RFID LAW JOURNAL

YOUR RFID LEGAL RESOURCE™ © 2006 RFID LAW JOURNAL, LLC. LEARN MORE AT WWW.RFIDLAWJOURNAL.COM.

FRIDAY, SEPTEMBER 15, 2006

The Elephant in the Room - Making Sense of the RFID Privacy Debate

RFID Law Journal
Newsletter No. 12
September 15, 2006

In terms of "mass deployment" experience, RFID is an early stage technology even though its history can be traced back several decades. In recent years, RFID started growing up, especially in connection with the rollout of several large initiatives by both the U.S. federal government (e.g., the Department of Defense) and several major retailers (e.g., Wal-Mart, Metro, Target, Albertson's, Best Buy, etc.). These early adopters are the auto identification technology industry's leading participants and enablers, and they recognize that these latest mass deployment efforts place them near the tipping point of realizing significantly enhanced capabilities for tracking objects within their supply chains. In their line of sight, the early adopter supply chain managers can visualize RFID grid systems facilitating substantially improved visibility of their institutions' shop floors, distribution warehouse, depots, etc. In our view, it doesn't seem likely that attorneys or policy makers will be dissuading these institutions from moving ahead with their deployments of 'supply chain' (object-based) applications.

But the same RFID technology that is capable of yielding a plenary vision of objects within a supply chain may also provide a security professional with similar visibility for tracking people. As governmental institutions increase their investments in such people tracking applications, it is increasingly likely that privacy advocates will ratchet up their objections to human tracking applications.

Industry advocates and many laissez-faire policy makers share the vision that new technologies, like RFID, require incubation, and after sufficient experience, would consider legislation or regulations following such world experience. On the other hand, privacy pundits suggest that the usage of RFID presents security and privacy concerns, especially in the context of human tracking applications, and would mandate legislation to control its deployment.

The Important Policy Question

Should policy makers rely upon existing legal frameworks to combat security concerns or are additional laws or restrictions required at the federal and/or state level with respect to RFID's usage?

Federal Government Policymakers are Educating Themselves about the Issues

At this point, both branches of the federal government are learning more about auto identification technology. It's fair to assume that these legislators and policy makers will increasingly thinking about privacy and security issues. Do existing laws sufficiently address legitimate concerns? Would it be jumping the gun to dictate detailed procedures without sufficient experimentation into potential applications at this stage?

In December, 2004, the Executive Branch explicitly called upon federal agency heads (see GSA Bulletin FMR B-7 (Radio Frequency Identification)) to review their processes and consider strategies for the future use of RFID technologies with a view toward improving personal property management, asset visibility, and maintenance practices and facilitating supply chain management improvement. (In other words, namely object-based supply chain applications.) As a result of this directive, many federal agencies have proactively considered RFID deployment, with more than a dozen agencies currently engaged in RFID-enabled projects. Having started its work with RFID nearly a decade earlier, the DoD is leading the way in terms of RFID supply chain (object-based) applications.[1]

More recently, Congress entered into RFID policy discussions.

Among other things, Senators Dorgan and Cornyn recently launched a RFID Caucus to facilitate a better understanding of the RFID industry and its technology. Earlier this year, Congressmen pushed on the FDA to speed up its e-pedigree rollout. RFID industry participants can only hope that this enthusiasm for educating itself about RFID won't lead to an effort to legislate it (as has been the case at the state level).[2] Indeed, industry participants contend that the RFID market is fragile and nascent, requires a chance to find its efficiencies. For them, the unfortunate side effect of inappropriate legislation is its ability to stunt the deployment of a promising technology.

Department of Homeland Security ("DHS")

At present, at least one significant federal agency, the Department of Homeland Security, has expressed itself, though it's unclear that those responsible for articulating the DHS's views on privacy share the same objectives as those actually responsible for ensuring that the nation's borders are safe.

