INFORMATION TECHNOLOGY RESEARCH INSTITUTE

WORKING PAPER SERIES

ITRI-WP114-0608

The Politics of RFID - Implementation

Issued: 06.10.2008

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

THE POLITICS OF RFID:

IMPLEMENTATION

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**

INTRODUCTION

As a political scientist tasked with examining how the advent of RFID technology will play out as a *political* issue, I find myself initially reflecting on some of the truisms of politics in general. It is not accidental that the word *politics* is always plural. Issues that enter the political arena are always multifaceted. When understood in their full complexity, they raise different questions, impact on different constituencies, and unevenly distribute costs and benefits throughout the community

If this complexity were not confusing enough in its own right, a second truism about politics also must be noted. Politics is a *process* that unfolds at different times and under different sets of rules. For our purposes, there are really two very different perspectives on the politics of RFID. The first deals with the initial politicization of the issue, and has already been discussed in considerable detail in an earlier white paper entitled *The Politics of RFID: The Issues.* At this stage, new issues emerge, are defined, and become a part of the political agenda. As argued earlier, that is a critically important stage in which the rules of engagement and the identity of the key players are defined. Now rapidly unfolding before us, that stage seems to indicate that the eventual regulatory environment within which RFID technology will operate will be forged through consultation among the most important stakeholders. Those who produce and use the technology are now a part of a dialogue that includes those with legitimate concerns about its impact on issues like privacy and those in government at all levels tasked with creating the legislative and regulatory environment within which it will operate. In the parlance of American politics, the issue is now solidly in the "center," at least for the present, and the process is moving forward as it does for most new issues that do not polarize the community.

There is a second process that also bears careful examination. Usually called something like the "policy implementation process," it focuses on the application of the political decisions reached in the first stage. For most issues, and especially for highly technical or complex issues like RFID, legislators are content to hand down general guidelines, mandate jurisdictions and responsibilities, and then leave it to the bureaucrats in various regulatory agencies to sort out the details and make the day-to-day decisions about what the rules really mean and who is, and who is not, following them. In many ways, this phase of policy implementation may be equally, or even more important to the stakeholders, especially if the regulatory officials have considerable latitude to tilt policy in ways that affect how vigorously the rules are applied or favors certain interests within the RFID community over others.

Given the complexity and multi-layered nature of the politics of RFID, where do we go from here? This white paper addresses several issues, and should be read in conjunction with its parallel effort, *The Politics of RFID: The Issues*. Taken together, they are meant to address the nature of the issues that will become a part of the political agenda, the processes through which this will occur, and the cast of characters in the RFID community, in government, and in the community of concerned stakeholders who will take part in the process.

THE POLITICS OF RFID REGULATION

As noted above, the politics of RFID regulation is a game now in progress. Like all new political issues, it is characterized both by the relative uncertainty that is present because it is a new and (at least by the public) poorly understood technology and by the complex nature of the playing field. A review of that complexity sets the stage for our understanding of the possible scenarios through which the eventual regulatory setting will be formed.

Multiple Issues: As we have pointed out, the deployment of RFID technology raises many different political and economic issues, and it is not our purpose here to view that complexity in detail. But it is important to note that each of these issues means different things to different constituencies. While privacy is the more widely acknowledged concern of many who question the impact of RFID technology, other issues such as the environment, job security and the treatment of workers, and even the technology's implications for religious values are significant to others. While no "united front" has emerged to link all of these concerns into a concerted opposition, it nonetheless remains true that there is some potential for coordinated opposition to RFID technology. The nuances of such possible alliances will be discussed below.

Multiple Constituencies: Also of significance is the great diversity of the constituencies that have a stake in RFID technology. As with many political issues, there are multiple "stakeholders" who perceive they have something to gain or lose. They range from the producers of the technology and the corporate giants like Wal-Mart to small public interest lobbies like CASPIAN or The Electronic Privacy Information Center. Aside from their intrinsic interest in the nature and implications of the technology, they also have something else in common: each is realistically aware of their assets and liabilities as a participant in the political game, and each is likely to employ rational strategies to press their case on legislators, regulatory agencies, and the general public. This is not to argue, of course, that all are equal; as the battlefield over RFID regulation begins to take shape, it is obvious that certain groups possess more resources than others and are more likely to play a dominant role in shaping the policies that emerge. But it is to argue that all have a reasonably good sense of how the political game works, and how to employ their resources to carve out a niche for themselves as participating stakeholders in the policy making and implementation processes.

