

OLD WINE IN A NEW BOTTLE: RFIDS AND COOKIES

Rajiv C. Shah & Jay P. Kesan
University of Illinois at Urbana-Champaign

2004 Telecommunications Policy Research Conference
October 1-3, 2004
George Mason University School of Law

Correspondence:
Email: rshah@a5.com, kesan@law.uiuc.edu
Web: <http://www.GoverningWithCode.org>

OLD WINE IN A NEW BOTTLE: RFIDS AND COOKIES

The use of Radio Frequency Identification (RFID) technologies on consumer products is generating concerns over privacy. RFID tags are attached to physical objects and can maintain information about the item as well as aid in tracking the item. A potential nightmare scenario is that RFID tags in a book in your luggage or currency in your pocket could be used to identify you and track your movements, thus creating a new surveillance regime. In response to these privacy concerns, a number of public interest organizations led by the Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) and the Privacy Rights Clearinghouse have put forth guidelines for the consumer use of RFID technology (2003). These guidelines are based on a privacy framework known as the principles of Fair Information Practice (FIP). This paper also provides privacy guidelines, however the basis is the Recursive Regulatory Model for Technology (RRMT).

RRMT is not based upon privacy concerns, but is a more general theoretical framework for analyzing the interaction between technology and society. This permits scholars to analyze not only how technologies affect society, but also how society can influence technologies. The goal of RRMT is to provide a more rigorous treatment of the notions by Kapor that “architecture is politics” and Lessig’s “code is law” (Lessig, 1999). While policymakers recognize that technology affects societal concerns, they have little to guide them in analyzing technology. RRMT’s analytical framework allows scholars to assess how technologies regulate or influence a variety of societal concerns including privacy, freedom of speech, accessibility, and intellectual property protection.

RRMT was developed after analyzing several case studies, including the cookies technology developed by Netscape. This case study is of particular interest for RFID

technology, because cookies are the digital equivalent of RFID technology. Cookies are digital identifiers placed by web servers to identify users. RFID tags are identifiers placed by merchants to identify consumer goods. This striking similarity is useful when applying RRMT to RFID technology. While RRMT can provide recommendations for alleviating the privacy problems, the history of cookies provides a detailed description of why these recommendations are relevant and what may happen if they are not followed.

The paper begins with a section providing background on RFID technology and how it may affect consumer privacy. This section also summarizes the guidelines developed by several public interest groups on the use of RFID on consumer products. The second section shows how cookies are the digital equivalent of RFID technology. The third section provides a brief overview of the RRMT. The next three sections are based around the three important relationships with RRMT. Each of these sections offers recommendations for addressing privacy issues with RFID. The fourth section focuses on the development of RFID technology. The fifth section focuses on how individuals may use and modify RFID technology. The final section focuses on measures that society may take to influence RFID technology to better address privacy issues.

Background on RFID Technology and Privacy Concerns

Radio Frequency Identification (RFID) technology consists of a small computer chip capable of transmitting a small amount of information (Mayfield, 2002). RFID was originally developed in the 1940s and was first used to identify friendly aircraft during World War II. In the 1970s, the government used RFID for tracking livestock and nuclear material. Today, RFID is used in a variety of locations to identify things. For example, libraries use RFID to prevent

theft (Boss, 2004). Automatic toll collection systems, e.g., EZ-pass, depend upon cars with RFID tags, which can then be read as cars pass through a toll both.

RFID tags are small computer chips attached to objects. The tags hold a small amount of information, typically a serial number that identifies a product. The most common tags, the passive tags, can be read by an RFID reader from a range of about 20 feet. Another type of RFID tag, known as an active tag, contains batteries to broadcast a signal and therefore has a much longer read range. The technology most analogous to RFID tags is the bar code. It contains a small amount of information and is attached to products. The advantages of RFID over bar codes is its much longer read range and no requirement that the tag be within the line of sight of the RFID reader. This allows hundreds of RFID tags can be read within a second.

The advantages of RFID and the expected drop in price of RFID tags to 5 cents by 2006 is leading to its increased use for inventory management ("The Best Thing Since the Bar-Code," 2003). RFID is touted to lower supply chain costs, reduce theft and counterfeiting, and ensure better tracking of products whether they be cattle, drugs, or clothing. A number of entities from Wal-Mart to the Department of Defense are using RFID tags to trace the movement of goods (Gross, 2004). Because the tags currently cost around fifty cents apiece, tagging has been limiting to pallets of goods and not individual consumer items.

