe firm, not collecting information about individuals, can achieve a better result simply by charging an appropriate higher price that is less than the cost of protecting information for enough individuals that they consume from the fringe. Even if the fringe can price discriminate when matching the dominant firm price, this strategy results in a greater fringe firm profit than if they choose to compete directly with the dominant firm on price. On the other hand, if individuals are more homogeneous in their privacy preferences, then they will not sort out in this manner. The price strategy of the dominant firm will force the fringe firm to behave in a similar manner. As a result, both firms collect personal information and engage in price discrimination. Unfortunately, the most prevalent data about individual privacy preferences, such as the Westin survey results, don't provide enough insight into individual behaviors to accurately answer this question.

Combining these market and individual uncertainties produces a third important result and insight into policy options that might succeed despite the uncertainties in the problem. Of the policies evaluated, the RFID blocker tag was shown to enable the greatest collection of information, and therefore, the broadest use across all applications. At the same time, because this policy allows for information to be protected at the level desired by each stakeholder, it offers the least competition between stakeholders with different marginal costs or benefits. One interpretation of this outcome is that this policy is successful because it distributes the cost of using information more equitably to each stakeholder, according to

that actor's own marginal costs and benefits. It does this through having a larger share of the policy cost implemented in a variable (per unit) mechanism. At the other end, the policy with the greatest fixed cost (RFID Bill of Rights), which is largely imposed on only one stakeholder, generally results in the slowest adoption of RFID technology, and less information collection. It does this for the benefit of one aspect of one stakeholder interest, individual privacy. Although the industry self-regulation policy resulted in slightly greater rates of information collection and technology adoption, it also suffers from placing too much of the cost burden upon one stakeholder, in this case individual consumers, for the benefit of firm cost-savings. If either outcome holds, then general RFID adoption is likely to similarly follow a slow path, since it will be deprived of the economy of scale benefits of (one of) the largest potential applications. As a result, many other applications and benefits (and costs) of the technology, including those in arenas with no direct impact on individual privacy, will be slower to transpire.

These results are specific to the RFID policy problem analyzed here, but this research can be generalized and applied to other intersections of technology and privacy that are experiencing similar debates. This includes both other application areas for RFID, and other technologies, such as biometrics. For example, a number of retailers are beginning to use biometric technologies like fingerprinting both to monitor employees and as a method of identifying a customer, and linking to a pre-approved account, such as a credit card.[22] The exact tradeoffs in this application are different, but the same approach can be taken. Applying the qualitative framework of chapter three to the specific problem and then refining an economic model to evaluate the specific costs and benefits can provide a clearer understanding of the implications of various policies. A cursory consideration of this simpler

[22] See www.paybytouch.com for one example of a fingerprint-based customer payment system.

problem also suggests that the importance of understanding individual heterogeneity still holds. If, for example, customers have a wide range of preferences with regard to using the fingerprinting system, then some stores will choose this method of payment, others will not, and individuals will sort themselves accordingly. However, if preferences are much narrower, then it becomes more important to understand them, in order for the firms to make the best decision.

Based on these research outcomes and the continuing debate over RFID and other technologies, several recommendations suggest themselves. These include steps for improving the accuracy and utility of the model, improving the general ability to analyze these types of problems, and addressing policy issues.

The first recommendation is to collect more and better data on both individual preferences for privacy versus consumption and policy costs to firms, individuals and government regulatory agencies. Data on individual preferences can come from several sources, including better survey instruments or economic experiments than those discussed and relied upon in this analysis. Better still would be econometric research capitalizing on natural economic experiments on a much larger scale. One such natural experiment is the differential introduction of supermarket club cards into a retail market. These club cards are a means of price discrimination for the retailers, based on their ability to profile individuals. Over time, these cards have been differentially introduced by multiple firms in common markets and by single firms across multiple markets. This offers the possibility for an econometric investigation into the effect of club cards on retail prices, and shopper behavior. Data on prices are available, at substantial cost, from services that aggregate and market this information to the supermarket retailers. This type of distributional data, along with a clearer understanding of the market dynamics between the dominant and fringe firms would allow

more specific testing of model results, and might enable meaningful predictions of the impact of each policy.

Second, the analysis presented here can be expanded and improved in numerous ways. First, the existing model can be exercised more thoroughly, not only with better preference data as recommended above, but also through increased variation in firm characteristics, the implementation of more polices, and better characterization of the true costs of those polices. Additionally, the current analysis relies on specific functional forms to describe the behavior of individuals and firms, and the strategic interaction of the firms. Although these forms were tested, and found to have only a small effect on the outcomes, other forms can be tested, as well. Even better, more general models can be developed and applied.

A third and final recommendation is that policies that are flexible and adaptable to changing circumstances should be preferred, especially if they are implemented prior to developing any better understanding of individual preferences. Adopting a policy-making approach such as Assumption-Based Planning, which is specifically designed to deal with uncertainties, would help to accomplish such flexibility.(Dewar, Builder et al. 1993) Further, policies with large fixed costs to just one stakeholder should be avoided. Although they might turn out to be optimal if their costs fortuitously match the overall social costs and benefits of implementing RFID, they are also likely to have a substantial negative impact on the overall information commons. Policies that have a more broadly distributed overall cost are likely to be more robust to shifting preferences, and to preserving the overall information commons, and therefore allowing further use of RFID technology in other applications. This recommendation, in particular, is significant for all arenas of the technology/privacy/security debate.