It is also important to note that, at least in the procedural sense, that the politicization of RFID technology is pretty much "politics as usual," that is, within the conventional mainstream of how issues are recognized and defined and how the conventional rules of engagement set the stage for their eventual resolution. To be sure, other scenarios are possible; the next section of this white paper discusses a number of alternatives that have been suggested in the literature, some more likely than others. But for the most part, the nascent debate over the potential regulation of RFID has taken the form of broadly inclusive consultation involving the representatives of both proponents and critics. Caution has marked the process, both in the sense that state, federal, and international policy making bodies have not rushed to judgment and imposed far-reaching controls at the early stages of the technology's deployment, and in the sense that members of the RFID community itself, such as EPC Global and AIM Global have taken the lead to reach out to concerned officials and advocacy groups and to propose guidelines that address (and from their perspective, hopefully defuse) many of the issues.

Multiple Arenas and Battlegrounds: Further complicating the politicization of RFID technology is the complexity of the arenas and battlegrounds on in which policy will be formulated and implemented. As noted above, *politics* is plural not only in the sense that there are many issues and actors involved in the game, but also because it takes place in a multitude of overlapping venues. At least in the early phases of regulation, there may be attempts to regulate RFID technology at a number of overlapping administrative and geographic levels. In the American context, overlapping regulation at the state and federal level is both possible and likely, perpetuating the inevitable constitutional questions of the role of state and federal government and bringing the judicial system into the process of policy formation and interpretation. Attempted regulation is even possible at the local level, as demonstrated by the effort in Berkeley, California to limit the application of RFID technology to the local library because of potential job losses. International and regional regulatory efforts are also inevitable. Supranational entities such as the European Union have moved rapidly to recognize the broader political questions involved with RFID technology and to initiate a process of broad public debate and consultation about its deployment, and such efforts are inevitable in other regional trading blocs.

This is not to suggest, however, that the multitude of potential sources of legislation and other regulatory edicts will necessarily make it easier for the opponents of RFID to advance their agenda. To be sure, in some instances this may be possible, especially to the extent that a single-issue focus – for example, opposition to the implantation of RFID chips for identification or tracking purposes – may make it possible for a few advocates to make their case. But in the broader context, the evidence thus far seems to suggest that a relatively high level of caution and a wait-and-see attitude prevails. Following an extensive program of consultation and public commentary, the European Union has recommended against the creation of an extensive set of regulations at this time, deferring action both in recognition of the technical complexity of the issues and (more importantly, at least from the political perspective) in anticipation that an attempt to write sweeping regulations would encounter considerable opposition from major economic interests. California has taken much the same tack, deferring to the eventual creation of federal guidelines, and many other states have eschewed definitive action in favor of the creation of study commissions charged with studying the issue and suggesting future action. At the national level, similar purposeful inaction seems likely, at least until both the technical issues and the political fallout are better understood. And when action is finally taken, as inevitably it will be, there will be a strong propensity to defer to the leadership of small groups of legislators such as the Senate RFID Caucus, both because of their acknowledged expertise on the area and their close ties to important stakeholders.

To any student of the politics of the regulatory process, none of this is particularly surprising. In any policy making setting characterized by multiple and overlapping jurisdictions and offering multiple points of access to those who influence policy, it is inevitable that the initial stages of policy formation, especially when the issue first becomes a part of the accepted political agenda, that there will be much initial confusion over who will take the lead. The case of RFID technology, that means that opponents will seek initial victories at the state or local level, where their limited resources may be more influential, in the hope of setting precedents and shaping public opinion. More powerful lobbies that favor the deployment of the technology will focus on the national or supranational level, hoping both to delay decisions until the deployment acquires a sense of inevitability and to influence the creation of the least invasive regulatory environment possible.

Two additional political realities about the introduction of new issues militate in favor of the RFID community, at least in the long run. The first is the tendency among legislators to defer to their colleagues who have acquired particular expertise in an area; the more complex and technical an issue, the greater the willingness to permit those legislators to take the lead in framing policy. In the case of RFID technology, the small community of legislators who seem most involved are clearly in favor of its deployment. While there are a few notably exceptions such as Joseph Simitian, a Democrat in the California Senate who has repeatedly (but largely unsuccessfully) introduced anti-RFID legislation, the vast majority of those who have spoken out or taken part in organized policy groups like the Senate RFID Caucus are supporters rather than critics. Not surprisingly, some of the most vocal advocates such as Byron Dorgan of North Dakota, a co-founder of the Caucus, represent districts that have a considerable stake in RFID related industries. To be sure, no individual legislator will ignore the interests of his or her constituents in deference to a colleague who is simply better informed. But the threshold of those political risks must be fairly high to compel a legislator to ignore the advice of the acknowledged experts among his or her colleagues.