A number of public interest organizations led by CASPIAN have called for a moratorium on consumer use of RFID until a technology assessment is completed. Their concern is that RFID technology applied to consumer goods may "jeopardize consumer privacy, reduce or eliminate purchasing anonymity, and threaten civil liberties" (Consumers Against Supermarket Privacy Invasion and Numbering, 2003). In response, Linda Dillman, executive vice president and chief information officer of Wal-Mart, states that item level tagging, where individual

products are identified with RFID chips, is about 10 years away (Gross, 2004). Nevertheless, a number of companies, including Wal-Mart are now testing RFID on consumer products.

There are two main concerns regarding privacy by these public interest organizations. The first concerns how RFID tags and readers may be concealed from consumers. Tags can be attached or embedded into consumer goods so they are effectively invisible. Moreover, RFID readers may be concealed while in operation, because they have a maximum range of 10 to 20 feet. The result is that consumers would not know their possessions are storing information and leaking that information to third parties. These possessions could include pharmaceuticals, books, and currency.

The second concern with RFID tags is as American Civil Liberties Union's (ACLU) director of the Technology and Liberty program Barry Steinhardt suggests, RFID creates "a whole new surveillance regime" (Gross, 2004). RFID tags will likely have unique identifiers to represent the good it tags. By combining the RFID tag information with the sale of an item, a global registration system could be created in which every tagged object is identified and linked to its purchaser. A further concern is that this global registration system could then be aggregated with other personally identifiable data creating enormous profiles of individuals' habits and possessions. Moreover, this data could then be used to identify and track people. For example, RFID readers could identify items and therefore people at a political rally, thus allowing for a whole new surveillance regime.

A public interest groups as well as scholars have put forth the following guidelines for RFID guided by the principles of FIP (Consumers Against Supermarket Privacy Invasion and Numbering, 2003; Eschet, 2004). The principles of FIP are based upon principles of notice, choice, access, security, and enforcement. One source of FIP comes from the Organisation for

Economic Co-operation and Development's (OECD) Privacy Guidelines. This reliance on overarching principles of privacy is not surprising, because these groups are seeking more general privacy legislation and are not solely focused on the RFID issue.

The first principle put forth for RFID use is openness. Retailers should make public how they will use RFID technologies. Consumers must be informed and there should be not surreptitious reading of RFID tags. Second, is purpose specification, which means RFID consumers must be notified of the purpose of RFID tags and readers. Third, the collection of information should be limited to the purpose at hand. Fourth, RFID users should be held legally accountable to ensure implementation and the collected data are handled according to these principles. Fifth, there must be security safeguards that are verified by outside third parties. These security safeguards concern the transmission and storage of a persons' information.

The guidelines also state the following should be prohibited. First, merchants can't force consumers into accepting RFID tags. Second, consumers must be allowed to detect and disable tags. Third, RFID must not be used for tracking of individual movements. Fourth, RFID should not be used to eliminate or reduce anonymity, e.g, incorporating RFID tags into currency.

The guidelines offered by the public interest groups are sensible. They follow from the larger framework on privacy, FIP, that the public interest groups support. Indubitably, these guidelines will form the basis of most discussion concerning privacy issues for RFID technology. While this is one approach, the remainder of this paper develops guidelines based upon a more general analysis of the RFID technology. This analysis is based upon RRMT. The next section shows how RFID technology is analogous to the cookies technology.

Cookies and RFID: Old Wine in a New Bottle

This paper argues that cookies are a similar technology to RFID, so that lessons from the history of cookies can be applied to RFID technology. This section argues that cookies are an excellent analog for RFID in ways that other technologies that affect privacy are not. These other technologies could include supermarket loyalty cards, biometrics, e.g, fingerprints, video surveillance, monitoring computer use, wiretapping, social security numbers, national ID cards, digital rights management, and caller-id.

First, both cookies and RFID technology allow either web sites or retailers to maintain information on their users or customers. Both technologies place unique information on either the person's computer or their purchased item. The unique information is analogous to a serial number for identifying users and their products. In the case of cookies, web sites place information on a user's computer, which can uniquely identify them and track their movements across a web site. The cookies technology gave the web a memory and without cookies web sites would not be able to maintain persistent information on their users. Similarly, RFID tags allow for the unique identification of physical objects. In the past, retailers had information from either a label or bar code uniquely identifying a product, e.g., box of Gillette razors, but could not uniquely identify each individual razor. RFID tags allow Gillette to place a unique serial number on each razor.