Finally, it is important to note that technology continues to evolve, both in its capabilities and uses. Individual preferences and behaviors will also continue to evolve, both naturally in response to these new technologies, and as a result of external events. As an area of research and policy, much is still left to learn about these continuous changes, and how best to deal with them. Almost certainly, the best solution is not the continued creation of specific policies crafted in response to particular real or perceived issues, such as for every new technology. As seen, these tend to result in solutions that place a large burden on one set of stakeholders, for minimal overall benefit. Rather, it would be better if we, as a society, developed a broad conception of how to understand the interaction between privacy, technology, and security, which would then be applied as needed. Hopefully, the research presented here is a small step in that direction.

Appendix A: Laws and other agreements pertaining to RFID and privacy

Principles of the OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Information"

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.
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 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.
4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 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 unauthorised 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 the 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 sub-paragraphs (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. (OECD 1980)

US/EU Safe Harbor Principles

- Notice: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.

- Choice: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party[1] or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

- Onward Transfer: To disclose information to a third party, organizations must apply the Notice and Choice Principles.

- Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

- Data Integrity: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.

- Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

- Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations. (US Department of Commerce 2000)

State laws pertaining to RFID

Table A-1: 2005 US State Legislation Related to RFID

State	Status	Retail	Disclosure	Remove or Deactivate	Link to Personal Information	Prohibits	Other
Calif.	Legislature Adjourned	No	Required		Prohibited	Use in driver's licenses, K-12 student Ids, government health and benefit cards, and public library cards	Criminalizes remote reading without owner's knowledge
Illinois	Referred to committee	No					Requires hospitals to use RFID during Surgery to identify patient + surgeon, date+ type of surgery, and body part to operate on
Mary.	Legislature Adjourned	Yes					Creates a task force to study RFID use by retailers and manufacturers
Mass.	Referred to committee	Yes	Required	Required			Attorney General to develop regulations
Missouri	Legislature Adjourned	Yes	Required				
Nevada	Legislature Adjourned	Yes	Required				
New Hamp.	Referred to committee	Yes	Required				
New Mexico	Legislature Adjourned	Yes	Required	Required	Prohibited		
Rhode Island	Vetoed	No				State of municipal tracking movement or identify as a service condition	
South Dakota	Legislature Adjourned	Yes		Required	Requires permission	Use in humans	
Tenn.	Legislature Adjourned	Yes	Required				
Texas	Legislature Adjourned	No				Mandatory tracking or ID of public school students	

State	Status	Retail	Disclosure	Remove or Deactivate	Link to Personal Information	Prohibits	Other
Utah	Enacted	Yes					Exempts collecting information with RFID from the Computer Crimes Act
Virg.	Legislature Adjourned	No					Requires a privacy impact analysis when authorizing or prohibiting use of RFID
Virg.	Enacted	No					Individually identifiable data generated by toll-collection systems requires a court warrant for disclosure
Wyom.	Enacted	No					Authorizes telepharmacies to use RFID in inventory control

(adapted from National Conference of State Legislatures 2005)

Appendix B: Data

Rank Ordering Summary Tables

Table B-1: Rank ordering of policies for key outputs in all simulations; Strategic Interaction Scenario 2

Parameter	Rank	Blocker Tag	Self-Regulation	Bill of Rights	No Regulation	Pre-Regulation
π_w	1	228	15	18	230	13
	2	49	241	106	89	19
	3	203	204	34	52	11
	4	24	39	292	119	30
	5	0	5	54	14	431
π_f	1	4	20	6	27	279
	2	88	57	84	91	16
	3	60	119	78	58	21
	4	59	91	112	62	12
	5	125	49	56	98	8
Nact	1	383	42	40	39	0
	2	33	147	251	73	0
	3	30	243	98	133	0
	4	58	72	115	259	0
	5	0	0	0	0	504
Q	1	115	125	98	166	0
	2	67	187	122	128	0
	3	94	118	181	111	0
	4	228	74	103	99	0
	5	0	0	0	0	504
Consumer Surplus	1	6	28	6	133	331
	2	48	152	46	234	24
	3	58	232	140	34	40
	4	124	68	240	42	30
	5	268	24	72	61	79

Note that Scenario 2 includes Cournot, dominant-fringe, and monopoly models of interaction, so there are more cases than in the other scenarios. The monopoly model is not applicable for the fringe firm profit, and in the case of quantity, the monopoly quantity is substituted.