In May, 2006, drafters of a report entitled "The Use of RFID for Human Identification" for the DHS Emerging Applications and Technology Subcommittee to the Full Privacy and Integrity Advisory Committee criticized the use of RFID devices for human identification purposes and recommended that DHS disfavor its use for human identity tracking. Simply put, these policy makers advocate blocking all 'RFID' applications (for human tracking) early in the adoption cycle. Such a policy would include blocking or unwinding usage of RFID for the SENTRI and NEXUS 'trusted' traveler cards, the 'laser visa' Mexican border crossing card, and the Free & Secure Trade Card for truck drivers.

There is little debate that the U.S./Mexican border is a security mess. Our Congress is considering spending billions of dollars to construct and maintain a 700-mile fence -- akin to deploying a 13th century moat instead of 21st century enabled security drones to address the problem. Most Homeland Security specialists recognize that better security will likely require the use of a more effective mix of technology and human intelligence deployment, as the task of managing millions of people crossing over this border is googlistic. Such an effort might include building a moat, but it's difficult to imagine entirely ruling out the use of RFID applications at this stage.

Having heard the DHS officials rave about the US VISIT program at FOSE in March, 2006, “The Use of RFID for Human Identification” report is a bit confounding. DHS is experimenting with RFID, and other auto identification technologies, to leverage its manpower. One might think of the U.S. VISIT’s ‘trusted’ traveler program as an entrepreneurial endeavor that balances risks in a fairly measured way. DHS allows “trusted” aliens, i.e., individuals who (i) shuttle themselves back-and-forth across the border frequently (think “commuter”) and (ii) submit themselves to a pre-screening background check, to commute with the ease of an E-Z Pass commuter. While this particular RFID application may not be without some risks (e.g., terrorist steals trusted traveler’s car to cross border), this RFID-enabled program could free up DHS manpower, and in doing so, allow DHS agents to focus their energies on higher threats than trusted commuters.

The smart-card industry has noted that the deployment of RFID technology for tracking and authenticating human identities is not as secure as a contactless smart-card which protects individual privacy and secures the identity of individual users. However, that really misses the point of why DHS is using RFID technology within its U.S. VISIT program. It is isn’t about controlling access in a Level 5 Security Area. It isn’t about the existence of more effective alternatives for identification, e.g., biometrics. It isn’t about guaranteeing aliens with the same ‘right of privacy’ the government must afford U.S. citizens under the U.S. Constitution. It’s about designing and implementing an opt-in program for ‘trusted’ travelers who submit themselves to the inconvenience of a background check and install a tag into their vehicles for the purpose of affording a slightly more convenient commute. The ‘dividend’ for DHS is freeing up manpower to concentrate on greater threats. Given its significant manpower restrictions, DHS requires all the leverage it can muster, and it probably need more breathing room, not less, to find the optimal automation tools to solve the border patrol problem.

A few thoughts on Commercially-Developed Human Tracking Applications

One cannot discuss auto identification technologies and privacy without looking at ongoing commercial development. While entrepreneurs are developing a variety of human and object tracking tools, most reside on the supply side (i.e., object tracking) of the equation. Commercial development of human tracking tools is stirring the privacy policy pot.

One of the leading developers of ‘people tracking’ RFID applications is VeriChip, a subsidiary of publicly-traded Applied Digital Solutions, Inc. (http://www.verichip.com/). VeriChip is the developer, manufacturer and marketer of customized RFID solutions, including a number of applications for human tracking. It goes without saying that a couple of privacy groups are critical of several of its products. However, upon examination of VeriChip’s online product catalog, its bread-and-butter commercial products appear to be largely “opt-in” applications. Among other things, its website touts wander protection, infant protection and medical emergency protection. In each case, VeriChip lays out the facts for why a consumer might want purchase such products. For example, noting that 98,000 deaths are annually attributed to medical error in the United States, VeriChip supports the case for its medical emergency protection product, which consists of an implantable microchip containing a 16-digit proprietary number that hospital physicians can use to access, for example, an unconscious patient’s medical information from VeriChip’s secure database. This VeriChip product is presumably sold on a case-by-case, story-by-story basis (e.g., it saved my life, and it can do so for you, too), and given the aging U.S. population, may fuel growth of this company for the next decade. Taking a Libertarian perspective on such deployments, even a hardline privacy advocate might accept such opt-in ‘human tracing’ applications of RFID.

Some thoughts on Expanding Human Tracking Applications

How would the arguments unfold if it were the case that one or more governmental agencies purchased and deployed, for example, VeriChip’s implantable microchips in their own employees? That scenario usually draws a fairly strong line of demarcation from privacy advocates. While it may not sit comfortably in the stomach of many of us, certain agencies, like the Department of Defense, could likely articulate some supportable reasons for enacting such policies, such as justifying the use of the implantable microchips to protect the safety and security of soldiers. Deployment would arguably save some lives because the technology would give personnel exactly the right information at critical times, and as such, support the "Agile WarFighter" initiative.[3] Would other federal and state agencies extend such arguments to include, for example, first responders? Other federal employees? Like other intrusions, such as the pre-mission inoculation of soldiers (and others at risk) with a host of vaccines, would an implant procedure be deemed just another condition of their employment?[4] No matter how you personally feel about this issue (and no matter how compelling of a case you can build in favor of deployment), it's a fairly safe bet that any mass deployment of such human tracking applications within the federal government would likely arise only after a vociferous set of objections are raised by privacy advocates.

If marking members of the military or first responders bothers your gut, what kind of scrutiny would be required to justify the deployment of such tracking technologies among their social opposites, i.e., convicted felons? Would it be appropriate to use such technology to track individuals during their probations? Can our judicial system rely upon RFID and related technologies (e.g., RFID or another A.I.T. coupled with GPS) to track non-violent, convicted felons who are, for example, subject to home arrest? Would it save precious funds, meaning it justifies itself based on its ROI? Should we set up RFID grids in our nation's prisons to promote safer interactions among prisoners? (Check out the following site to see how our prisons can deploy RFID identification tags to track prisoners: http://www.pdcorp.com/law-enforcement/rfid_wristbands.html). Should RFID (coupled with other technologies such as GPS) be an enabling technology to track sex offenders?

What about approving deployments of RFID technology offshore? Should the U.S. government allow foreign powers, such as the Chinese military, to acquire U.S. technology for either object or people tracking applications?[5] What if an unsavory dictatorship were interested in acquiring the technology? In such case, would it be in the U.S. national interest (in addition to its citizens' "moral" interest) to block the sale of such technology?

Some Initial Conclusions about the Elephant in the Room

Although RFID is a nascent technology, it is a good bet that as the DoD and Wal-Mart supply chain deployments pick up steam in the coming year, policy makers, industry proponents and attorneys alike will be hearing about a variety of new applications being introduced by the RFID industry. In considering new "privacy" legislation, policy makers should be careful not to unduly restrict technological innovation.[6] Institutions require time to gain experience with RFID and other auto identification technologies, and policy makers must craft wise rules based upon hardened experience. The RFID industry and its proponents need to work together with policy makers and legislatures to ensure that optimal policies for deployment evolve over time.

You can reach the DHS' draft report "The Use of RFID for Human Identification – A Draft Report from DHS Emerging Applications and Technology Subcommittee to the Full Privacy and Integrity Advisory Committee" (2006) at: http://www.dhs.gov/interweb/assetlibrary/privacy_advcom_rpt_rfid_draft.pd.

Learn more about RFID legal issues at http://www.rfidlawjournal.com/. You may contact our editor about this publication at editor@RFIDLawJournal.com. The information provided herein is for your informational purposes only and is not to be construed as legal or other advice (including, without limitation, investment advice) or as a substitute for legal counsel or other such advice. