ITRI

INFORMATION TECHNOLOGY RESEARCH INSTITUTE

WORKING PAPER SERIES

ITRI-WP113-0608

The Politics of RFID – The Issues

Issued: 06.05.2008

UNIVERSITY of ARKANSAS 1871

SAM M. WALTON COLLEGE of BUSINESS

INFORMATION TECHNOLOGY RESEARCH INSTITUTE

University of Arkansas
Fayetteville, Arkansas 72701
http://itri.uark.edu

THE POLITICS OF RFID:

THE ISSUES

Donald R. Kelley

Director, Fulbright Institute of International Relations

University of Arkansas

Prepared for the RFID Research Center of the Sam M. Walton College of Business
at the University of Arkansas

RFID AS A POLITICAL ISSUE

RFID technology is beginning to enter the political arena. In 2006, seventeen states considered RFID-related legislation, and the European Union created a commission to make recommendations on possible future regulation. As with all new technologies that hold widespread implications for the way we do business and live our lives, it will be perceived by some as a helpful addition to the toolbox of social technologies that permit us to become more efficient and by others as a threat to values and entitlements that are dearly held. And as with all such issues that touch intimately on our lives, it will end up in the political arena.

There is nothing new in this process, except of course, for the unique character of the RFID technology. To belabor the obvious, every new technology or reorganization of the way we manage our lives has been met with its advocates and skeptics who have offered us pictures of a future reality vastly improved or profoundly corrupted by the new tricks we have learned.

The goal of this white paper, and of a subsequent effort entitled *The Politics of RFID: Implementation*, is to look at the emerging debate about RFID technology as a political issue. The focus is not on the technology per se, but rather on how the technology and its broader economic and social ramifications will be comprehended and dealt with in the political arena. To foreshadow the argument, understanding the *politics* of RFID technology will depend on recognizing four realities:

1. The first reality is that we already know a lot about how issues enter the public arena, and that understanding will help us to forecast the possible scenarios through which RFID will reach the public stage, and what will happen when it gets there;

2. The second reality is that this will be a global process, occurring both in advanced industrial economies but also in less advanced labor-intensive manufacturing economies, and that the cultural diversity of these very different nations will have an impact on how the technology is applied;

3. The third reality is that many very different political issues will be raised by RFID deployment. For some, it will evoke a debate about privacy and individual rights, while for others the debate will focus on the environment, or job security, or religion, or public health. It would be a potentially dangerous mistake not to recognize and prepare for these very different issues; and

4. The fourth reality is that the political game is never over. Once policy has been made, it must be implemented, usually by regulatory agencies with considerable discretionary power that substantively affects the outcome. In a very real sense, the struggle over applying the rules is as political as the battle over making them,

and in policies, the fat lady never sings. This final issue is the focus of a subsequent white paper entitled *The Politics of RFID: Implementation.*

How an Issue Becomes an Issue

While it is inevitable that RFID technology will become the focus of public debate, and that the debate will shape both public attitudes and the legislative and regulatory environment in which that technology is put to use, *how* this occurs is not predetermined. And *how* RFID enters the political arena, how the debate over its utilization and broader social implications is defined, and how the rules of engagement of the political struggle that will determine its fate are set, will determine the outcome of the struggle.

How do we understand these political realities? What questions do we ask, and to whom do we turn for advice and counsel on political issues that go beyond the laboratories in which the technology was developed or the corporate headquarters attempting to apply it? For some, RFID technology is a question of more efficient management; it can be used to improve supply chains, strengthen public security in an increasingly threatening world, improve medical procedures, and the like. But for others, that same technology is seen primarily as an intrusive threat to their privacy, as a question of labor relations and job security, as a threat to the environment, or as negation of certain aspects of their religious beliefs. And in the global economy of today's world, how do the values of different cultures affect their responses to RFID technology and its broader social implications?

None of this is new to students of public policy. Like all social scientists, they have looked for patterns and commonalities in what they call "agenda setting" on a wide variety of issues. Their studies suggest that we can anticipate and perhaps shape how RFID technology becomes a political issue, and in doing so, affect the outcome of the debate. What these students of agenda setting do clearly tell us is that there is a "policy window" which gives us, as well as all other interested parties, the opportunity to define the issues in ways friendly to our cause and shape the debate that follows.[1]

RFID technology has several unique features that will affect how it passes through this "policy window".

First, the technology itself is new and relatively unique. While there are analogies to earlier technologies like bar coding, RFID raises new issues in terms of its broader social implications. Moreover, it is at best only partially understood by most policy makers and the public at large, although recent surveys suggest that increasing the level of technical information about how it works tends to reduce skepticism and hostility. Most importantly for our purposes, the very newness of the issue creates a situation in which both proponents and critics must compete for public attention, each trying to put its own spin on the question.

Second, there are competing perspectives on how to comprehend RFID technology. Each side of the debate is trying to write its own ending to the sentence, "RFID technology is really a question of …." If the last words are "efficiency" or "safety," then the debate will be framed in terms of its best application toward those ends. But if the ending reads "an invasion of my privacy," or "the loss of jobs to the next wave of automation," or "the question of environmental quality," or "a direct violation of God's will," then the technology will be rejected because of the collateral damage it wreaks in areas far removed from its intended purpose.

The third feature is closely linked to the second. Students of agenda setting speak frequently of the association of new issues with what they term "core values," meaning the things that we judge to be most important. Clearly many of the alternative endings to the sentences above contain such core values: privacy, job security, the environment, and religion. The more intensely the debate involves such core values, the more heated the political struggle and the less likely that compromise will emerge easily. Policy making – politics – is not just about majorities and minorities; intensely committed minorities frequently carry the day against irresolute or weakly committed majorities.

Agenda Setting as a Political and Social Process

As is always true in politics, there is more than one way to set an agenda. Analysts traditionally speak of three scenarios through which agenda setting occurs, each evoking a different passage through the policy window, and each biased toward a particular outcome in the struggle.

From the perspective of the RFID community, it is important to understand that these scenarios will shape the regulatory environment within which the rollout of the technology will occur. In the American and European contexts, it seems likely that the "insider access" scenario described below will prevail, probably producing compromise policies in which all stakeholders have had some input. But that could change, either because the complex process of consultation breaks down, or because events change the way in which RFID issues are perceived.

One scenario casts the government in the dominant role in setting the agenda for policy debate and serving as the critical gatekeeper who decides what issues emerge and how they are conceptualized. Clearly that scenario does apply in many nations, but certainly not in the United States or the European Union, where the debate over RFID is most intensive. The exception, especially in the American case, has occurred and may again occur when some overriding national priority such as public security temporarily permits the government to play a greater role in setting the public agenda. Such dominance is usually short-lived and subject to revision as critics become more articulate and as a once dominant issue such as public security declines in salience and is joined by other issues – privacy, for example -- claiming equal priority.[2]

In most democratic nations in which the debate over RFID technology will be most intense, two other scenarios are more likely to apply. One is called the "outside initiative" scenario, in which citizens' groups place a new issue on the public agenda. Aided by a sympathetic press which they use to raise public consciousness and define the issue in ways favorable to their ends, these groups take the initiative and strike the first blow. Choosing dramatic and compelling events to make their point, and linking them to core values that have deep resonance within the community, they usually win the first skirmishes in the battle over how the public will think about new issues and how the legislative and regulatory agencies will respond. Their ability to use the media and to build grassroots support are critical to sustaining the momentum of their initial victories, and the greatest danger to their cause lies in the threat that the issue will be "captured" by more moderate leadership anxious to add it to their political agenda and more willing to compromise for the sake of coalition building.

A third scenario is more likely, especially in highly pluralistic nations with well organized lobbies and a tradition of consultation and compromise. Termed the "insider access" scenario, it envisions the entry of new issues like RFID technology into the public policy arena through the actions of concerned and highly motivated "policy communities." Such communities are composed of interest groups, relevant governmental and regulatory bodies, both the producers and consumers of the new technology – in short, the "stakeholders" of a new issue. With access to government and the media, they attempt to shape both how the new issue will be interpreted and who will join in the eventual decisions over its regulation. In the best of all outcomes, the public will play little role, other than to internalize the interpretations offered them in the media and willingly accept the legislative and regulatory outcomes generated by decisions over which they had little direct influence.

The "insiders" have much to offer through their expertise on the issue, and daunting resources at their disposal in terms of their access to policy makers and influence on the media. In another context, they are the feared but nonetheless respected "iron triangles" of American politics, the close and symbiotic networks that link lobbies, key legislative committees, and regulatory agencies in a congenial and mutually beneficial good 'ole boy network.

It is also important to note that in many highly developed democracies these "insiders" frequently represent many different points of view. While this diversity may not represent true "countervailing power" – the notion that all sides of the issue are fairly and equally represented – they do provide a thoughtful and frequently lively discussion of most issues both in the media and in the legislative arena. In the American context, this means that long established privacy advocates such as the American Civil Liberties Union are assured a place at the table along side the representatives of industry and commercial interests, although less well established groups such as CASPIAN may have to struggle to be heard in this venue.

But insider status may also be a weakness, especially on new issues or against newly formed and animated opponents. The unique nature of a new issue or ambiguity on how to interpret its broader implications may initially tend to level the playing field between insiders and outsiders, especially to the extent that the outsiders can capture media attention.

The changing nature of the media themselves also tends to level the field. No longer do a few dominant newspapers or networks control access to and interpretation of information about key issues. In the rapidly growing world of "cyber politics," many alternative modes of communication exist both to spread the word and mobilize the faithful. If you Google the phrase "RFID technology," the little box at the top of the screen tells you (in 0.7 seconds) that 24,600,000 entries have been found; in similar fashion, "opposition to RFID technology" produces 507,000 references. Even more significantly, the virtual world of the internet serves to connect policy communities in ways never before possible. Websites, chat rooms, and blogs provide ways for the outsiders to connect and develop strategies at virtually no expense and without the need for extensive formal organization.

The Prism of Culture

In the increasingly integrated world of a global economy, it is easy to underestimate the importance of culture as a mediating factor. While it is apparent that a global culture is emerging in many ways, it nonetheless remains true that the values, perspectives, and expectations of different cultures will provide a nuanced response to new issues that enter the public policy agenda. From our current perspective of agenda setting, cultural values will affect the definition and framing of RFID issues, determine the core values by which they will be assessed, and define the nature of the potential responses that may emerge.[3]

While the different issues that are associated with the advent of RFID technology will be discussed at length below, it is instructive to examine a few from the perspective of how culture mediates their interpretation.

Privacy

The idea of privacy is deeply rooted in a nation's culture. It touches on the nature of the relationship between the citizen and the state, between citizens and the multitude of corporations and other nongovernmental institutions of society, and among citizens themselves. Moreover, it is always thought of in terms of the threats that may compromise its sanctity, and in the modern world this easily translates into growing concern with the development of technologies, RFID among them, that might lead to what the American Civil Liberties Union terms the "surveillance society."[4]

The nature of the relationship between the citizen and the state plays a large role in defining privacy. Clearly nations with long-standing democratic traditions are more likely to sustain a culture that defends privacy. It is not accidental that the greatest concern about the privacy implications of RFID technology manifest themselves in the United States and the European Union, and that the issue has far less public resonance in nations with authoritarian governments such as Russia and China, or in areas like Latin

America, where democratic government is less deeply rooted, or other issues such as economic development are more central.

Culture defines the boundaries between the public and the private self. What is quintessentially private in one society – religion or political views, for example – may be regarded as the stuff of common knowledge in another. The distinction is particularly sharp between cultures with a strong orientation toward individualism as opposed to those with a collectivist sense of identity. The former are characteristic of the U.S. and most European nations in which the individual is seen as possessing an inherent sense of identity and self-worth. Identity, and all of the safeguards that are needed to protect it, are idiosyncratic to each person. The individual stands alone in distinction from, and if need be, in defiance of the collective whole. In this setting, privacy is an inherent right of the individual vested in him/her for defense against the collective society; society's needs for order or security are secondary, except in the most exceptional and temporary cases.

In a collectivist society, the individual has no identity or meaning apart from his/her place in the broader collective. Russia clearly falls in the collectivist mold, as do most Asian cultures, although there may be significant generational differences within cultures. Defining privacy is therefore the primary concern of the society, not the individual. And in that setting, the boundaries between that which is private and that which is public are set to serve the interests of the broader whole; there is no intrinsic core of issues which are off limits to public scrutiny, and no legitimate defense by the individual to maintain the boundary.

Economic concerns, and especially the perception of the broader well-being of society, also affect a culture's attitudes toward privacy. In what has been termed the "culture of poverty," few issues rise to the significance of growth or survival, or in the context of today's global economy, of carving a niche in the world marketplace. Privacy is a luxury to be enjoyed by others in the so-called "post-material" cultures – advanced industrial societies now free to place high priority on quality of life or "dignity" issues rather than on the division of economic resources.

That said, it is also important to recognize that increasing globalization may soon begin to change that reality, at least to the extent that integration compels third world or emerging market producers to adapt privacy standards of more advanced nations. There is an increasing tendency to copy at least the more general outlines of privacy legislation in the United States and the European Union, and the need to utilize advanced technology to integrate data bases, especially to facilitate outsourced production, has led to the acceptance of advanced safeguards and practices.

Therein lays a dilemma for less affluent economies seeking to define their place in the global economy or for rapidly changing economies such as Russia and China. As noted, technical reasons may compel them to adopt the guidelines and best practices of the more advanced economies to which they are linked. But these may be culturally out of tune with the values of the host country, and may produce political conflict with authoritarian regimes.

Privacy is not just about who we are and what we wish to withhold from others; it also defines who we think is the primary threat to that privacy. Culture plays a significant role in identifying that enemy, and thus in suggesting how we respond to the threat. For most Americans, the "threat" is government. Big brother is watching, or at the least, wants access to all of the information about us already held in nongovernmental data bases. Ever more sophisticated technologies – RFID among them – hold the potential for the creation of a "surveillance society." Whatever the disclaimers, the threat exists. The solution, paradoxically, lies in part in relying on more laws at the federal and state levels to regulate government. Lest the contradiction not be apparent, a large part of the response takes the form of asking government to pass laws that not only limit the intrusion of new technologies like RFID as they are applied in the private sector but also limit the ability of government to gain access to private sector data bases. And in a distinctly American turn of events, heavy reliance also is placed on the courts and on the ability to file individual and class-action suits against those in government and the private sector that cross the line.

For most Europeans, in contrast, the threat is not government and the state but the world of corporations and private organizations. Government is seen as the solution to the problem; at least to the extent that it limits private sector intrusions into the lives of its citizens. The European Union requires each nation to develop privacy legislation, and predictably while they address a common core of issues, there are subtle differences. Recent EU hearings specifically addressing RFID issues underscored similar results. Germans offered 43 percent of the comments, followed by the French at 24 percent. These consultations also revealed distinctly European preferences for how any perceived RFID threat should be addressed; 70 percent preferred a technological solution to any threat to privacy, while 55 percent called for the passage of more legislation. This suggests that there are striking national differences in the perceived salience of RFID issues and in the level of concern about its deployment. Least frequently heard from were the new EU members from the former soviet bloc, undoubtedly reflecting their greater concern with the economic and social adjustments that accompany membership.[5]

Despite the reality that cultures do shape attitudes toward privacy issues and will play a role in the regulation of RFID technology, it remains true that none of the nations examined placed the issue at the center of public attention. The American case probably is typical. While there is growing public debate about privacy related issues such as a national identity card, e-passports, and RFID technology, the issue has not yet become a political question, at least in the sense that it has been forced on reluctant leaders through the "outsider access" style of agenda setting described above. From our earlier perspective, it has not yet made it to the agenda of a mass audience, and may not do so if the "insider access" mode of policy formation prevails. There is much to suggest that, rhetoric aside; the general public shows little real interest in privacy related issues. A recent survey revealed that only seven percent of Americans questioned had actually changed how they behaved to protect their privacy. Even more revealing were the findings of a study that tried to find out what incentives it would take to convince consumers to surrender personal information such as phone numbers and addresses. The threshold was a fifty cent coupon.

Environment

Culture also plays an important role in shaping attitudes toward environmental protection, an issue that is frequently central to the deployment of any new technology. In play are both the culture's intrinsic view of the relationship between man and the natural world and its attitudes toward economic development. Frequently the two may be at odds, especially to the extent that the nation finds itself at the beginning stages of industrialization and/or integration into the global economy.

While RFID technology does not present an extensive threat to the environment, there are certain aspects of its deployment that has potentially important environmental implications. Most important is its impact on recycling. Certain components – copper in antennas, silver in conductive inks, and the silicon substrate the tags are formed on – may complicate the recycling process, especially as the technology is further deployed to item-level tagging.

It is likely that this problem will be taken most seriously in advanced industrial societies with high standards of living. The sheer volume of tags entering the recycling stream will be greatest. But other factors also will be in play. Such presumably affluent society are far more likely to hold "post-material" values that stress quality of life issues such as the environment over rapid industrialization, and their political systems, if democratic, are more likely to present favorable opportunities for environmental groups to make their case to sympathetic audiences.

Religion

Culture and religion are inexorably linked. Religious values may affect the deployment of RFID technology either indirectly through their more general attitudes toward economic development and change or directly in those areas in which the technology itself seems to contradict religious edicts.

Virtually no immediate threat to the rollout of RFID technology is likely to result from the former. The producers, consumers, and likely stakeholders in this technology all function within relatively advanced, market-oriented economies or in the major trading partners linked to such economies. Simply put, whatever differences may exist do not challenge the overriding consensus that economic growth and prosperity are desirable outcomes.

Unless, of course, some aspect of RFID technology seemingly directly contradicts some fundamental aspect of the faith. Two examples may be cited. Some fundamentalist Christians argue that RFID technology represents "the mark of the beast" mentioned in the Book of Revelations. In a more limited vein, both the Amish and Mennonite sects forbid the marking and registration of farm animals, a process touted by RFID advocates.

While the political implications of these issues will be discussed below in a more thorough examination of the issues, it is important that we remain sensitive to the possibility that religious faiths may raise concerns.

THE ISSUES: WHAT THE DEBATE IS ABOUT

The coming debate about RFID technology will be a debate about many issues. While privacy has dominated the discussion to date, there are many other concerns that will become a part of the public agenda. And as do all questions that become a part of that public agenda, these issues will be affected not only by the details of RFID technology but also by the way in which the issue enters the political arena.

What follows is a discussion of the most important issues that will emerge in connection with the rollout of RFID technology *as political issues.* It is not our purpose to comment directly on the technical issues, except as they are perceived in their political context. And it is not our intent at this stage to discuss strategies for or the likely outcomes of the political struggles that will occur; that commentary follows in a second white paper. Rather it is our intent to clarify the issues, noting the “big picture” within which decisions ultimately will be reached and discussing the ways in which the context of the debate will shape the outcome.

Privacy as a Political Issue

Clearly the issue of privacy is the most volatile flashpoint in the current discussion of RFID technology. The projected wide-scale deployment of RFID technology is clearly perceived as eventually touching the lives of virtually all citizens of contemporary society. Whether touted as an instrumental improvement in the way we do business or conduct our daily lives, offered as a meaningful enhancement of our personal and corporate security in an increasingly dangerous world, or lamented as an Orwellian intrusion into that which should remain private, RFID technology produces strong reactions when the bottom line is about opening our private lives to further scrutiny. For many, it is a “quality of life” or “dignity” issue that should take precedence over questions of convenience, efficiency, or material reward.

How the Privacy Issue Becomes Political

In terms of the agenda setting processes discussed above, no one mechanism of politicization will be completely dominant. Sometimes, especially when the policy area touches on privacy issues and national security or the direct improvement of governmental operations, the model in which the government takes the initiative and largely structures the debate will be dominant. This is not to argue, of course, that at least in democratic contexts, the government will always get what it wants. And it is not to argue that the initial victories by those who would reduce privacy in the interest of national security or efficiency may not be reduced or qualified by subsequent actions by legislative bodies and the courts. But it is to argue that the initiative will come from government officials, and that both commercial and concerned citizens’ groups will be placed in a reactive mode, a disadvantage if not a total liability. In this setting, privacy concerns will initially be relatively low on the priorities of those who initiate policy, and their advocates will have an uphill battle before them.

For many issues concerned with the commercial applications of the technology, the insider-access model is the likely mechanism through which places the question on the public agenda and sets the ground rules through which it is resolved. It is the normal stuff of politics, the give and take of private interests, legislatures, and regulatory agencies which hammers out an acceptable, if not optimum, outcome. Privacy concerns will be but one of many competing priorities and their advocates will be struggling with strong commercial interests and their allies in government. This is not to argue that at the end of the day privacy concerns will be ignored. Their presence will reflect both the political strength and skill of privacy advocates and the willingness of both government and commercial interests to work productively with more moderate advocates whose positions can more easily be reconciled with the application of RFID technology.