The second reality concerns the political wisdom of procrastination. Especially concerning new issues where the political costs of making a choice may not be readily apparent, expediency may dictate that no decision is the most politically correct decision. Every politician knows that the decision you didn’t make is less likely to bite you at the next election than the decision you did make. That creates an understandable predisposition not to jump into the fray until the issue has been defined by others with a more direct stake, and that reality tends to favor the more powerful and established interests, in this case most clearly identified with the RFID community than with its critics.

THE POLITICS OF RFID REGULATION: POSSIBLE SCENARIOS

The plural nature of "scenario*s*" also is important to note. There are many possible scenarios through which the politics of RFID deployment may play out. What follows is an examination of those possible scenarios at two levels. The first deals with the possible scenarios that have been offered in the RFID literature. It expands on the analysis of the issues provided in an earlier white paper. The second level focuses on what happens next in the implementation phase; once the general policy guidelines have been determined the day-to-day task of interpreting and implementing the rules begins.

THE POSSIBLE SCENARIOS: EXISTING POSSIBILITIES

The possibility that alternative scenarios may play out has not escaped the attention of some members of the RFID community. Writing in Simson Garfinkel and Beth Rosenberg, edsl, *RFID: Applications, Security, and Privacy* (Addison-Wesley, 2006), Ari Schwartz and Paul Bruening suggest four possibilities. The first, termed "No One Wins," envisions a situation in which RFID opponents score significant victories. Working primarily at the state level, predictably in California and Massachusetts, their efforts result in the passage of stringent controls that become the model for subsequent legislation elsewhere. Facing prohibitively high costs associated with meeting such strict technical standards, and with the possibility of high punitive damages from legal challenges, both producers and potential users abandon RFID technology and turn to other alternatives such as face recognition technology to track consumer behavior and deal with shoplifting and other security issues.

The second scenario is labeled “Shangri-La,” after the mythical utopia of the James Hilton’s novel, *Lost Horizon.* Recognizing the potentially controversial nature of RFID technology, producers and users of the new technology undertake a broad program of consultation and consciousness raising targeting the concerns of potential stakeholders and the general public. Working with consumer and privacy groups, industry coalitions, legislative and regulatory officials, the RFID community develops an extensive program of self-regulation. Regulations are accepted that both govern how and where the technology may be employed and the use and safeguarding of any information that may be collected. Everyone “wins,” at least in the sense that a common middle ground emerges on which all parties can stand

More ominously, the third scenario is called “the Wild West.” RFID technology is deployed virtually without any effort to address the concerns of privacy advocates or other critics. Both effective self-regulation and formal state-sponsored regulation are absent or inadequate. In desperation, opponents engage in destructive vigilante efforts to thwart the technology, randomly killing existing tags in stores and governmental installations or placing cloned tags in similar locations to render tracking and security efforts useless. In frustration, producers and retailers abandon the technology. Modern-day Luddites, like their earlier counterparts who opposed industrialization by destroying the machines that made it possible, carry the day.

Scenario four is “trust but verily,” the phrase coming from Ronald Reagan’s observation that he was willing to trust the Soviet Union to destroy elements of its nuclear arsenal – providing they were willing to let him independently verify that they were doing it. In this less than fully trustful world, the federal government establishes "baseline privacy protections" that apply to all current and future technologies, based on long-established principles concerning notice, choice, security, access, and recourse to govern the collection and management of consumer information. Both RFID producers and users willingly accepted these guidelines, although unresolved ambiguities exist in applying them to the specifics of the technology. Despite the best efforts on the part of most commercial users, a number of lawsuits are eventually filed against outright abusers or to resolve these ambiguities.

The fifth scenario comes from Katherine Albrecht, co-founder of CASPIAN, writing in the same volume. Termed by her "the doomsday scenario," it foretells widespread corporate and governmental abuse both in the surreptitious deployment of chips and readers and the creation of comprehensive and interlinked data bases that permit uncontrolled identification and tracking of virtually anyone.

While these scenarios offer some possible outcomes, for the most part they are a bit naïve when it comes to an understanding of the political process through which regulatory policy will be created and applied. It is therefore our purpose in the next section to address that more complex reality, taking into account the important distinctions between the *policy making* and the *implementation* phases and reflecting the reality that regulatory efforts will be driven by the more widely shared concern with the privacy implications of RFID technology than by any other issue.