Second, both of these technologies are ubiquitous. They can be placed by anyone anywhere for increasingly little cost. In the case of cookies, they can be set by any web site for virtually no cost. Nowadays, most web sites place cookies on a person's computer. RFID tags can be placed upon or embedded in any physical object that consumers purchase. RFID tags are

expected to become very cheap, as little as a few cents, in the next few years. As RFID tags drop in price, they will likely appear on more and more products.

Third, the information contained within cookies and RFID tags can foster the profiling of individuals. After all, a serial number can be processed by computers and easily linked to other online databases. In the case of cookies, web sites can keep detailed records on how often and where a person goes within a web site. Moreover, because of the privacy flaw of third party cookies, companies such as DoubleClick, can aggregate this information across multiple web sites. This allows for detailed profiles of an individuals online activity. These online profiles can then be linked to offline data, such as catalog sales, to create massive profiles of consumers. In the case of DoubleClick, they agreed to not combine such information after intense public pressure. As the previous section discussed, there are the exact same privacy concerns with RFID. RFID technology can also foster the creation of online profiles by maintaining unique serial numbers that can be linked to other databases.

Fourth, the information within these technologies can be accessed and revised surreptitiously. For some time, people were not informed that cookies were maintaining information on their web surfing behavior. This was easily accomplished, because the cookies technology was not made apparent to users. However, newer web browsers incorporated cookie management tools and users can now prevent surreptitious use of cookies. RFID technology can also be used surreptitiously. Both the tags and readers can be hidden from view and can operate without consent.

The Recursive Regulatory Model for Technology

The Recursive Regulatory Model for Technology (RRMT) is a theoretical framework for understanding how technology regulates. This model is largely based upon Giddens

structuration theory with some insights from Actor-Network Theory. The model strives to understand the relationship between technology and people. Specifically, how technology affects individuals, but also how individuals affect technology. This theory was developed to assist scholars and policymakers striving to understanding how technologies regulate. The issue of technology regulating individuals has been brought to the forefront within telecommunications policy, as these technologies can affect a variety of fundamental societal concerns, such as privacy, e.g., cookies, and intellectual property rights, e.g., digital rights management.

Structuration theory provided the inspiration for RRMT, however structuration theory has its limitations in understanding how technologies regulate. Structuration is a leading social theory that captures the dynamic relationship between individuals and structures. Structuration argues against social and technological determinism. Instead, the relationship between people and technology is a combination of technology enabling users, while also constraining users. This is an accurate and widely agreed account of how technology operates. One area it has been successfully applied is analyzing how communication technologies interact with organizations (Orlikowski, 1992). However, structuration does not provide the analytical tools to move beyond this enable/constrain relationship. It does not contain the necessary concepts, frameworks, or relationships to provide a fine grained analysis of the interaction between people and technology (Monteiro & Hanseth, 1995). These criticisms are recognized within the field. Recently, Orlikowski and Iacono concluded that scholars need to better theorize the information technology artifact and move beyond the simple enable/constrain distinction (2001).

RRMT also relies upon concepts from Actor Network Theory (ANT). ANT is another approach for understanding the relationship between technology and society. ANT has

developed into a widely used descriptive framework for studying how technology operates. In this context, ANT considers and provides concepts for analyzing why technology regulates in a particular manner, identifying key actors, and examining the malleability of technology. However, ANT suffers from two distinct problems. First, ANT's analytical framework does not have a place for persistent macro level concepts, such as institutions. ANT holds that every technology must be studied in its own context. As a result, high-level concepts, such as institutions, are inapplicable. However, a variety of scholars studying communication technologies have found an institutional unit of analysis valuable (Agre, 1999; Fountain, 2001; Schmidt & Werle, 1998). Secondly, ANT is a descriptive theory and provides little analytical and normative guidance. While useful for analyzing how a technology developed, it doesn't provide a general framework to study how technology develops.

The elements of the RRMT consist of institutions, individuals, and technology as shown in Figure 1. RRMT recognizes a recursive relationship between society and technology. This is then analyzed in three separate stages. The developing technology stage argues that institutions are central to understanding how technology is produced. Institutions are intermediate social actors with origins in social rules and interactions. Technology regulating and reconfiguring technology stage considers how technology constrains and facilitates certain types of actions by inscribing norms and values inscribed into technology. It further recognizes the individuals have agency in deciding whether to use technology, that individuals may use technology in unanticipated ways, and that individuals can modify technology depending upon its durability. The last stage concerns how humans can act individually or collectively to influence the development of technology. This may include actions such as consumer pressure through the market or government regulation.