The fate of legislation to limit the use of RFID technology in identity documents in California is probably typical of the way such struggles will play out when the insider access model applies. Initially submitted by California Senator Joe Simitian (D, Palo Alto), the draft legislation originally called for a ban on the introduction of such technology, coupled with the criminalization of any attempt to read data from such documents surreptitiously. Over a two-year period of "vigorous debate," the bill underwent substantial amendment, resulting in the substitution of a three-year moratorium on the deployment of such identity documents, and subsequently the elimination of the moratorium in favor of a number of interim, security based conditions users would need to meet. As the bill neared its final vote, most RFID advocates and commercial users dropped their opposition to the legislation, and its initial advocates softened their position to argue that the problem was not RFID technology per se but rather the absence of technology based security safeguards. Governor Arnold Schwarzenegger eventually vetoed the compromise bill, arguing that any state standards should be governed by future federal guidelines.[6]

The development of broadly accepted guidelines is another example of the process of consultation and compromise that emerges from the collaborative decision making involving the "insiders" on all sides of the question. In May, 2006, a working group made up of some of the nation's companies, public interest, and consumer advocates unveiled a set of best practices that would ensure consumer privacy. Based on fair information practices already in place in the United States and Europe, the guidelines outline how consumers should be notified about RFID data collection, what choices they should have with regard to their own personal information, and how that information should be handled and safeguarded by the companies collecting it. Involved in the drafting of these guidelines were groups as diverse as the American Library Association, the Center for Democracy and Technology, Cisco Systems, Ili Lilly, IBM, Intel, Microsoft, the National Consumers League, and Visa. The guidelines will be reviewed periodically in light of changing technology.[7]

Similar consultation between government and privacy advocacy groups has resulted in the creation of “privacy impact assessment” studies. Mandated by the E-Government Act of 2002, these assessments are to analyze the privacy implications whenever government agencies develop a new information technology or change the procedures by which they collect, store, and disseminate information. While vigorous debate continues over the results of such studies – controversy over the introduction of e-passports is the most recent example – the creation of the assessment process has institutionalized the mechanism through which both private and governmental interests on all sides of the question may exchange views.

In March, 2007, the European Commission announced that a “stakeholders’ group” composed of representatives of industry and consumer groups would be formed to advise on future privacy guidelines for RFID deployment in Europe. The group is expected to issue “recommendations” to member states on the creation of privacy safeguards in 2008. Coupled with the Commission’s assurances that it would eschew direct regulation of this new technology through the passage of additional legislation, the creation of this group strongly implies that the insider access mode of policy making will prevail within the European Union.[8]

But if government initiative and insider-access policy styles are the more likely modes through which RFID technology reaches the public agenda, there is another less sanguine possibility from the point of view of the RFID community. Termed the “outside initiative model,” it envisions the rapid politicization of the issue through association with a dramatic event that seemingly confirms to worst fears of its opponents. Just as oil-soaked seagulls on Santa Barbara’s beaches and the threat of a “silent spring” portrayed by Rachel Carson introduced most Americans to the threat of environmental degradation, so too could some mishandling of RFID technology be exploited. For those already opposed to the technology, or for politicians and would-be public intellectuals looking for votes and a cause, the temptation to seize upon some more extreme application – human implants, or the ability to track people – would be a real temptation.

Not surprisingly, only the most extreme circumstances have prompted such action, at least to date. In 2006 Wisconsin passed a law making it a crime to require that someone accept a RFID implant, and Ohio considered similar legislation.[9] Similar bills are pending elsewhere.

Playing to a broader audience, Senator Charles Schumer (D-NY) held a press conference on a Manhattan street corner during the Christmas shopping season in 2006 to denounce the threat inherent in no-swipe credit cards. Amid holiday shoppers, he warned that, “You might as well put your credit card information on a big sign on your back.”[10]

This is not to say, however, that such efforts to exploit some incident would be successful. At least in democracies, there are always many issues seeking to push their way into the public limelight and thus on to the political agenda. Success depends, as the literature on agenda setting well establishes, on their ability to command media attention and on the willingness of the system’s “gatekeepers” – those in government, usually at the level of key legislative committees or in regulatory agencies, that is, those who are already significant players in the "insider-access" game – to let them slip by.

How the Costs and Trade-offs between Privacy and RFID Technology Will Be Calculated

In a world of rational decision makers and measurable priorities, it would – in theory, at least – be a simple task to weigh the consequences of the application of RFID technology in different settings and to assess the trade-offs with other social priorities such as privacy. But that is not the world of political decision making, and the rational calculus of preference curves and trade-off costs cannot easily be calculated. How much increased security is worth diminished privacy? And to whom, assuming that the benefits and costs will be unevenly distributed throughout the society? It is one thing to measure the improved efficiency of a supply chain; when more goods get to the shelves of a Wal-Mart store in a timely fashion, and at a reduced cost, then the conclusion is easy and quantifiable. But how does one measure increased security against terrorists, or the peace of mind of parents whose children can be tracked through RFID chips in their school uniforms? And how does one compare those undeniable benefits with the unquantifiable costs of reduced privacy?

The answer is that there is no logical answer, at least in the conventional sense. While each individual can make his or her own assessment of the trade-off costs, the broader issue of collective action becomes a question of political choice, and that ultimately becomes a contest of political power. At the risk of initial oversimplification, in authoritarian societies that choice is made for the citizen, and in democracies it is reached through the one quantifiable measure of public choice – the vote. But this simplistic portrayal will not hold.

In the context of privacy issues, that suggests that the public acceptance or regulation of RFID technology will be determined by 1) the society's general sense of where the boundary lies between the private and public spheres, and 2) how effectively the political actors define the issue in terms of their priorities. As noted above, the former is largely defined by the culture in question; certainly American and West European cultures have accepted privacy as an important, if not dominant concern, while other cultures or nations that attach a high priority to economic growth over other concerns, position it lower on the agenda.

The latter – the definition of the privacy issue in political terms, and the relative skill of the players – will create the equation by which the trade-offs between privacy on the one hand and efficiency and development on the other will be measured. To the extent that RFID technology is seen as compatible with the maintenance of an acceptable level of privacy, compromises over its application and regulation will be relatively easy to reach and implement. The proponents and opponents will not perceive the issue as a zero-sum game, and to the extent that all participants in the debate can agree that each side must emerge with some benefits as well as make some concessions, compromise is possible. This agreement is all the easier to reach if the solution seems relatively simple. A quick and reliable technological "fix" would be best: RFID tags could be killed at the cash register, or detached with the sales tag, or other technology-based counter measures could be implemented. To the extent that the "fix" entails more profound compromises on institutional interests or principles, the more difficult will be the road to agreement.

Privacy of What, from Whom, and How Protected?

Much of the political debate about the privacy implications of RFID technology turns on three questions: 1) *Privacy of what*, or, in other words, what information would the deployment of RFID technology make available to others, with or without the permission of the subjects themselves? 2) *Privacy from whom*, or, in other words, who gets to know our business, and does that assortment of know-it-alls significantly change with the introduction of RFID technology? And 3) *How protected*, or, in other words, do we rely on technology-based fixes to implement the answers to the first two questions, or do we legislate additional safeguards and/or ban the deployment of RFID technology in certain highly sensitive areas?

Finding politically acceptable answers to the first question – what should be known, and by whom – is an extension of a long-standing debate between privacy advocates and representatives of the governmental and corporate worlds. What the government or other organizations in society need to know has always animated a vigorous debate, one settled, at least in the United States, both by the legislature and the courts. It cannot be ignored, however, that RFID potentially raises the stakes by extending the potential body of knowledge that can be collected on our location, behavior, associations, and consumption. It is therefore highly probable that the eventual compromises that emerge will be based upon an extension of existing privacy regulations and limitations.

In the American context, these guidelines will be patterned after the 1973 Code of Fair Information Practices established by the U.S. Health, Education, and Welfare Department. These standards adhere to five guiding principles:

- There must be no personal data or record keeping systems whose existence is a secret;

- There must be a way for citizens to find out what information is kept as a matter of record and how it is used;

- There must be a way for the citizen to prevent information collected for one reason from being used for another purpose or made available to other parties without his/her agreement;

- There must be a way for a citizen to amend or correct information contained in records; and

- Any organization creating, maintaining, using, or disseminating information about any identifiable person must be accountable for the reliability of the information and must take reasonable precautions to ensure its security.

Other nations have modeled their privacy guidelines on the 1980 policies for Europe set forth by the Organization for Economic Cooperation and Development, which calls for:

- Accountability by all organizations collecting and storing information;
- Disclosure of the reasons why the information is being collected;
- Consent of those about whom information is collected;
- Limitations on the kind and amount of data collected;
- Limitations on the use, disclosure, and retention of data;
- Checks on the accuracy of the information;
- Safeguards for its security;
- Disclosure by organizations collecting data on its use and management;
- Access by individuals to files; and
- Mechanisms by which compliance with the above regulations may be challenged.

Following an extensive set of hearings and public commentary in 2006 – 2007, the European Commission has promised to amend these guidelines by 2008 in ways that, at least in theory, balance the commercial need for further deployment of RFID technology with reasonable protection of privacy that are consistent with earlier guidelines. Arguing in March, 2007 that it was too early to impose regulations, Viviane Reding, the European Union's Commissioner for Information Society and Media, called for further study of the technology and its social implications and appointed an advisory group of industry representatives, privacy advocates, consumers, and scientists to make recommendations.[11]

But while there is widespread general agreement that the contemporary capabilities of RFID technology are sufficiently constrained by the limitations of the technology itself – reading range, size, and other technical limitations that at present make it impossible realistically to envision the Orwellian world of surveillance forecast by the most pessimistic critics – it nonetheless remains true that the technology inevitably will improve over time. Therein lays one of the fundamental problems in regulating use of any technology: the fear that increased capabilities will prove too tempting to government authorities or commercial interests. It is the "if it can be built, someone will use it in ways we did not anticipate and cannot control" argument that would have kept Benjamin Franklin out of the thunderstorm (electricity makes electric chairs possible) and the Wright brothers on the ground (no airplanes means no bombers). It is the technological equivalent of what the military laments as "mission creep," the unintended and always in the end self-destructive tendency to take on more commitments since they are seemingly implied by the initial sense of the mission.

When the point is made facetiously about electricity and airplanes, the answer is obvious. Society must and does find ways to make political decisions about the relative importance of the costs and benefits. But as we have argued above, the difficulty in calculating the trade-off costs between privacy and efficiency or profits is far more difficult. As long as the argument holds that RFID technology in its current and potentially more invasive future applications are, by analogy, merely extensions of past questions for which we have determined the broad guidelines of policy, then the debate will remain at the center of the political spectrum. Consensus will eventually emerge, even if that means shifting the center slightly in one direction or the other.

But that consensus can be upset by two developments. First, the technology itself may be perfected to a level in which the old analogies no longer seem appropriate. For commercial purposes, an RFID chip can probably always be thought of as a more powerful version of the barcode. The technical realities are not the important consideration. What is important is our perception of its function as a tagging device.

But if applied to the collection of potentially sensitive information about people and their social, political, and economic behavior, improvements in RFID technology may cross an as yet unidentified threshold. We are beginning to understand a little bit about where that threshold may be and what shapes that perception. Greater knowledge of the limitations of the current technology, for example, seem to make better informed consumers more willing to tolerate its deployment in commercial applications. But what we don't know is whether fear of future improvements may convince important segments of the policy community that its noncommercial applications may be so dangerous to privacy that further development and deployment should be preemptively halted. Clearly the growing sentiment to limit human implantation of RFID devices, or at the least, to ban government compelled implants, are an extreme example of this fear. So too may the fear of the tracking implications of RFID driven identity cards provoke a similar response.

Second, the consensus can be upset by some dramatic event that reshapes our willingness to accept a different trade-off formula between privacy and increasingly invasive, technology driven surveillance for the sake of national security, public health, or whatever else may seem to be at risk. Events such as 9/11 have shifted the balance through the introduction of e-passports, although there also has been stiff political resistance. It is not inconceivable that other threats such as a pandemic might seemingly justify more extensive application of the technology to monitor the spread of disease.

As noted above, the issue of privacy is not only about *what* can be known but also about *from whom* such information is to be protected. We care little, for example, that our medical records are known to our physicians, or our reading habits are known to the local librarians. But we do care far more about the potential for data base sharing in ways about which we are not informed and cannot control. The real fear is that the deployment of RFID technology in both commercial applications and in various identity documents such as e-passports will deepen the content of such data bases and set the stage for the sharing of information between commercial and governmental entities. Culture plays a role in shaping the perception of such a threat. As noted above, Europeans generally tend to fear that corporations and other business-related entities pose the greatest danger to their privacy; RFID technology enhances their ability to monitor the consumers' economic behavior and thus to influence their purchasing decisions. For Americans, the fear is of government surveillance; it is the noncommercial applications that bode most ominously in terms of deepening government awareness of how citizens behave in ways that reveal their political identity. But for both, the expanding danger lies in breaking down the barriers that formally separate the two, permitting government to access information obtained from commercial surveillance, and vice versa. RFID technology simply enriches both data bases, further tempting both sides to cross the boundary.

The final question – how do we protect whatever level of privacy we wish to establish – also evokes controversy. It is reassuring to believe that an easy "fix" is possible once we've made the more difficult political choices about how much privacy is necessary and from whom we need to protect our private selves. Just remove the tags at the point of sale, or find some way to encrypt the data more securely; "good" technology trumps "bad" technology, a thought easily accepted in our computerized, cell-phoned, Blackberried world. The European Union's survey on RFID technology revealed that 70 percent of the respondents thought that adequate safeguards would result from the development of "privacy enhancing technologies" (otherwise undefined), and 67 percent believed that raising the awareness of consumers concerning the dangers of identity theft would do the trick. Only 55 percent thought "additional legislation" (also undefined) would be necessary.[12]

Fear of a "Surveillance Society"

Even in the face of the seemingly most reasonable arguments and warnings about the potential use of RFID technology as the cutting edge of a new invasion of privacy, the case undoubtedly seems extreme to those members of the RFID community who know its current and likely future technical limitations and who are working to establish reasonable guidelines and protections against its misuse. But it is important for that community to understand the worst fears of their opponents. Underlying both the more extreme criticisms of groups like CASPIAN and more mainstream groups such as the American Civil Liberties Union is the fear of what the latter has termed a "surveillance society." From their perspective, the problem is two-fold. The first element lies in the increasing sophistication of the technologies themselves. "The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics and other technologies," avers Barry Steinhardt, Director of the ACLU Technology and Liberty Program, "in just the last ten years is feeding what can be described as a surveillance monster that is growing silently in our midst." "The fact is," he concludes, "there are no longer any *technical* barriers to the creation of the surveillance society."[13]

The second element of the problem lies not in technology but in public policy. Steinhardt continues, "While the technological bars are falling away, we should be strengthening the laws and institutions that protect against abuse. Unfortunately, in all too many cases … we are weakening the legal chains that keep it from trampling our privacy." What follows is the usual litany of threats linked both to the generally more conservative drift of American politics and to the specific government actions following 9/11.