PHASE I: CREATING THE REGULATORY SETTING

In an earlier white paper, considerable attention was devoted to the process through which new issues enter the political arena. Understood by political scientists and policy studies specialists as *agenda setting*, it is a process through which issues are identified, defined, framed (that is, placed within an already identifiable and routinized political and institutional context), and linked to certain "core values" in any given society that give both identity and emotional salience.

Now it is time for a more detailed examination, with particular attention to how the issue of RFID technology may be linked to already existing issues. On the positive side, we are quite sure in general how the process of agenda setting works, and how that process creates the regulatory milieu that follows the initial politicization of the issue; as political scientists, we have analyzed enough issues and played out through enough scenarios that we are sure that we understand how any possible scenario might evolve. Also on the positive side, we are already well into the agenda setting cycle for RFID technology; the game has been joined by many actors at many levels. We are probably somewhere around half-time or the fourth or fifth inning, to belabor a sports analogy. We have a pretty good idea of how the game is going, and the strengths and weaknesses of the teams are, we hope, readily apparent. But there is a reality that any sports fan must admit, and in some ways savor: the outcome is not certain. That, as Len Berman loves to remind us, is why they play the game.

The same is true in politics. We are then ready to take the next step in very specific terms to pose two important questions: 1) which issues will be dominant, and how will they interact in the broader political arena and 2) how will the game change when we move from the initial policy formation into the secondary policy implementation phase?

Privacy Issues Frame the Agenda

Although it remains true that a number of issues are associated with the politicization of RFID technology, it is increasingly obvious that the question of privacy will be the primary factor in shaping the political response. While other issues such as the environment, employment, religious values, and health concerns will have some impact, they are tangential to the question of privacy. In the American case, this is hardly surprising both in light of the traditional priority attached to privacy and the fear of government surveillance and the political clout of lobbies such as the American Civil Liberties Union. While the issue is perceived slightly differently in Europe – the most common fear is of corporate, not government surveillance – concern with the privacy implications of the technology will shape the public response and the regulatory environment. Although it is true that privacy issues are less salient in other areas such as Latin America or Asia, the public perception of the issue and the eventual regulatory environment even there will be shaped by the American and European experiences, more in response to the need for global standards to facilitate the deployment of the technology than any sense of cultural standardization.

If the privacy issue is the lens through while all other concerns will be viewed, what are the implications, both for how these issues are perceived and how the politics of their regulation plays out? While the question cannot be answered with complete certainty, it is possible to make some educated guesses about both the content of the policies that emerge and the politics that govern their creation.

Existing Privacy Guidelines Will Be Extended and Creatively Interpreted. No body, and especially not a politician dealing with a new and potentially volatile issue, likes to be responsible for reinventing the wheel. This suggests that the most intellectually defensible and least politically risky course of action is to base future privacy regulations of RFID technology on the existing – and already substantial – regulatory regime that exists for other technologies. Public policy specialists call it "incremental decision making," and it usually results in a minimally invasive approach that tinkers with existing rules based on two new elements in the equation. The first of these is the changing technology itself, and the ways in which it is applied. At least to date, the consensus seems to be that RFID technology is an extension, albeit a potentially more invasive one, of similar applications of existing technology. As long as this interpretation holds and the regulations can be adjusted or interpreted with flexibility, there is little reason from the technical or legal perspective to reinvent the wheel

The second potentially new element in the equation may be more disruptive – the entry of new actors on the political stage, or a realignment of existing forces in ways that make the old consensus less politically acceptable. This outcome is unlikely *unless* the RFID privacy issue is itself redefined to suggest that the old guidelines cannot be adapted to deal with the perceived threat, or *unless* the already existing and accepted privacy advocacy groups are upstaged by new actors or coalitions who radicalize the issue. As we have suggested earlier in the white paper on issues, this would require both the emergence of a new set of activists who could establish their credibility and the mobilization of a new constituency of concerned citizens. Paradoxically, it is probably true that the "privacy" constituency is already as well organized and mobilized as it is likely to get in American politics. Only a serious challenge to the privacy of a substantial number of currently unconcerned citizens would vastly expand this constituency, and it is unlikely that the issue of RFID technology will rise to that level of concern. While the privacy lobby, if it can be called that, will be willing to add the issue of RFID technology to its own agenda (and on its own terms), it is probable that such action would deepen the concern of, but not necessarily expand the size of its constituency of activists and concerned citizens.