RRMT uses a technology-oriented perspective to examine how technology develops, interacts with individuals, and how technology is shaped by those interactions. RRMT is indifferent to any specific societal concern. Instead, RRMT accepts that there are many different social and technical values embedded into technologies. Moreover, individuals and society can influence how these values are embedded into technologies. As a result, RRMT can provide practical guidelines for assessing how a technology operates as well as recommendations to foster specific societal concerns. In the next three sections, RRMT provides insights for addressing consumer privacy uses with RFID technology.

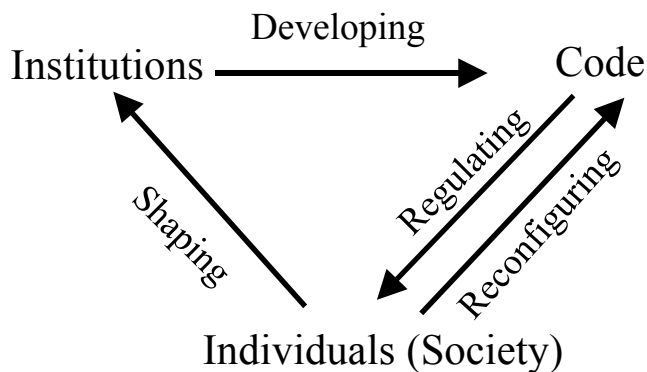


Figure 1. Recursive Regulatory Model for Technology

Developing

RRMT recognizes that institutions play a central role in the development of technologies, because they mediate how values are inscribed into technology. Developers work within institutions, and these institutions favor certain values over other and inscribe them into technology. The inscription process refers to how beliefs, norms, motives, values, biases, and political prejudices are incorporated into the technology. The inscription process has been described by philosophers of technology (Feenberg, 1991; Winner, 1985), and documented in

communication technologies (Flanagan, Farinola, & Metzger, 2000; Friedman, 1997; Introna & Nissenbaum, 2000).

The first part of the RRMT analysis considers the role of institutions in the development process. There are many different institutional sources for technologies. In the case of RFID technology, firms have done virtually all of the research.¹ Firms are concerned with how best to exploit this technology reliably and cost effectively. Not surprisingly, there is little research or scholarship on consumer privacy issues. To foster such thinking, policymakers should provide incentives for research and experimentation by universities and hobbyists on privacy issues. This work could lead to new ideas and methods for ameliorating RFID privacy issues as well as identifying previously unforeseen issues.

The development of cookies was similar to RFID in that firms led the initial development. However, university research funded by the National Science Foundation (NSF) as well as Mozilla open source project have lead to concrete improvements for consumer privacy by leading and accelerating the development of cookie management tools. These tools provide users with the ability to better manage the privacy and security issues with cookies. Specifically, they allow users to understand what cookies are, notify them when cookies are being use, and provide them to control cookies by web site. The control by web sites allows users meaningful control over their privacy by deciding which cookies may store information about them and which cookies should be purged.

The second part of the RRMT analysis acknowledges that technical attributes of technology are malleable. These attributes include features such as open standards, intellectual

¹ The research was actually accomplished through a consortium, the Auto-ID Center, of which MIT was a members. The work was accomplished in collaboration with several firms, including Coca-Cola, Gillette, Target, Home Depot, and Wal-Mart. The purpose of the center was to develop standards and specifications for RFID implementation (Gilbert, 2003).

property protection, documentation, and usability. In assessing RFID technology, one characteristic that must be emphasized is open standards. The rationale for open standards comes from two sources. First, security experts are largely of the opinion that more open a design is, the more secure and hence more privacy favoring is a technology. Simply put, experts do not favor “security by obscurity”, and instead support public scrutiny or peer review of technologies with privacy implications (Mercuri & Neumann, 2003).

The second rationale for open standards emerges from the case study of cookies. Cookies were a technology rapidly developed within Netscape. The standard was not an open standard initially and was not peer reviewed. This proved fatal, because there were flaws in the cookies standard, which permitted the use of third party cookies. This refers to third parties being able to set and read cookies that the user would not expect to set cookies to set cookies. These third parties, most notably DoubleClick, could then develop profiles of online user activity across multiple web sites. This was the most significant privacy flaw in cookies and also one that could have been prevented if cookies were subject to peer review.

To prevent similar flaws, RFID technology should be based upon open standards. If there are objections to open standards, policymakers should still urge developers to have their standards reviewed by security experts privately. If RFID technology is not scrutinized, it is foreseeable that there will be latent security flaws, which will later be discovered. Open standards will not prevent all security problems, but it is a reasonable precaution to limit flaws, especially considering the potential impact of RFID on privacy.