Table B-2: Rank ordering of policies for key outputs in all simulations; Strategic Interaction Scenario 3

Parameter	Rank	Blocker Tag	Self-Regulation	Bill of Rights	No Regulation	Pre-Regulation
π_w	1	96	2	0	210	28
	2	29	203	0	78	26
	3	190	113	1	30	2
	4	20	18	249	16	33
	5	1	0	86	2	247
π_f	1	1	6	0	8	321
	2	82	14	210	26	4
	3	175	34	92	27	8
	4	19	257	23	34	3
	5	59	25	11	241	0
Nact	1	322	3	7	4	0
	2	6	156	168	6	0
	3	6	175	92	63	0
	4	1	1	69	262	3
	5	1	1	0	1	333
Q	1	167	8	1	160	0
	2	23	233	34	42	4
	3	141	66	53	68	8
	4	4	22	247	54	9
	5	1	7	1	12	315
Consumer Surplus	1	54	7	3	150	122
	2	25	162	15	103	31
	3	85	133	52	23	43
	4	68	25	185	40	18
	5	104	9	81	20	122

Table B-3: Rank ordering of policies for key outputs in all simulations; Strategic Interaction Scenario 4

Parameter	Rank	Blocker Tag	Self-Regulation	Bill of Rights	No Regulation	Pre-Regulation
π_w	1	89	0	0	194	53
	2	45	202	4	53	32
	3	164	119	4	43	6
	4	34	15	216	44	27
	5	4	0	112	2	218
π_f	1	0	173	69	82	12
	2	0	2	104	212	18
	3	0	2	67	34	233
	4	23	137	95	8	73
	5	313	22	1	0	0
Nact	1	327	3	2	4	0
	2	3	103	226	4	0
	3	5	226	87	18	0
	4	1	4	21	310	0
	5	0	0	0	0	336
Q	1	196	6	6	128	0
	2	17	213	37	64	5
	3	113	95	46	78	4
	4	4	16	243	52	21
	5	6	6	4	14	306
Consumer Surplus	1	43	4	6	73	210
	2	75	84	4	139	34
	3	64	159	54	33	26
	4	117	73	91	27	28
	5	37	16	181	64	38

Table B-4: Estimates for significant parameters for Strategy 1, all outputs

Parameter estimate	P_sc1	Q_Sc1	Qf_Sc1	Qw_Sc1	πf_Sc1	πw_Sc1	CS_Sc1
$\underline{R}^2$	0.92	0.91	0.83	0.94	0.89	0.91	0.90
R	3.79	0.27		0.44	52.69	112.60	127.10
Ds							
S_p							
I	0.60	0.36	0.15	0.22	10.79	22.40	15.09
%NL=0	7.15	-4.31	-3.11	-1.39	80.63	177.50	389.30
%NL=max	12.83			1.43	245.40	475.00	524.20
σ_I	0.10	-0.07	-0.04	-0.03	1.75	2.20	10.04
σ_{NL}							
Bill of Rights (BoR)							
Blocker Tag (BT)							
Industry Self-regulation (ISR)							
Dominant-Fringe (DF)	1.81	-1.40	1.34	-2.73	25.94		-70.28
Monopoly	18.72			0.59		506.20	-667.00

Table B-5: Estimates for significant parameters for Strategy 2

Parameter estimate	P_sc2	Q_Sc2	Qf_Sc2	Qw_Sc2	πf_Sc2	πw_Sc2	CS_Sc2	N_Sc2	Nact_Sc2
$\underline{R}^2$	0.86	0.89	0.22	0.55	0.39	0.85	0.83	0.62	0.74
R	5.83		-1.94	1.00	-135.80	-108.98	256.46	-2.70	-1.24
Ds	-5.77	1.49		3.50		230.97		1.05	0.65
S_p	-7.76	2.49	4.51		160.94	394.13	-368.15	2.39	1.03
I	0.56	0.38	0.11	0.27	8.78	25.99	13.76	0.01	0.01
%NL=0	-6.96		7.05	-4.15	350.96	448.33	194.95	4.73	0.89
%NL=max	15.42				-264.75		687.66	-4.97	-5.92
σ_I	0.07	-0.06	-0.11		-3.54	5.61	8.17		
σ_{NL}	-0.89	0.91	3.14	-1.71	126.37	-64.05	33.64	-0.33	-0.63
BoR	1.79	-0.56				-80.46			
BT	1.13	-0.56	-1.27				-54.78	1.23	0.52
ISR									
DF	-1.40					134.33	-27.09	0.69	0.50
Monopoly	13.40			-4.25		461.72	-546.79	0.53	1.00

Table B-6: Estimates for significant parametric deltas between Strategy 2 and Strategy 1

Parameter estimate	ΔP_Sc2	ΔQ_Sc2	ΔQf_Sc2	ΔQw_Sc2	Δπf_Sc2	Δπw_Sc2	ΔCS_Sc2
$\underline{R}^2$	0.53	0.55	0.20	0.41	0.21	0.66	0.53
R	2.04		-1.79	0.56	-188.50	-221.59	129.40
Ds	-5.77	1.48		3.49		230.98	53.32
S_p	-7.77	2.49	4.51		161.03	394.14	-368.81
I	-0.04	0.02	-0.04	0.05	-2.01	3.59	-1.33
%NL=0	-14.11	4.50	10.16		270.33	270.85	-194.36
%NL=max	2.58	-1.51		-3.74	-510.15	-510.55	163.45
σ_I			-0.07	0.06	-5.29	3.41	-1.88
σ_{NL}	-1.13	0.88	3.11	-1.72	120.86	-78.85	45.78
BoR	1.79	-0.56				-80.46	-29.00
BT	1.12	-0.56	-1.26				-55.43
ISR							
DF	-3.21	1.62	-1.71	3.33		153.53	43.18
Monopoly	-5.33			-4.84		-44.49	120.20