The Further Erosion of Privacy Is Inevitable. Studies have suggested that the general public accepts that the further erosion of privacy is probably inevitable. To the extent that concerns have arisen, they are linked more to the issues of identity theft (*a* concern, but not the *primary* issue raised by RFID opponents) than to issues associated with the commercial application of RFID technology. Strengthening this trend is the seeming willingness of consumers to surrender information for the sake of discounts or other enticements. While the notion of privacy in the abstract still remains popular, consumers are surprisingly willing to reveal information about themselves and their occupational and financial status to obtain the discounts provided by in-house credit cards or consumer loyalty cards.

That said, it is still significant to note that 40 percent of the respondents in a November 2007 poll conducted by the Ponemon Institute indicated that the privacy issue would be “very important” (15%) or “important” (25%) in their evaluation of presidential candidates. The same issue was slightly more important to younger voters in the 18-28 age range (18% calling it “very important” and 34% “important”), than older voters over 58 (14% to 26% responding in the same categories). Among both Democrats and

Republicans, mainstream candidates like Hillary Clinton and Rudy Giuliani were seen as least committed to privacy issues, while the less mainstream candidates Barack Obama and John McCain received the highest ratings.

"Good" Technology Will Trump "Bad" Technology. Consistent with the growing reliance on potentially intrusive technology in virtually all other aspects of our lives in modern society, there seems to be an unquestioning assumption rooted in American, and to a lesser extent European culture, that technological fixes will emerge to deal with the worst privacy threats. Tags can be "killed" electronically after they have served legitimate commercial purposes, or other technical safeguards can be found to limit both the potential that information will be read by unauthorized personnel and that threat that ever-growing data bases will expand beyond control. Coupled with the assumption that there are ways to physically "opt out" of the growing RFID network – tags can be limited to disposable packaging or removed from items such as clothing after sale – there will be a tendency to accept the idea that every clever advance in the technology will be checkmated by an equally clever step forward in terms of countervailing technologies that will protect the consumer and citizen. The mouse is just as clever as the mousetrap maker.

The Watchdogs and Activists Are Equal to the Task. Even if one is skeptical of the adequacy of possible technology-based solutions, there is a general acceptance that watchdog groups like the widely known and respected American Civil Liberties Union are highly motivated and vigilant. Especially in the context of American politics, it is assumed (usually correctly) that *everybody* and *every point of view* has a lobby, and that politics is a hotly contested process of competitive advocacy. *Somebody* will keep an eye on things, even if it’s an uphill battle. And if things get bad enough, these *somebodies* will know how to mobilize the media and public opinion, or how to use the courts to good advantage. In a litigious and over-lawyered society, there will always be a hungry attorney who will take the case, or a vote-hungry elected official who will make our cause his own (especially if there seem to be a lot of *us*).

LOCATION, LOCATION, LOCATION

The often cited comment that the most important things about real estate are location, location, and location is also true about the politics of RFID regulation. Important decisions will be made in different places, both in terms of the overlapping hierarchy of local, state, and federal jurisdictions found in the United States and in terms of the growing importance of supranational and international regulation found in entities such as the European Union or regional trading blocs. While control and regulation will occupy center stage at certain points in time, other important questions such as standardization, either through government decision or through voluntary compliance with standards set by manufacturing and commercial users, will also be addressed.

This abundance of playing fields offers both hope and potential frustration for those who would influence regulatory policies. To be sure, some playing fields are more important than others; especially on key issues such as privacy, the major battles will be won or lost in the United States at the federal level, and at the international arena at the level of major players like the European Union, whose decisions will become the templates for subsequent action by smaller multinational entities or individual countries. But given the federal nature of the American system, and the wide number of issues potentially involved with RFID technology, it is highly likely that state-level regulation also will be enacted. A pattern seems to be emerging in which federal authorities are reluctant to take quick action in the face of the low level of general public concern, the complexity of the technology, and the increasing willingness of RFID producers and users to draft what hopefully will be politically acceptable guidelines for self-regulation. As yet, there is no Democratic or Republican position on the issue, and only a few candidates for the House of Representatives or the Senate (and none for the presidency) have made the issue a part of their stump speech to the voters. While the privacy issue is a concern of some voters as they evaluate presidential candidates, it is not specifically linked to the impact of RFID technology. The issue has not yet reached the radar screen of most politicians, and those who are aware of it are reacting cautiously. Let sleeping dogs lie, at least until we are sure whom they will bite if awakened.

From the broader political point of view, the multiple and overlapping venues in which policy will be made will extend the timeframe for creating a comprehensive and widely accepted framework regulating RFID technology. Part of that reality stems from the fact that the battle may be fought many times over the same issue; the "winners" at the federal level will be quite content to let the matter rest, while the "losers" will try to salvage as much as they can at the state level or through the courts. Adding to the complexity is the latitude permitted to regulatory agencies such as the Federal Trade Commission, whose power of interpretation is in fact real power to determine the details of regulation. The same complexity will play out in different institutional form at the international level, where supranational entities like the European Union or trading association will shape the general guidelines but surrender the details to local authorities or the bureaucracy.

THE POLITICAL IMPACT OF OTHER ISSUES

While the question of privacy will be the primary issue that shapes the regulatory environment of RFID technology, other issues will make their mark. As we have argued in a previous white paper, RFID deployment is not just about privacy. Other concerns such as employment, health, the environment, and religious values will have some impact on the politicization of the issue. In most cases, it is unlikely that these issues will mobilize either an effective groundswell of public concern or animate powerful lobbies and interest groups to put the issue at the center of their agenda. The impact of RFID deployment on employment provides a good example of the likely scenarios that will play out. While it is true that the technology will cost some people their jobs, especially among less skilled workers, there will be little incentive for trade unions to elevate this issue high on their political agenda. In the broader perspective, there are simply too few workers (and probably the wrong workers, at least from the unions' point of view) who will be affected. Rather the question will be treated as an "add on," that is, something to be tacked on the existing shopping lists of worker-oriented appeals and political demands, probably fairly low in the hierarchy of needs. As an "add on," it will be spun in several ways that link it to other issues, and hopefully from the unions' perspective, to other already mobilized constituencies. This is already evident in the emphasis placed on RFID technology as a potential invasion of workers' privacy. The argument is that such technology will lead to unacceptably invasive monitoring of workers' performance or to the extension of such surveillance into the workers' legitimate private space at the workplace. Spinning the issue in such a fashion also links workers' and union concerns to the much broader and highly motivated community of privacy activists such as the

ACLU. Successful political action frequently is based on the art of coalition building, and framing the issue in this fashion links two powerful and well organized communities of activists who would benefit from the collaboration.

In the same spirit, unions' concerns about potential layoffs are also likely to be linked to the demographic consequences of such actions, which will probably impact disproportionately on female and minority workers. Political reality suggests that there is less leverage associated with this spin to the issue. The more politically powerful trade unions do not organize their members in terms of gender or ethnic/racial distinctions and probably would be loath to disrupt their efforts to build a broad based sense of worker solidarity for questionable political gains, and those few worker or professional associations that organize along such lines possess little political clout.

RFID issues related to public health are far more difficult to treat as "add ons," at least in the sense of building political coalitions. The nature of any potential threat is not well documented within the scientific community, and there are no powerful lobbies or public health advocacy groups that have taken up the cause. Among the vast and well documented potential threats to public health ranging from the environment to personal choices such as smoking, RFID related hazards have not yet risen to the status of a low altitude blip on the radar screen. There are no other public health advocacy groups who would be natural allies for activists concerned with RFID issues. To the extent that RFID related health issues become political concerns, they are likely to enter the public arena through the courts, based on individual or class action suits whose first task would be to assemble a convincing body of scientific evidence that the technology was culpable of some injury. As the long history of litigation against the tobacco industry demonstrates, that is a daunting task. If successful, such outcomes would create pressure for tighter regulation. But it is probably true that the real action would remain in the courts in the hope that substantial punitive judgments would pressure the industry itself to reduce health hazards.

RFID related environmental issues also would be difficult to treat as “add ons” to the already lengthy agenda of the major environmental lobbies. As noted, it is primarily an issue of recycling and solid waste management, where commercial interests are well organized. While potentially significant, that question is not the central concern of the nation’s most powerful environmental lobbies. In political terms, they simply do not need the limited political clout that the anti-RFID community could bring to the table, and the introduction of a new and poorly understood question could only muddy the waters. In addition, the proactive stance of key actors such as the corrugated box industry will do much to defuse the question and keep it low on the radar screen that tracks public policy issues.

The politics of RFID as a religious issue is the hardest to predict. On the one hand, whatever happens, it will not be treated as an “add on” issue in the manner discussed above. Other than sheer political opportunism, there are few if any connections either intellectually or politically between the concerned publics that would respond to privacy, workplace, or environmental issues and those that would respond to religion-based concerns. Even in American politics, the notion of a natural alliance between the ACLU and usually conservative fundamentalist churches stretches the imagination. While groups like CASPIAN have suggested that a common interest exists, there is no evidence that a viable connection has been made. Simply put, fundamentalist churches do not need groups like CASPIAN as allies if they do decide to elevate their concerns about RFID technology to the level of a political issue. Their own resources, and the dedication and discipline of their members, are more than adequate to the task.

PHASE II: THE POLITICS OF REGULATION

Perhaps understandably, much of the discussion within the RFID community about the politicization of this new technology has focused on the agenda setting stage of the process – that is, how it is initially defined as a political issue, what forces are in play to define whatever regulatory regime is created, and the cost and opportunities that will arise when this process has played to its conclusion. But in the longer term, there is a second phase that should not be ignored – the politics of regulation. It would be both a political and tactical error to think that once the laws and regulations are in place, the important questions have been decided, and that little will change. As we have noted before, in politics, the fat lady never sings, and the political struggle will continue in different form, but with significant opportunities and costs for the RFID community.

At the outset, it is important to remember that the regulatory process is a disguised version of a political process. In most regulatory settings, the original legislation that sets the playing field seeks to define three aspects of the regulatory process: 1) the general parameters of acceptable policy; 2) the identity of the regulatory agency (ies) that will determine policy within those parameters; and 3) the rules of engagement between the regulatory agency (ies) and the broader community of organized stakeholders. In truth, none of these determinations is precise or lasting. Ambiguity is inevitable, and sometimes purposeful.

Setting the general parameters of acceptable policy illustrates the point. At least at the initial stages, industry sponsored “guidelines” may influence both government and private sector decision makers, especially if they have emerged through a process of broadly inclusive consultations, which seems to be the case with emergent RFID standards and best practices. But at some point, some portions of these “guidelines” will inevitably become “regulations”, that is, formal enactments by some level of government making them both mandatory and enforceable. While these guidelines will probably influence the eventual legislation, the shift to formalized regulation raises the stakes. Even the most carefully drafted formal regulations have their limits. Only a few hard-and-fast regulations will be set down by legislative bodies, and those will be determined more by the political pressures of the moment than by any objective criteria. Within those parameters, regulatory officials will be given considerable latitude to interpret legislative *intent,* that is, the spirit rather than the letter of the law. That interpretive act will not occur in a vacuum; it will be influenced both by the regulators’ reading of the intentions of the legislature as well as by their interaction with the multiple stakeholders who, in all likelihood, also had considerable input into the creation of the original legislation. Each participant in that interpretation will have several and usually conflicting priorities. First, all will share the hope that whatever struggle occurs over dotting the I’s and crossing the T’s, it will not become so disruptive or contentious that it shatters the regulatory regime that has been created. In most cases, both regulators and those regulated have a stake in playing the game that has been created for them (winning, to be sure, the most they can) but not in fundamentally changing the nature of the game. In that game, they are the “insiders,” and changing the game carries as many risks as potential benefits. From their perspective, this is a game that will be played over and over for incremental wins and losses, not a zero-sum, winner-takes-all contest.

All the players in this regulatory dance will play to – and be held accountable by – multiple constituencies. To be sure, their first loyalties lie with the agency, or industry, or public interest group they directly represent. In the eyes of their superiors, they must "win" enough to justify their existence. This is termed *vertical accountability,* that is, responsibility to one's superiors and sponsors for the successful advocacy of their cause. But "winning" will have different meanings. For the direct stakeholders, "winning" is measured by policy impact; tilting the regulations in the desired direction and staying within the generally accepted parameters so that no one cries "foul."   For the regulatory agencies, however, "winning" is about how skillfully they have managed the process and led the way toward whatever compromise emerges. In the best of all worlds, at least from their perspective, "regulation" means finding compromise that will lead to voluntary compliance, not enforcing rules through sanctions or legal action.

All the players in the game also will have an equally important responsibility to one another for playing by the rules and maintaining the viability of the regulatory process. This is termed *horizontal accountability,* and success is measured not in terms of policy outcomes but rather in terms of the smooth and predictable functioning of the regulatory process, in which all players have a stake.

Second, determining the identity of the legitimate players – the stakeholders – also is a disguised political process that changes with time. The initial passage of legislation and the choice of regulatory agency (ies) partially defines that playing field. That legislation resulted from a process of structured consultation, usually taking place both through legislative hearings in which virtually all stakeholders have given testimony and through the participation of the regulatory agencies which possess acknowledged expertise in the area. Under normal conditions, that consultation is weighted heavily toward those with the greatest stake in the outcome both in the private sector and in government. Representatives of what may be termed the "loyal opposition" – the ACLU or trade unions would be good examples in this case - are invited to have their say, and even token participation of more radical opponents – CASPIAN, in this case - is encouraged.