The third part of RRMT analysis recognizes that social values, such as privacy, can be inscribed into technologies. After all technologies are not value-neutral, but can favor or foster certain values. Consequently, privacy is a crucial part of the design of RFID technologies,

whether or not it is publicly admitted. Policymakers need to emphasize to the designers of RFID technology that they need to consider privacy. This forces designers to more seriously consider privacy issues when designing technologies. Some issues for designers include limiting information in RFID tags and preventing third parties from accessing information in tags surreptitiously. Designers can anticipate these issues by considering how RFID tags can prevent third parties from accessing information. This could include designing limits to the transfer of information, allowing consumers to modify the tags, blocking radio frequency access to the tags, or killing the tags to ensure the information is unusable.

This recommendation follows from the history of cookies in which Netscape designed in privacy limitations into cookies. The foremost concern of Netscape was to limit access by third parties to the cookies data, because of the privacy concerns. This led them to limit read/write access for cookies to the web site that placed the cookies. This would ensure that third party web sites could not access cookie data. While a loophole was later found, Netscape did try to design in limitations to third party access. Additionally, Netscape included an expiration date and limited the amount of information that could be stored to address privacy issues. Similarly, if RFID designers can implement meaningful measures to protect privacy, this can alleviate the concerns of these public interest groups and limit governmental involvement.

Regulating and Reconfiguring

The next part of the RRMT analysis focuses on how technology regulates, but can also be reconfigured. This work recognizes that to understand how technology regulates, it is necessary to examine the inscriptions placed in technology. However, there is a recursive element here. While technology affects individuals, individuals can affect technology by reconfiguring

technology. As a result, one cannot understand how technology regulates without studying its interaction with individuals.

Users also play a crucial role in how technology regulates. They can decide whether to use a technology, how to use a technology, and whether to try to modify the technology.

Scholars have repeatedly shown that users do not always use the technology as intended by developers. The history of communication technologies is full of examples of how unanticipated uses, such as the use of the telephone for personal use by women (Fischer, 1992). Although developers inscribed a technology with norms and values, this doesn't mean it will be used in that manner. Orlikowski synthesizes past research in recognizing that "through error (misperception, lack of understanding, slippage) or intent (sabotage, inertia, innovation), users often ignore, alter, or work around the inscribed technological properties" (Orlikowski, 2000, 409).

The ability of technology to influence societal concerns, such as privacy, is mediated by a number of factors including the design of the technology and the response of users. The first key issue is whether users are informed about a technology. If users are uninformed they can't reconfigure the technology. Therefore, we recommend that consumers be notified of RFID use, which means no surreptitious use of RFID. RFID technology should not be concealed, instead retailers should be open and state the benefits associated with RFID technologies. If consumers understand the benefits, they are much less likely to object to privacy intrusions.

The issue of notification occurred with the development of cookies by Netscape. Netscape stealthily implemented cookies in their first web browser released in 1994 in four ways. First, Netscape turned the feature on by default without notifying or asking the consent of users (Millett, Friedman, & Felten, 2001). Secondly, there was no notification mechanism to

alert people when cookies were being placed on their computer. Users did not know that information about them was being saved. Third, the cookies technology was not transparent. Examining a cookies file provides no information about what is stored in the cookie file. Fourth, there was no documentation available that explained what cookies were and their privacy implications.

It was not until early 1996 that the public became aware of cookies. The *Financial Times* broke the story on February 12, 1996 with an article on cookies and privacy (Jackson, 1996). This was followed by a story the next day in the United States, “Web ‘Cookies’ May Be Spying on You” (Gomes, 1996). The article immediately drew attention to cookies and resulted in a great uproar over the use of cookies. Over the next few years, cookies became one of the top Internet privacy issues, largely because people were scared and afraid of cookies. Cookies were blamed for all sorts of computer and privacy issues, largely because people felt they didn’t understand them and information about them was being concealed. To prevent a similar chain of events, it is important that users be informed of the privacy issues and not feel like they are being spied upon.