Both elements could lead to the creation of an Orwellian nightmare that Steinhardt describes at length:

"RFIDs would allow for convenient, at-a-distance verification of ID. RFID tagged IDs could be secretly read right through a wallet, pocket, backpack, or purse by anyone with the appropriate reader device, including marketers, identity thieves, pickpockets, oppressive government, and others. Retailers might add RFID readers to find out exactly who is browsing their aisles, gawking at their window displays from the sidewalk – or passing it without looking. Pocket ID readers could be used by government agents to sweep up the identities of everyone at a political meeting, protest march, or Islamic prayer service. A network of automated RFID listening post on the sidewalks and roads could even reveal the location of all people in the U.S. at all times."

Lest our purpose be misunderstood, we are not arguing for the literal merits of the case or that the fears are justified. We are instead trying to convey to the RFID community the perceptions and fears – and the emotional strength of those reactions – of those who see the commercial deployment of these devices as the introduction of a slippery slope leading to an Orwellian world of government control.

The Environment as a Political Issue

While the privacy implications of RFID technology quickly come to mind, environmental issues appear at first to be less obvious. But like any new technology, RFID will have an impact on the environment that ultimately will raise issues of regulation. The nature and degree of that regulation will stem both from the general political climate in which environmental issues become matters of public policy and the degree to which the industry itself proactively anticipates and deals with emerging problems.

The political climate surrounding environmental issues is constantly changing. In the areas of solid waste disposal and recycling most relevant to RFID technology, there is a clear trend toward more stringent requirements at both the federal and local levels, especially concerning exceptionally dangerous pollutants such as heavy metals and other toxic substances. Both political and economic pressures create incentives to increase the general level of recycled materials and to deal with particular attention with those that are regarded as particularly hazardous.

On the positive side, RFID Technology will make the task of environmental management more efficient, both through its ability to track and locate potential environmental hazards and its improvement in supply chain management. In the latter case, improved inventory management will result in more efficient and fuel-saving delivery operations. Similar savings are likely in other sectors of the economy as the so-called "internet of things" leads to more efficient resource management.

As noted, the greatest concern will lie in the areas of recycling and disposal. RFID chips will enter the refuse stream in two ways, either through their use on bulk packaging and shipping venues such as pallets, or directly into trash bins through their use on item-level tagging. Although research is in progress to create more environmentally friendly RFID chips, at present the technology presents a number of problems. Chips and antennae can affect recycling efforts in a number of ways:

- They can make it more difficult to recycle cardboard containers;
- They can affect the recycling of pallets since pieces of the electronic components survive the shredding process;
- They can limit the recycling of steel products since copper and plastic will contaminate the metal;
- They will affect the recycling of glass since metal and ceramic fragments will damage glass kilns;
- They will limit the reconditioning of metal drums since electrostatic effects are possible; and
- They will affect plastic recycling since metal fragments can be contaminants.[14]

The regulations governing the recycling of RFID chips require that they be treated as electronic wastes and place them in the same category as computers, televisions, phones, and the like. The U.S. Environmental Protection Agency characterizes them as hazardous wastes under the provisions of the Resource Conservation and Recovery Act, and the European Union's Restriction of Hazardous Substances law imposes similar restrictions. Chips containing lead solder violate the packaging standards of the European Union and nineteen states in the U.S.

Initially there was little consultation between the RFID community and the recycling industry, although closer cooperation is now emerging. The corrugated box industry has taken the lead in adapting to the new technology, a necessary step since nearly seventy five percent of all such containers are recycled.

More environmentally friendly technologies are on the drawing boards. One possibility is the use of conductive polymers instead of toxic metals to print the tags, while another is the production of organic tags that would pose less threat.

The technical issues aside, it is important to remember that the environmental implications of RFID technology may evoke a stronger than expected response within the general public. The growing importance of the “green” vote is readily apparent to politicians regardless of their party affiliation, and already influential environmental lobbies that now focus primarily on questions of air and water pollution or endangered species may want to add the RFID-as-a-pollutant issue to their agenda if they perceive that it will increase their appeal. Like privacy, the environment has become one of the core values of most economically advanced nations, and any threat to that core is all the more likely to bring strong opposition.

Religion and RFID Deployment

As noted earlier, the response to any new technology is filtered through the cultural norms of society. In most instances, these norms will be neutral, implying little about the nature of the technology itself, or relatively flexible, permitting the technology to be employed in ways that are socially acceptable. In many cases, there will be general consensus about what is permitted or forbidden – the internet, for example, can be used to transmit information and communications but not child pornography. New technologies inevitably raise issues on which religions take a stand.

While religion is among the most important of these cultural norms in most societies, the general acceptance of a secular market economy in most advanced industrial nations, where RFID technology will be most widely used, mitigates against any general clash between church and chip.

But there are exceptions. The Amish, for example, are reputed to reject modern technology per se, choosing to live simply in a world without the gadgets we take for granted. But in fact, local community leaders are permitted to authorize the use of certain technologies such as electricity and internal combustion engines *as long as they do not make the community dependent on others or deeply intrude into the local culture.* The problem is not the technology per se, but rather that most modern technologies risk breaking down the barriers that preserve the distinctiveness of the community. RFID technology falls into this category in some instances, but perhaps not all.

There also may be specific faith based prohibitions. For example, both Amish and Mennonite faiths forbid tagging farm animals, which runs contrary to efforts to create a National Animal Information System, an effort motivated by commercial and public health concerns.

At least in the context of Western society, and most particularly among American fundamentalist Christians, the most important question centers on whether RFID technology denotes "the Mark of the Beast." Without debating the finer points of theology, it is possible to discern from the usually cited passage in Revelations that there are several elements of concern:

> He also ***forced*** everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead ***so that no one could buy or sell unless he had the mark,*** which is the ***name of the beast or the number of his name.*** (Rev., 13:16-18, emphasis added)

Most significant, of course, is the "beast" reference, signifying a demonic connection that is exemplified by the "mark," which can be expressed numerically. Later passages in Revelations promise "God's fury" for those who bear the mark.