Table B-7: Estimates for significant parameters for Strategy 3

Parameter estimate	P_sc3	Q_Sc3	Qf_Sc3	Qw_Sc3	πf_Sc3	πw_Sc3	CS_Sc3	N_Sc3	Nact_Sc3
$\underline{R}^2$	0.78	0.90	0.81	0.87	0.77	0.80	0.84	0.65	0.74
R	8.22	-1.35	0.24	-1.59	127.64	-168.48	225.43	-3.13	-1.48
Ds	-12.59	5.74	-1.48	7.21	-197.93	299.32	206.20	2.50	1.19
S_p	-16.00	8.04	-1.91	9.95	-250.57	510.72	-307.18	2.76	1.12
I	0.47	0.40	0.13	0.28	7.78	23.63	18.12	0.02	0.01
%NL=0	-12.98		-4.34	2.80	-221.49	597.16	180.85	6.61	2.84
%NL=max	18.97	-12.29	1.50	-13.79	373.73		564.53	-4.33	-7.53
σ_I			-0.02			5.17	8.62		
σ_{NL}		-0.91		-0.97					-0.45
BoR	3.06	-0.95	0.36	-1.31	47.79	-114.52	-71.73	0.42	0.16
BT	2.68		0.26		41.61		-59.59	1.47	0.62
ISR								0.31	
DF	3.30	-3.72	1.59	-5.31	47.04	32.01	-150.97	0.51	0.26
Monopoly									

Table B-8: Estimates for significant parametric deltas between Strategy 3 and Strategy 1

Parameter estimate	ΔP_Sc3	ΔQ_Sc3	ΔQf_Sc3	ΔQw_Sc3	Δπf_Sc3	Δπw_Sc3	ΔCS_Sc3
$\underline{R}^2$	0.68	0.74	0.59	0.76	0.71	0.63	0.50
R	4.82	-1.62	0.38	-2.00	75.40	-265.17	83.37
Ds	-12.69	5.73	-1.46	7.19	-199.00	296.98	204.04
S_p	-15.99	8.02	-1.91	9.94	-250.51	510.74	-308.18
I	-0.10	0.04	-0.02	0.06	-3.03	3.75	
%NL=0	-18.79	2.68	-1.27	3.95	-304.55	450.47	-248.17
%NL=max	7.81	-12.96	2.29	-15.25	132.45	-564.81	
σ_I			0.02		-0.79	3.35	-1.82
σ_{NL}		-0.95		-0.98		-45.34	
BoR	3.03	-0.96	0.36	-1.32	47.39	-115.22	-72.15
BT	2.66		0.26		41.24	-40.41	-61.06
ISR							
DF	1.53	-2.32	0.25	-2.57	21.46	51.94	-80.43
Monopoly							

Table B-9: Estimates for significant parameters for Strategy 4

Parameter estimate	P_sc4	Q_Sc4	Qf_Sc4	Qw_Sc4	πf_Sc4	πw_Sc4	CS_Sc4	N_Sc4	Nact_Sc4
$\underline{R}^2$	0.76	0.87	0.73	0.87	0.78	0.80	0.72	0.66	0.74
R	10.37	-1.63	-0.29	-1.34	127.98	-141.83	386.31	-3.30	-1.69
Ds	-13.26	6.62		5.83	-133.22	234.61		2.26	1.17
S_p	-18.91	8.61	1.95	6.66	-308.68	504.52	-860.38	3.68	1.54
I	0.47	0.42	0.16	0.26	8.67	22.69	14.69	0.01	0.01
%NL=0	-11.52	-3.75	-4.25		-130.41	548.57	-322.04	5.46	1.90
%NL=max	21.75	-17.57	-7.53	-10.04	378.64		703.41	-4.81	-7.64
σ_I			-0.02			4.89	8.24		0.01
σ_{NL}		-1.15	-0.45	-0.70					-0.45
BoR	3.61	-1.39	-0.43	-0.96	-22.88	-81.08	-71.62	0.50	0.21
BT	3.18		0.74					1.15	0.51
ISR									
DF	3.67	-4.58	-2.30	-2.28	34.80	78.77	-191.83	0.93	0.62
Monopoly									

Table B-10: Estimates for significant parametric deltas between Strategy 4 and Strategy 1

Parameter estimate	ΔP_Sc4	ΔQ_Sc4	ΔQf_Sc4	ΔQw_Sc4	Δπf_Sc4	Δπw_Sc4	ΔCS_Sc4
$\underline{R}^2$	0.65	0.71	0.58	0.72	75.33	0.61	0.61
R	6.94	-1.90		-1.76	-132.94	-239.39	244.17
Ds	-13.25	6.61		5.81	-308.66	234.86	
S_p	-18.91	8.60	1.95	6.65	-307.19	504.48	-861.56
I	-0.10	0.06	0.02	0.04	-2.13	2.82	-3.35
%NL=0	-17.22			1.69	-211.07	405.73	-747.76
%NL=max	10.33	-18.33	-6.76	-11.57	133.22	-517.71	
σ_I	-0.06	0.03				3.07	
σ_{NL}		-1.18	-0.48	-0.71		-43.81	
BoR	3.61	-1.39	-0.43	-0.96	-22.95	-81.17	-72.00
BT	3.18		0.74				
ISR							
DF	1.86	-3.18	-3.64	0.45		97.93	-121.74
Monopoly							

Sample Linear Regression Model

Below is a sample of the linear regression report for one output, Price, in for the first model of strategic interaction (no information collected.) Each other output produced a similar report. Reports are summarized by the above tables, B-4 through B-10.