A crucial part of RRMT concerns how individuals can reconfigure technologies. Reconfiguration can occur in several ways including when individuals have a choice in using a technology, individuals use the technology in unintended ways, and when individuals modify the technology. The first way individuals can reconfigure a technology is by choosing whether to use the technology. This leads to the suggestion that individuals be able to purchase a variety of consumer goods without having to accept RFID technologies. Otherwise, they are effectively being coerced into using RFID technologies. In reality, this proposal is rather Pollyannaish. If RFID tags have substantial cost benefits, they will likely be on all consumer products just like

bar codes, despite the privacy concerns of a few people. Just as web sites did not back down using cookies, it is unlikely that retailers will not use RFID tags in consumer items. Moreover, RFID tags are likely to be mandated in certain products such as pharmaceuticals for safety reasons. Thus the key privacy issue is not whether consumers have a choice, but how consumers can control or reconfigure RFID tags to address their privacy concerns. After all, if consumers can't reconfigure RFID technologies, they are truly being regulated by RFID technology and are at the mercy of retail outlets. In such a case, the only solution would be to look for governmental involvement to ensure the privacy of consumers is not violated.

Reconfiguration of RFID tags allows consumers to manage the privacy intrusions and will lead to fewer concerns over the privacy issues. An example of reconfigurability is RFID tags that can be modified. This can ensure that privacy sensitive information can be removed or modified. The modification could occur either at the time of purchase by the retailer or at a later time by the end user. In the case where merchants would like to maintain information on the tag to aid their customers in the future, the information could be modified to not use publicly available identifiers. The scenario we are addressing is when you go into the Hilfiger store that detects your RFID tagged Armani underwear and tries to sell you a pair of their underwear. While it may be useful to keep the tag in the Armani underwear, individuals should be allowed to ensure such information remains private. This suggests the need for reconfigurable RFID tags in consumer products, especially in products where RFID tags are not removable.

A final method of reconfigurability is the destroying or killing of RFID tags. This could be done either through removal of the tag or destruction of the tag. RFID tags could be placed on or in an easily removable component that is prominently identified. This would permit individuals to remove tags. Other approaches could include tags that can be neutralized by

consumers or at the retailer's point of sale. The number of technological approaches is varied, but all of these allow consumers to ensure that the RFID tags no longer carry useful or usable information.

This history of cookies shows how reconfigurability alleviates privacy concerns. The privacy concerns over cookies were at the height when cookies were impossible or difficult to manage. However, as browsers began developing tools for individuals to manage cookies, the privacy concerns ebbed. These tools allow individuals to decide what cookies they should accept and how long that information should be preserved. Nowadays, cookies have receded as a privacy issue simply because individuals have the tools to manage cookies.

Shaping

RRMT recognizes that society can react to technologies by prompting developers to remove, modify, and create new versions of technologies. After all, the development of technology is partially influenced by society. This part of RRMT concentrates on methods society can use to ensure technologies to comport with societal goals. Its goal is to highlight all the options available to society to shape technology, while also noting pertinent regulatory and technological issues (Kesan & Shah, forthcoming).

RRMT offers a number of methods for incorporating societal concerns in technology. Viewing this from a cost benefit standpoint, the ideal solution for consumer products is to rely on market forces to incorporate specific societal concerns into technologies (Harper, 2004). However, societal concerns may not be incorporated into technologies because of market failures (Shah & Kesan, 2003). In these cases policymakers need other options.

RRMT provides a range of options from informing consumers, pressuring developers through the bully pulpit, to government regulation. Each of these measures has costs and benefits associated with it. A first step for addressing market failure is to cajole firms and inform consumers into considering societal concerns. Privacy is an example of a societal concern that public interest groups and government have attempted to pressure firms into, while ensuring consumers were informed.

In the case of cookies, cookie management tools were eventually developed because of pressure from government, privacy advocates, and the open source movement, and not consumer pressure. This point is significant because the introduction of cookies management tools was not solely because of consumer demand. First, the changes appeared to be led by the legal department and not the marketing department. Unlike other features of web browsers, there has been no marketing of these improved cookie management tools. The implication is that Netscape didn't think consumers desire these features. Second, the implementation of these features involved hiding them behind complex menus with little documentation. This suggests these features were not meant for everyday users, but rather to show regulators and privacy advocates that Netscape was complying with their demands. Third, the slow gradual development of these tools reflects how Netscape felt it was being pushed to implement these features. The features are not technologically complex and could have been included in their full form initially. Instead, Netscape decided to slowly introduce these features ensuring users had to wait several years before they have meaningful control over cookies.

Ideally, RFID technologies will be privacy sensitive because of market pressure. However, it is likely that a market failure will occur for RFID technologies as it did for cookies. This will lead to the inclusions of public interest groups and government into the debate.

Policymakers should foster this debate if market forces are not adequately addressing privacy concerns. As cookies shows, congressional hearings and reports from public interest groups can influence the development of RFID technology!