The element of compulsion also is significant, for according to the passage, the mark is to be "forced" on everyone. This issue resonates with other concerns of RFID opponents, who fear compulsory implants for whatever reasons or warn that pressures from employers, educators, or public safety officials will de facto force us to carry or wear such devices.

There also is a clear link between this Biblical injunction and the world of commerce, where RFID will have its most extensive application. The notion that "no one could buy or sell" without the mark suggest both that in its presence such transactions would somehow be tainted and that the mark itself would be ubiquitous.

How concerned should the RFID community be about this issue? On the one hand, no organized religion has come out against RFID per se on the grounds of this passage in Revelations, and it is unlikely that mainstream denominations would lend support. For the present, the issue has been discussed most extensively on little known websites and blogs. It should not be forgotten, however, that the internet is an increasingly important medium for political communication and has become especially powerful in linking and mobilizing single-issue constituencies whose areas of concern are outside the mainstream.[15]

On the other hand, there is one significant exception, and it tells us much about the political uses of religion. Conventional wisdom about contemporary American politics tells us that fundamentalist Christians have a lot of clout, both in terms of their mobilization at the grass roots level and their financial backing of candidates and social issues. Any cause that can count them as allies has acquired significant leverage.

That brings us to the second edition of Katherine Albrecht and Liz McIntrye's book on RFID technology. Both are the leading representatives of CASPIAN, which opposes RFID. The first edition of this book was published in 2005 under the title *Spychips: How Major Corporations and the Government Plan to Track Your Every Move with RFID.* A year later, virtually the same book, but with a few added references to the passage from Revelations, was published under the title *The SpychipThreat: Why*

Christians Should Resist RFID and Electronic Surveillance. In politics, spinning the message for the audience is an important skill.[16]

Employment and Other Trade Union Issues

The deployment of RFID technology also will have important implications for employment and other trade union issues. Like all new technologies that affect the way we work and the nature of the workforce, RFID will bring both opportunities and challenges.

Two important employment-related issues have emerged:

- the potential for layoffs associated with the increasing automation of or elimination of jobs impacted by RFID technology, and the need for employee reassignment or retraining; and
- the potential use of RFID technology to more closely monitor employees as they perform their jobs, raising the question of where the line is to be drawn between legitimate supervision of the employee's activities and location and the violation of his/her privacy.

There is no comprehensive or reliable estimation of exactly how RFID deployment will affect employment. Some general estimates have been offered. In 2007, the Yankee Group averred that it would "affect" some four million employees in that year, resulting in "some job loss" – no exact figures were offered – but also in the shift of most workers to "more value-added" positions.[17] This admittedly vague estimation was misinterpreted by most of the media that reported it to mean that four million jobs would be *lost;* offering an important lesson on how such news can mislead the reader. With similar imprecision, the German retailer Metro Group reports that RFID will result in the loss of "thousands" of jobs, some of which will be shifted to customer service activities.

Occasional anecdotal evidence is also available. Proctor and Gamble has reported that it was able to reduce the number of fork-lift drivers in a factory in Spain, and Ford Motors revealed that it obtained a ten percent labor reduction in one factory in the USA. Such anecdotes also suggest that opposition may result from such layoffs. The Berkeley, California Public Library faced a firestorm of public criticism when a local newspaper reported that RFID-automated updating of its operations would result in the dismissal of twelve low-level employees. Library officials argued that the issue had been raised in Berkeley to forestall the adoption of similar automation in the much larger San Francisco library.[18]

While the arguments that RFID deployment will eventually lead to the shift of employees to more value-added positions and that it will create new jobs in the industry itself are undoubtedly true, there is a short term political rise that cannot be ignored. At the present time, RFID-driven layoffs will target certain low skill employees in potentially great numbers. Toll collectors and cashiers will be particularly hard hit, as will supply chain workers, and they may be less amenable to transfers to other jobs or retraining than other more skilled employees. One study also points out that such layoffs will disproportionately impact on female or minority employees, adding further sensitivity to the issue. It also should not be forgotten that the threat of extensive layoffs in this element of the workforce certainly will be used as a recruiting tool by trade unions, who are seeking to organize in essentially service-oriented areas or in large-scale retailers such as Wal-Mart, where their efforts have been unsuccessful.

A second and seemingly equally important concern expressed by trade union officials is that RFID technology will be used to monitor workers through the inclusion of such devices in their identification badges or uniforms. The issue is tied both to concerns about pressures for greater productivity – what the worker is doing and where he or she is will be known at all times – and with more conventional questions of potential violations of their legitimate right to privacy – with whom worker is associating, even when on legitimate breaks. While the first of these issues is idiosyncratic to traditional trade union concerns, the second – privacy – places them on common ground with the larger community of RFID critics who are concerned with similar questions, potentially setting the stage for de facto cooperation.[19]

At least to date, the response of most trade union officials who have addressed the concern is limited to calls for "consultation" or what they term a "social dialogue." There is no evidence that trade unions have formed alliances with other RFID critics over issues of workers' rights and privacy. The Union Network International, a global consortium of trade unions, has created an advisory "code of good practices" calling for:

- The presence of a written policy concerning RFID deployment and use;
- Negotiation and "social dialogue" between companies and trade union officials;
- An assessment of how RFID technology will affect the work environment and whether it will lead to the "deskilling" of workers;
- Full transparency concerning RFID use, including information on the location and active/passive nature of tags, and the location and range of readers;
- Prohibition against embedding RFID tags in uniforms, except for laundering purposes;
- Worker access to information collected through RFID monitoring;
- No non-negotiated linkage between RFID collected information and other employee records;
- Limited monitoring of workers' location, and no monitoring during break times;

- Worker ability to remove or switch off tags during break time;

- Prohibition that RFID obtained information will be used for disciplinary purposes, unless a crime has been committed; and

- Prohibition against linking RFID obtained data with other surveillance technologies (GPS monitoring, video or audio monitoring, and keystroke or internet monitoring).[20]

Public Health

There is no doubt that increasingly sophisticated RFID technology can play a positive role in increasing public health. RFID chips will soon be employed to track drug shipments and authenticate drugs in the face of increasing counterfeiting; requirements that drugs be given what is termed an "e-pedigree" will go into effect in California in January, 2009, and other state and federal regulations are sure to follow. But such advancements do not come without concern. The American Pharmacists Association, for example, has demanded protection against liability suits should counterfeit drugs slip through the new tracking system.[21]

As noted, RFID chips implanted in farm animals through the National Animal Identification System could be used to track contagious diseases within the animal population and protect consumers from related illnesses. But the extensive implementation of such an identification system has encountered opposition on both religious and privacy-related issues.

Similar objections will be raised about other medical applications such as patient tracking. Opposition will be especially strong if they involve the injection of monitoring devices such as the suggestion to use glucose monitoring chips in diabetics. One over-the-top website warns that there is a plot in the making to secretly inject all newborns with RFID chips.