Price_Sc1

```
Call:
lm(formula = y ~ ., data = rfiddf)

Residuals:
    Min      1Q  Median      3Q     Max
-7.5719 -3.0836 -0.2016  1.8265 11.1666

Coefficients: (3 not defined because of singularities)
                       Estimate Std. Error   t value Pr(>|t|)
(Intercept)           2.875e+00  7.869e-01     3.654 0.000265 ***
x.Econ_ModelDF        1.805e+00  2.084e-01     8.660  < 2e-16 ***
x.Econ_ModelMonopoly  1.872e+01  2.084e-01    89.822  < 2e-16 ***
x.Policy7             2.694e-03  2.405e-01     0.011 0.991064
x.Policy9            -1.389e-09  2.409e-01 -5.77e-09 1.000000
x.Policy10           -4.782e-09  2.409e-01 -1.99e-08 1.000000
x.NL_mean                    NA         NA        NA       NA
x.NL_s                2.360e-01  2.216e-01     1.065 0.287058
x.NL_min                     NA         NA        NA       NA
x.Income_mean         6.003e-01  5.203e-03   115.376  < 2e-16 ***
x.Income_s            9.572e-02  1.330e-02     7.197 8.64e-13 ***
x.N0                         NA         NA        NA       NA
x.NL.N0               1.283e+01  1.028e+00    12.487  < 2e-16 ***
x.NL.0                7.150e+00  1.028e+00     6.958 4.65e-12 ***
x.corr                3.793e+00  1.656e-01    22.909  < 2e-16 ***
x.Dw                  4.490e-03  5.673e-01     0.008 0.993686
x.PD_scale            2.694e-03  3.404e-01     0.008 0.993686
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 3.824 on 2005 degrees of freedom
Multiple R-Squared: 0.9243,   Adjusted R-squared: 0.9238
F-statistic:  1883 on 13 and 2005 DF,  p-value: < 2.2e-16
```

References

Directive 95/46/EC of the European Parliament and of the Council (1995). **Official Journal L 281:** 31-50.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002). **Official Journal L 201:** 37-47.

Acquisti, A. and H. R. Varian (2005). "Conditioning Prices on Purchase History." Marketing Science **24**(3): 367-381.

Adar, E. and B. A. Huberman (2000). "Free Riding on Gnutella." First Monday **5**(10).

Anderson, R. (2001). Why Information Security is Hard - An Economic Perspective. Annual Computer Security Applications Conference, New Orleans, LA, Applied Computer Security Associates.

Auto-ID Center (2003). What is Automatic Identification? **2003**. **http://www.autoidcenter.org/aboutthetech_whatis.asp**

Auto-ID Labs (2000). About Cambridge Auto-ID Lab. **2006**. **http://www.autoidlabs.org.uk/**

Ayres, I. and M. Funk (2002). Marketing Privacy: A Solution for the Blight of Telemarketing (and Spam and Junk Mail), SSRN.

Balkovich, E., T. Bikson, et al. (2005). 9 to 5: Do You Know if Your Boss Knows Where You Are? Santa Monica, CA, RAND Corporation.

Baumer, D. L., J. B. Earp, et al. (2005). Quantifying Privacy Choices with Experimental Economics. Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University.

Berendt, B., O. Gunther, et al. (2005). "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior." Communications of the ACM **48**(3).

Bezanson, R. P. (1992). "*The Right to Privacy* Revisited: Privacy, News, and Social Change, 1890-1990." California Law Review **80**(5): 1133-1175.

Boritz, E., W. G. No, et al. (2005). Internet Privacy Research: Framework, Review and Opportunities. Waterloo, Ontario, Canada, University of Waterloo.

Brandeis and Warren (1890). "The Right to Privacy." Harvard Law Review **4**(5).

Brin, D. (1998). The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? Reading, Massachusetts, Perseus Books.

Byford, K. S. (1998). "Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment." Rutgers Computer and Technology Law Journal **24**(1): 1-74.

Campbell, D. (2005). RFID and the United States Regulatory Landscape. RFID Applications, Security, and Privacy. S. L. Garfinkel and B. Rosenberg. Upper Saddle River, NJ, Addison-Wesley**:** 99-136.

Carson, S. (2005). 2004 Program Evaluation Findings Report. Cambridge, MA, MIT OpenCourseWare.

Cate, F. H. and R. Litan (2002). "Constitutional Issues in Information Privacy." Michigan Telecommunications and Technology Law Review **9**: 35-63.