A final recourse for influencing RFID technologies is government involvement. Some obvious ways government can influence the development of RFID include fiscal measures, such as funding research into privacy issues, or by using government's procurement power to stimulate privacy sensitive approaches to RFID. A more stringent measure may be relying on government regulation to ensure RFID technologies to not violate consumer privacy. This article does not address the multitude of ways government can act or the costs of these actions. Instead, this article seeks to point out that RRMT provides policymakers with schematic for incorporating societal concerns, such as privacy, into technologies.

Discussion

The debate around RFID has largely rested upon the FIP. FIP contains a number of principles to guide actions towards technologies that affect privacy. These principles are based upon philosophical principles of human rights and include notice, choice, access, security, and enforcement. These principles provide clear guidance for the guidelines for consumer use of RFID. Table 1 contains the guidelines proposed by CASPAIN, which are derived from the FIP.

The principles behind RRMT are not founded on philosophical principles of human rights, but rather on how a technology develops, changes, and affects individuals. The three key analytical distinctions are based around the development of a technology, how a technology interacts with individuals, and how individuals can influence the development process for a

technology. From these three areas, a number of guidelines for the consumer use of RFID technology were developed as summarized in Table 1.

Table 1. Summary of Recommendations for RFID & Consumer Privacy

#	FIP	RRMT
1		Support R&D
2	Openness	Users should have notice of RFID
3	Purpose specification	
4	Collection limitation	
5		Designers should consider privacy in their design
6	Accountability	
7	Security safeguards for information	Encourage open standards (to identify security flaws)
8		
9	Choice for consumers	Choice for consumers
10	Allow the detection & disabling of RFID	Allow the detection & disabling (reconfiguring) of RFID
11	No tracking with RFID	
12	RFID should not affect anonymity	
13		Maintain pressure from privacy groups
14		Encourage government involvement

The recommendations in Table 1 place similar recommendations side by side. This was done to show areas where FIP and RRMT were similar and dissimilar. Some areas of agreement revolve around notions that individuals should have notice (#2, #3), choice (#9), and the ability to reconfigure RFID technologies (#10).

FIP and RRMT had a number of related recommendations that differed in emphasis. FIP focuses on information, while RRMT focuses on the technology. For example, concerning security (#7), FIP focuses on safeguards for the information, while RRMT's emphasizes developing secure technology. Similarly, while FIP favors collection limitations for information

(#4), RRMT focuses more on encouraging designers to incorporate limitations directly into the technology (#5).

A number of recommendations differed drastically between FIP and RRMT. RRMT did not emphasize issues of enforcement (#6) or specifically limiting how RFID in some circumstances, e.g. whether RFID technologies should be used for tracking individual movements (#11, #12). RRMT did emphasize the malleability of technology with recommendations concerning the role of research and development (#1), the role of designers in embedding privacy in RFID technologies (#5), and the role of public interest groups and government in influencing the development of RFID technologies (#13, #14). As a result, RRMT provides policymakers with recommendations for fostering privacy in technologies.

In sum, both approaches provide policymakers with key recommendations for protecting consumer privacy. The recommendations both emphasize issues of notice, choice, and reconfigurability. However, FIP and RRMT do diverge in other areas. FIP's recommendations focus on information, while RRMT's recommendations on technology. This difference can be seen in RRMT's acknowledgement of the malleability of technology, which leads to recommendations for how best to shape technology.

Conclusion

The goal of this paper was two-fold. First, we sought to present some concrete guidelines for consumer use of RFID technology, based on the history of cookies. After all, cookies are the digital equivalent for RFID technologies. Both technologies can maintain information, are ubiquitous, foster profiling, and allow surreptitious use. The privacy issues with cookies concerned notice, choice, and the sharing of consumer data. This paper discusses why these

issues occurred and how they were addressed. This history is extremely useful and relevant for users of RFID technologies seeking to placate fears over privacy.

The second goal was to show the value of RRMT in analyzing technologies that affect societal concerns. RRMT analyzes how technologies affect individuals from the perspective of policymakers. This analysis consists of three separate parts: the development of a technology, how a technology regulates individuals and how individuals reconfigure a technology, and how individuals can work together to influence the development of a technology. This analysis does not focus on one specific societal concern, such as privacy, but instead can consider a variety of societal concerns, such as the freedom of speech, accessibility, or intellectual property protection.