The important point is that such initial consultation legitimates certain stakeholders and brings them within the accepted policy community, and inevitably marginalizes or excludes others. That distinction between the "ins" and the "outs" is likely to be institutionalized as a part of the subsequent regulatory process. All other things being equal, the identity and relative clout of these players will be institutionalized over time, both through the emergence of time-honored "iron triangles" linking legislative committees, lobbies, and private sector advocacy groups and through the mobility of individual lobbyists and policy makers between government and private sector employment.

But all other things are not always equal, and membership in this insider circle can be subject to challenge. To be sure, all of the "ins" have at least some interest in maintaining the boundaries that have made them a legitimate part of the process. But this does not guarantee tranquility. Marginalized or excluded advocacy groups will seek a greater role, frequently through mobilizing broader public support, as CASPIAN already has done and as religious groups may attempt to do. Even within the in-group, there will remain a constant tension over the relative importance of each participant. If regulatory activities are delegated to several government agencies, there is the constant threat of turf wars and other jurisdictional disputes. As in all politics, the game is never really over; it has just been institutionalized on a different playing field.

Maintenance of the rules of engagement among the in-groups is also a part of an ongoing political process. In terms of formal regulation, "lead" agencies are usually designated and subordinate or more peripheral agencies are expected to take their cues from the actions of the primary regulators. In the case of RFID regulation, the identity of the "lead" agencies may vary in accordance with the purpose of regulation. For many issues, the Federal Trade Commission will be designated as the "lead" agency; but for other concerns, primacy may go to the Labor Department, the Environmental Protection Agency, or the Occupational Safety and Health Administration. To the extent either legal or international issues arise – and they are inevitable given the nature of the technology – then appropriate divisions of the Justice Department, the Commerce Department, or the State Department may also be expected to weigh in. This point is that each will bring its own priorities and organizational cultures to the mix. Jurisdictional disputes over *who* regulates *what* will be complicated by the differing perspectives and standard operating procedures of competing regulatory agencies. As with all regulatory activities, over time the rules of engagement will be worked out, enforced and sustained both by an emerging consensus among the various regulators about the original intent of the legislation and by common agreement on the mutually acceptable benefits of playing within the lines.

Maintaining the boundaries between the regulatory agencies, the advocacy groups, and their broader constituencies also is an ongoing and sometimes barely concealed political struggle. Each has an interest in pressing its own case up to a point – the regulatory agencies actually regulating and affirming their power as the final decision maker; the advocacy groups in advancing the cause of their constituencies; and the constituencies themselves in keeping pressure on the advocacy groups to stay in touch with the grassroots and represent their interests as effectively as possible. But none has a real interest in disrupting a stable and mutually beneficial relationship among the three players in this relationship. The regulators should not over-regulate, and advocacy groups should not over advocate, and the constituencies should not press their spokespersons to be disruptively aggressive. All must accept the political wisdom of the adage "half a loaf is better than none." But the wisdom of that adage is sometimes hard to recognize in a world in which short-term advantage may seem preferable to long-term stability. In that setting, it is sometimes all too tempting to test the boundaries of these relationships, especially if new issues have arisen, which is likely with a rapidly developing new technology like RFID, or if the relationships among the players have been recently defined and lack the time-honored stability of long-standing iron triangles.

A final word about the politics of regulation is in order. Like any political formula, it institutionalizes a consensus about the relationship between choices made in the free market and choices made by public institutions. As we have noted above, the nature of RFID technology itself and the broader concerns about its impact on society lend themselves to a recurring debate about how long any regulatory regime will remain adequate. As RFID technology takes hold – and more importantly from our perspective, as its identity as a political issue evolves – there will probably be several rounds of an all-too-familiar debate that occurs on many rapidly evolving political issues. It will probably go something like this: “We’ve already decided that,” some will argue, seeking to sustain the existing regulatory regime which institutionalizes their participation and advances their cause within acceptable parameters. The counter-argument will be “That was then, this is now,” and it will be heard from those who believe that some technical or social impact threshold has been passed that justifies in raising the question once again as a fundamental policy choice. Which of these succeeds depends both on the technical and social merits of the arguments – sometimes things do change so fundamentally that going back to the drawing board is justified – and/or the political skills of those who advocate continuity or change. The purposeful ambiguity of “and/or” is why the RFID community occasionally should listen to specialists in politics of public policy formation, and why those specialists should look seriously at the emergence of RFID technology as a new and instructive case study of how technology and politics interact.