Cavoukian, A. (2004). Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology. Toronto, Information and Privacy Commissioner, Ontario.
Center for Democracy & Technology Working Group on RFID (2006). Privacy Best Practices for Deployment of RFID Technology. Washington D.C., Center for Democracy & Technology.
Chellapa, R. K. and R. Sin (2005). "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma." Information Technology and Management **6**(2-3): 181-202.
Cranor, L. F., J. Reagle, et al. (1999). Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, AT&T Labs.
Danezis, G., S. Lewis, et al. (2005). How Much is Location Privacy Worth? Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University.
Das, R. (2005). Chip versus Chipless for RFID Applications. 2005 joint conference on Smart objects and ambient intelligence, Grenoble, France, ACM Press.
Data Protection Working Party (2005). Working Document on Data Protection Issues Related to RFID Technology. Brussels, Belgium, European Commission.
Dewan, R., B. Jing, et al. (2000). "Adoption of Internet-Based Product Customization and Pricing Strategies." Journal of Management Information Systems **17**(2): 9-28.
Dewar, J. A., C. H. Builder, et al. (1993). Assumption-Based Planning: A Planning Tool for Very Uncertain Times. Santa Monica, CA, RAND Corporation**:** 1-78.
Dommeyer, C. J. and B. L. Gross (2003). "What Consumers Know and What They Do: An Investigation of Consumer Knowlesge, Awareness and Use of Privacy Protection Strategies." Journal of Interactive Marketing **17**(2): 35-51.
Eckfeldt, B. (2005). "What Does RFID Do for the Consumer?" Communications of the ACM **48**(9): 77-80.
EPCglobal (2004). The EPCglobal Network(tm). Lawrenceville, NJ, EPCGlobal Inc.
EPCglobal Public Policy Steering Committee (2005). Guidelines on EPC for Consumer Products, EPCGlobal. **2006**. **http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html**
EPIC (2002). The Video Privacy Protection Act (VPPA), Electronic Privacy Information Center. **2006**. **http://www.epic.org/privacy/video/vppa.html**
Eschet, G. (2005). "FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification." Jurimetrics **45**: 301-332.
Etzioni, A. (2002). "Implications of Select New Technologies for Individual Rights and Public Safety." Harvard Journal of Law & Technology **15**: 257-290.
Federal Trade Commission (2005). Radio Frequency Identification: Applications and Implications for Consumers. Washington, DC, Federal Trade Commission**:** 1-48.
Freidman, A. and L. Wathieu (2005). An Empirical Approach to Understanding Privacy Valuation. Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University.
Froomkin, A. M. (2000). "The Death of Privacy." Stanford Law Review **52**: 1461-1543.

Fudenberg, D. and J. M. Villas-Boas (2006). Behavior-Based Price Discrimination and Customer Recognition. Economics and Information Systems. T. Hendershott, Elsevier.
GAO (2005). Radio Frequency Identification Technology in the Federal Government. Washington, DC, Government Accountability Office.
Garfinkel, S. L. (2000). Database Nation. Sebastopol, CA, O'Reilly & Associates.
Garfinkel, S. L., A. Juels, et al. (2005). "RFID Privacy: An Overview of Problems and Proposed Solutions." IEEE Security and Privacy: 34-43.
George, J. F. (2002). "Influences on the Intent to Make Internet Purchases." Internet Research **12**(2): 165-180.
Good, N., J. Han, et al. (2004). Radio Frequency ID and Privacy with Information Goods. WPES '04, Washington, DC, ACM.
Gormley, K. (1992). "One Hundred Years of Privacy." Wisconsin Law Review **1992**: 1335.
Graeff, T. R. and S. Harmon (2002). "Collecting and Using Personal Data: Consumers' Awareness and Concerns." Journal of Consumer Marketing **19**(4): 302-318.
Hara, Y. (2006). Hitachi advances paper-thin RFID chip. EE Times.
Hardgrave, B. C., M. Waller, et al. (2005). Does RFID Reduce Out of Stocks? A Preliminary Analysis. Fayetteville, Ak, Information Technology Research Institute, Sam M. Walton College of Business, University of Arkansas.
Hardin, G. (1968). "The Tragedy of the Commons." Science **162**: 1243-1248.
Harper, J. (2004). RFID Tags and Privacy. World Data Protection Report. **4:** 19-24.
Harris Interactive (1999). IBM Multi-National Consumer Privacy Survey.
Hendershott, T. J., Ed. (2006). Economics and Information Systems (forthcoming). Handbooks in Information Systems, Elsevier.
Hermalin, B. E. and M. L. Katz (2005). Privacy, Property Rights & Efficiency: The Economics of Privacy as Secrecy. Unpublished manuscript, University of California at Berkeley. Berkeley, CA.
Hildner, L. (2006). "Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level." Harvard Civil Rights-Civil Liberties Law Review **41**(1): 133-176.
Hou, J.-L. and C.-H. Huang (2006). "Quantitative performance evaluation of RFID applications in the supply chain of the printing industry." Industrial Management & Data Systems **106**(1): 96-120.
Hughes, D., G. Coulson, et al. (2005). "Free Riding on Gnutella Revisited: The Bell Tolls?" IEEE Distributed Systems Online **6**(6).
Hui, K.-L. and I. P. L. Png (2006). The Economics of Privacy. Economics and Information Systems (forthcoming). T. Hendershott, Elsevier.
Hutto, J. and R. D. Atkinson (2004). Radio Frequency Identification: Little Devices Making Big Waves. Washington, DC, Progressive Policy Institute.
Jones, P., C. Clarke-Hill, et al. (2005). "The benefits, challenges and impacts of radio frequency identification technology (RFID) for retailers in the UK." Marketing Intelligence & Planning **23**(4): 395-402.
Juels, A. (2005). RFID Security and Privacy: A research Survey. Bedford, MA, RSA Security.