A second area of concern ultimately will emerge as the chips become ubiquitous – are the chips themselves a danger to health? The concern is not unlike the "my cell phone could give me brain cancer" argument. While the generally accepted technical evidence suggests that there will be no danger from RFID deployment, some respected voices are suggesting caution. The International Agency for Research on Cancer has voiced its concern that the widespread deployment of chip-tagged products and readers will result in exposure levels that might be carcinogenic, and the European Union's Directorate for Research has called for further study of the issue. If the argument catches on – and that will be determined more by the public mood than by the initial technical evidence – there will be strong pressure for government regulation and the temptation for chip- rather than ambulance-chasing lawyers to bring personal injury suits against producers of the technology and retailers who utilize it. One jury decision against the industry or one preemptive out-of-court settlement will open the floodgates for additional individual or class-action litigation. [22]

Conclusion: In Politics, Timing Is Everything

Like most that have broad impact on our lives, the deployment of RFID technology will become a political issue – or *issues* – which is the primary point of this effort. RFID will mean different things to different audiences. To some, it will be about efficiency, profitability, and perhaps security; to others, it will be about privacy, or the environment, or religion, or employment, or public health, or possibly other concerns that have yet to be identified. The capabilities of the technology itself will define its actual ability to accomplish whatever we task it to do and that will constantly change over time as the technology improves. But it is the *politics* of RFID deployment that will determine what we let it do, and in a way the politics will change far more slowly than the technology.

That suggests an important and timely lesson. Earlier we noted that social scientists who study how the public agenda is created speak of "policy windows" – critical moments in time when the question goes public and a consensus emerges on how we should think about and react to this issue. Once that consensus emerges, it is likely to change far less slowly than the technology itself. The legislation and/or the regulations will have been written, and the problem will have been "solved," at least to the satisfaction of the dominant political forces of the day, and the politicians and the media will move on to the next preoccupation.

The moment is now. As noted, seventeen states considered RFID related bills in 2006. The issue is now on the radar screen, admittedly at low altitude, of some members of Congress and the Senate. Important international bodies such as the European Union have created study groups to recommend legislation. While it has not yet reached the status of lead article on the national media, attention is growing. It is important that the RFID community understand the diversity and complexity of the issues and the political battlefield on which policy will be shaped.

[1] See, for example, Donald L. Shaw and Maxwell E. McCombs, *The Emergence of American Political Issues: The Agenda-Setting Function of the Press,* St. Paul: West Publishing, 1977, and Wayne Wanta, *The Public and the National Agenda: How People Learn about Important Issues,* Mahwah, NJ: Lawrence Erlbaum Associates, Publisher, 1997.

[2] R.W. Cobb, et al., "Agenda Building as a Comparative Political Process," *American Political Science Review,* 70, 1 (1976): 126-38.

[3] See Stephanie Perrin, "RFID and Global Privacy Policy," in *RFID: Applications, Security, and Privacy*, Simson Garfinkel and Beth Rosenberg, eds., Upper Saddle River, NJ: Addison Wesley, 2006, pp. 57-82; Bimal Sareen, "Asia: Billions Awaken to RFID," in Garfunkel and Rosenberg, *RFID*, pp. 451-66; and Jennifer Torres-Wernicke, "Latin America: Wireless Privacy, Corporations, and the Struggle for Development," Garfinkel and Rosenberg, *RFID*, pp. 467-78.

[4] The best example of this concern is found in the American Civil Liberties Union report *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, which is available on their website at www.aclu.org/privacy.

[5] Commission of the European Communities, *Radio Frequency Identification (RFID) in Europe: Steps Towards a Policy Framework*, Brussels, SEC 2007, 312.

[6] Mary Catherine O'Connor, "California Governor Terminates RFID ID Bill," *RFID Journal* available at www.rfidjournal.com, October 2, 2006; "Landmark Privacy Bill Wins Bipartisan Support from California Lawmakers: ACLU Calls on Governor to Sign RFID Law," American Civil Liberties Union news release, August 31, 2006.

[7] Center for Democracy and Technology press release, "RFID Privacy 'Best Practices' Aim to Protect Consumers," May 1, 2006, available at www.cdt.org/press/20060501press; the complete text of the guidelines is available at www.cdt.org/privacy/20060501rfid-best-practices.

[8]"EU Develops RFID Awareness Plan," *E-commerce Times,* March 15, 2007.

[9] Act 482 of the Wisconsin legislature, enacted on May 30, 2006; the Ohio draft is cited in Patrick Cain, "Bill Would Bar Mandatory ID Implants," *Akron Beacon Journal*, July 21, 2006.

[10] "No-swipe Credit Card Warning: Senator Schumer Calls for Regulation, Higher Encryption Standards," *MSNBC News*, December 4, 2006.

[11] Rhea Wessel, "EC Floats Plan to Facilitate RFID Usage," *RFID Journal,* available at www.rfidjournal.com, March 19, 2007.

[12] Commission of the European Communities, op. cit.

[13] "Statement of Barry Steinhardt, Director of the ACLU Technology and Liberty Program, on RFID Tags before the Commerce, Trade and Consumer Protection Subcommittee of the House Committee on Energy and Commerce," July 14, 2004, available at www.aclu.org/privacy/spying15744leg20040714.

[14] Jim Morrison, "Sudden Impact: RFID and the Environment," *RFID Journal*, available at www.rfidjournal.com/article/articleprint/1932/-1/212.

[15] John Soat, "IT Confidential: RFID: Be Smart, Not Cynical, About Religion," *Information Week,* November 7, 2005, available at www.informationweek.com/story/showArticle.jhtml?articleD=173500007.

See also Mark Roberti, “Be Wary of Religious Opposition to RFID,” *RFID Journal,* August 7, 2006, available at www.rfidjournal.com/article/articleprint/2543/-1/2.

[16] The most widely read statement of religious opposition is Katherine Albrecht and Liz MCIntyre, *The Spychip Threat: Why Christians Should Resist RFID and Electronic Surveillance,* Nashville, TN: Nelson, 2006. Their earlier, virtually identical work is *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID,* Nashville: TN: Nelson, 2005.

[17] Samuel Greengard, “Man Vs. Machine: The New Battleground,” *RFID Journal*, available at www.rfidjournal.com/article/articleprint/1181/-1/124.

[18] Matthew Artz, “Library’s New Technology Sparks Controversy,” *Berkeley Daily Planet*, February 15, 2005, available at www.berkeleydailyplanet/com/text/article/cfm?issue=2-15-05&storyID=20728.

[19] See, for example, “Unions Want Curbs on High-tech Snooping,” *UNI eBulletin*, September 2006, available at www.union-network.org/uninetnews.nsf/0/360D26E5F9165510C12571F0045FB80.

[20] “RFID in the Workplace: Uni Code of Good Practice, version 1.0, 27 April 2006,” available at www.uniglobalunion.org.

[21] “Big Blue’s RFID Fix for Drugs May Stall,” *C/net News.Com*, December 15, 2006, available at www.news.com.com/2102-1012_3-6143979. See also “Congress Hears Testimony on RFID for Pharmaceuticals,” *RFID Law Blog,* published by McKenna, Long, and Aldridge, July 13, 2006, available at www.rfidlawblog,mckennalong.com/archives/58.

[22] “RFID Security, Data Protection and Privacy, Health and Safety Issues,” European Commission RFID Consultation Website, available at www.rfidconsultation.eu/?id_categoria=38&id_item=264&action=10.