The ability of RRMT to address a variety of societal concerns stands in contrast to conventional approaches. In the case of RFID, the analysis and recommendations offered by scholars and policymakers were based around the principles of Fair Information Practices (Consumers Against Supermarket Privacy Invasion and Numbering, 2003; Eschet, 2004). RRMT offered a number of recommendations that were similar to those from an FIP analysis. The most striking difference was RRMT's emphasis on the malleability of technology, which FIP does not address. RRMT also has the added benefit of being useful in other contexts besides privacy, unlike FIP.

In sum, this paper has showed how the lessons from cookies can aid our understanding of the privacy issues with RFID technology. Additionally, this paper has served as a vehicle for illustrating a new theoretical approach to understanding and analyzing how technologies regulate.

References:

- Agre, P. E. (1999). The Architecture of Identity: Embedding Privacy in Market Institutions. *Information, Communication and Society*, 2(1), 1-25.
- The Best Thing Since the Bar-Code. (2003, August 8). *Economist*, 366, 72.
- Boss, R. W. (2004, May 14). *RFID Technologies for Libraries*. Retrieved August 24, 2004, from <http://www.ala.org/ala/pla/plapubs/technotes/rfidtechnology.htm>
- Consumers Against Supermarket Privacy Invasion and Numbering. (2003, November 20). *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*. Retrieved August 16, 2004, from <http://www.privacyrights.org/ar/RFIDposition.htm>
- Eschet, G. (2004). Adapting Fair Information Practices to Radio Frequency Technology (Draft). *SSRN*.
- Feenberg, A. (1991). *Critical Theory of Technology*. New York: Oxford University Press.
- Fischer, C. S. (1992). *America Calling, A Social History of the Telephone to 1940*. Berkeley: University of California Press.
- Flanagan, A. J., Farinola, J. M. F., & Metzger, M. J. (2000). The technical code of the Internet/World Wide Web. *Critical Studies in Media Communication*, 17(3), 409-428.
- Fountain, J. E. (2001). *Building the Virtual State: Information Technology and Institutional Change*. Washington, DC: Brookings Institution.
- Friedman, B. (1997). *Human Values and the Design of Computer Technology*. Stanford, CA: CLSI Publications.
- Gilbert, A. (2003, October 23). MIT Winds Down Radio Tag Activity. *CNET News.com*.
- Gomes, L. (1996, February 13). Web 'Cookies' May be Spying on You. *San Jose Mercury News*.
- Gross, G. (2004, July 14). RFID Users Say No Privacy Law Needed. *Network World*.
- Harper, J. (2004, June 21). RFID Tags and Privacy: How Bar-Codes-On-Steroids Are Really a 98-Lb. Weakling. *CEI OnPoint*.
- Introna, L., & Nissenbaum, H. (2000). Defining the Web: The Politics of Search Engines. *IEEE Computer*, 33(1), 54-62.
- Jackson, T. (1996, Feb. 12). This Bug in Your PC is a Smart Cookie. *Financial Times*.
- Kesan, J. P., & Shah, R. C. (forthcoming). Shaping Code. *Harvard Journal of Law & Technology*.
- Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

- Mayfield, K. (2002, May 20). Radio ID Tags: Beyond Bar Codes. *Wired News*.
- Mercuri, R. T., & Neumann, P. G. (2003). Security by Obscurity. *Communications of the ACM*, 46(11), 160.
- Millett, L., Friedman, B., & Felten, E. (2001). *Cookies and Web Browser Design: Toward Realizing Informed Consent Online*. Paper presented at the Conference on Human Factors in Computing Systems.
- Monteiro, E., & Hanseth, O. (1995). Social Shaping of Information Infrastructure: On Being Specific About the Technology. In W. Orlikowski, G. Walsham, M. R. Jones & J. I. DeGross (Eds.), *Information Technology and Changes in Organisational Work* (pp. 325 - 343): Chapman & Hall.
- Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organizational Science*, 3(3), 398-427.
- Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organizational Science*, 11(4), 404-428.
- Orlikowski, W. J., & Iacono, C. S. (2001). Desperately Seeking the "IT" in IT Research--A Call to Theorizing the IT Artifact. *Information Systems Research*, 12(2), 121-134.
- Schmidt, S. K., & Werle, R. (1998). *Coordinating Technology: Studies in the International Standardization of Telecommunications*. Cambridge, MA: MIT Press.
- Shah, R. C., & Kesan, J. P. (2003). Incorporating Societal Concerns into Communication Technologies. *IEEE Technology and Society Magazine*, 22(2), 28-33.
- Winner, L. (1985). Do Artifacts have Politics? In D. MacKenzie & J. Wajcman (Eds.), *The Social Shaping of Technology* (pp. 26-38). Milton Keynes, England: Open University Press.