Juels, A., R. L. Rivest, et al. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer PRivacy. 8th ACM Conference on Computer and Communications Security, ACM Press.
Käarkkäinen, M. (2003). "Increasing efficiency in the supply chain for shrt sheld life goods using RFID tagging." International Journal of Retail & DIstribution Management **31**(10): 529-536.
Kang, J. (1998). "Information Privacy in Cyberspace Transactions." Stanford Law Review **50**: 1193-1294.
Karjoth, G. and P. A. Moskowitz (2005). Disabling RFID Tags with Visible Confirmation: Clupped Tags are Silenced. WPES '05, ALexandria, Va, ACM.
Kelly, E. P. and G. S. Erickson (2005). "RFID Tags: commercial applications v. privacy rights." Industrial Management & Data Systems **105**(6): 703-713.
Kobolev, O. (2005). "Big Brother on a Tiny Chip: Ushering in the Age of Global Serveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response." North Carolina Journal of Law & Technology **6**(2): 325-342.
Kranich, N. (2004). The Information Commons. New York, Brennan Center for Justice at NYU School of Law.
Ku, R. S. R. (2002). "The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance." Minnesota Law Review **86**: 1325-1378.
Kumaraguru, P. and L. F. Cranor (2005). Privacy Indexes: A Survey of Westin's Studies. Pittsburgh, PA, Institute for Software Research International, School of Computer Science, Carnegie Mellon University**:** 1-22.
Kurt Salmon Associates (2005). Moving Forward with Item-Level Radio Frequency Identification in Apparel/Footwear, Kurt Salmon Associates.
Landt, J. (2001). Shrouds of Time: The history of RFID. Pittsburgh, PA, AIM Global.
Leahy, P. (2004). The Dawn of Micro Monitoring: It's Promise, And Its Challenges To Privacy And Security. Video Surveillance: Legal And Technological Challenges, Georgetown University Law Center.
Lester, T. (2001). "The Reinvention of Privacy." The Atlantic Monthly.
Menard, S. (2002). Applied logistics regression analysis, 2nd edition. Thousand Oaks, CA, Sage Publications.
Milberg, S. J., H. J. Smith, et al. (2000). "Information Privacy: Corporate Management and National Regulation." Organization Science **11**(1): 35-57.
Murthi, B. P. S. and S. Sarkar (2002). "The Role of the Management Sciences in Research on Personalization." Review of Marketing Science Working Papers **2**(2).
National Conference of State Legislatures (2005). 2005 Privacy Legislation Related to Radio Frequency IDentification (RFID), National Conference of State Legislatures. **2006**. **http://www.ncsl.org/programs/lis/privacy/rfid05.htm**
Nicholson, W. (2002). Microeconomic Theory: Basic Principles and Extensions, Thomson Learning.
Noonan, G., M. Cheyne, et al. (2004). RFID in the Supply Chain: A Balanced View, AMCOR Australasia; Hewlett-Packard.
O'Connor, M. C. (2005a). Alien Drops Tag Price to 12.9 Cents. RFID Journal.

O'Connor, M. C. (2005b). IBM Proposes Privacy-Protecting Tag, RFID Journal. **2006**. **http://www1.rfidjournal.com/article/view/1972/**
Odlyzko, A. (2003). Privacy, Economics, and Price Discrimination on the Internet. ICEC2003: Fifth International Conference on Electronic Commerce, ACM.
Odlyzko, A. (2006). Comments on draft manuscript. G. Bitko.
OECD (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development.
O'Harrow, R., Jr., (2005). No Place to Hide. New York, Free Press.
O'Neil, D. (2001). "Analysis of Internet Users' Level of Online Privacy Concerns." Social Science Computer Review **19**(1): 17-31.
Perrin, S. (2005). RFID and Global Privacy Policy. RFID Applications, Security, and Privacy. S. L. Garfinkel and B. Rosenberg. Upper Saddle River, NJ, Addison-Wesley**:** 57-81.
Phelps, J., G. Nowak, et al. (2000). "Privacy Concerns and Consumer Willingness to Provide Personal Information." Journal of Public Policy and Marketing **19**(1): 27-41.
Posner, R., A (1978). "The Right of Privacy." Georgia Law Review **12**: 393-422.
Post, R. C. (2001). "Three Concepts of Privacy." Georgetown Law Journal **89**: 2087.
Prater, E., G. V. Frazier, et al. (2005). "Future impacts of RFID on e-supply chains in grocery retailing." Supply Chain Management: An International Journal **10**(2): 134-142.
Regan, P. (1995). Legislating Privacy. Chapel Hill, NC, University of North Carolina Press.
Regan, P. (2002). "Privacy as a Common Good in the Digital World." Information, Communication and Society **5**(3): 382-405.
Reidenberg, J. R. (1992). "Privacy in the Information Economy: A Fortress of Frontier for Individual Rights?" Federal Communications Law Journal **44**: 195.
RFID Journal (2003). US Military Clarifies RFID Mandate. **http://www.rfidjournal.com/article/articleview/608/1/1/**
Roberti, M. (2004). DOD Releases Final RFID Policy, RFID Journal. **2006**. **http://www.rfidjournal.com/article/articleview/1080/1/1/**
Roberti, M. (2005). Wal-Mart To Expand RFID Tagging Requirement, RFID Journal. **2006**. **http://www.rfidjournal.com/article/articleview/1930/1/1/**
Rose, E. (2001). "Balancing internet marketing needs with consumer concerns: a property rights framework." Computers and Society **31**(1): 17-21.
Samuelson, P. (2005). RFID Workshop - Comment, P049106. Federal Trade Commission Public Workshop: Radio Frequency Identification: Applications and Implications for Consumers.
Schneier, B. (2004). RFID Passports, Schneier on Security. **2006**. **http://www.schneier.com/blog/archives/2004/10/rfid_passports.html**
Schwartz, P. (1999). "Privacy and Democracy in Cyberspace." Vanderbilt Law Review **52**: 1609,1611,1633-1634.
Shah, R. C. and J. P. Kesan (2004). Old Wine in a New Bottle: RFIDs and Cookies. 2004 Telecommunications Policy Research Conference, George Mason University, George Mason University School of Loaw.

Sheehan, K. B. (2002). "Toward a Typology of Internet Users and Online Privacy Concerns." The Information Society **18**: 21-32.
Sheehan, K. B. and M. G. Hoy (2000). "Dimensions of Privacy Concern Among Online Consumers." Journal of Public Policy and Marketing **19**(1): 62-73.
Simmons, R. (2002). "From *Katz* to *Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies." Hastings Law Journal **53**: 1303-1358.
Slobogin, C. (2002). "Peeping Techno-Toms and the Fourth Amendment: Seeing Through *Kyllo*'s Rules Governing Technological Surveillance." Minnesota Law Review **86**: 1393-1438.
Smith, A. (2006). Keeping tabs on Viagra et al, CNNMoney.com. **2006**. **http://money.cnn.com/2006/01/26/news/companies/RFID/index.htm**
Smith, H. J., S. J. Milberg, et al. (1996). "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." MIS Quarterly **20**(2): 167-196.
Smith, R. E. (2000). Ben Franklin's Web Site: Privacy and Curiousity from Plymouth Rock to the Internet. Providence, RI, Privacy Journal.
Solove, D. J. (2002a). "Access and Aggregation: Public Records, Privacy and the Constitution." Minnesota Law Review **86**: 1137-1218.
Solove, D. J. (2002b). "Conceptualizing Privacy." California Law Review **90**: 1087.
Solove, D. J. and M. Rotenberg (2003). Information Privacy Law. New York, Aspen Publishers.
Spiekermann, S. and H. Ziekow (2005). RFID: A 7-Point Plan to Ensure Privacy. 13th European Conference on Information Systems, Regensburg, Germany.
Staff of the Federal Trade Commission (2005). Radio Frequency Identification: Applications and Implications for Consumers. Washington, DC, Federal Trade Commission**:** 1-48.
Stanley, J. and B. Steinhardt (2003). Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society. New York, NY, American Civil Liberties Union.
Sullivan, L. (2004). Cattle Trails. Information Week.
Tang, Z., J. Hu, et al. (2005). Protecting Online Privacy: Self-Regulation, Mandatory Standards, or Caveat Emptor. Working Paper, Carnegie Mellon University. Pittsburgh, Pa.
Taylor, C. R. (2002). Private Demands and Demands for Privacy: Dynamic Pricing and the Market for Customer Information. Durham, NC, Duke University**:** 1-30.
Taylor, C. R. (2004a). "Consumer Privacy and the Market for Customer Information." RAND Journal of Economics **35**(4): 631-650.
Taylor, C. R. (2004b). Privacy and Information Acquisition in Competitve Markets. Durham, NC, Duke University**:** 1-28.
Taylor, H. (2003). Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits, Harris Interactive.
Tucker, R. (2006). Self-Incrimination in the Supermarket Checkout Line. New York.
Ulph, D. and N. Vulcan (2000). Electronic Commerce and Competitive First-Degree Price Discrimination. London, University College.
US Department of Commerce (2000). Safe Harbor Overview, Department of Commerce. **2006**. **http://www.export.gov/safeharbor/sh_overview.html**

Varian, H. R. and C. Shapiro (1999). Information Rules. Boston, Harvard Business School Press.
Ware, W. (1977). Privacy-Handling Personal Data. Santa Monica, Ca, The RAND Corporation**:** 1-10.
Wathieu, L. (2002). Privacy, Exposure and Price Discrimination. Cambridge, Ma, Harvard Business School.
Weinberg, J. (2005). RFID, Privacy, and Regulation. RFID Applications, Security, and Privacy. S. L. Garfinkel and B. Rosenberg. Upper Saddle River, NJ, Addison-Wesley**:** 83-97.
Weiss, R. M. and A. K. Mehrotra (2001). "Online Dynamic Pricing: Efficiency, Equity and the Future of E-commerce." Virginia Journal of Law and Technology **6**(11).
Westin, A. F. (1967). Privacy and Freedom. Information Privacy Law. M. Rotenberg. New York, Aspen Publishers.
Westin, A. F. (1999). "Freebies" and Privacy: What Net Users Think, Opinion Research Corporation. Sponsored by Privacy & American Business. **http://www.privacyexchange.org/iss/surveys/sr990714.html**
Westin, A. F. (2001). Proceed: But With Great Care, and With Adequate Safeguards, Harris Interactive and Privacy & American Business. **2003**. **http://www.privacyexchange.org/iss/surveys/sept01harris.html**
Wyld, D. C. (2005). RFID: The Right Frequency for Government. Washington DC, IBM Center for the Business of Government.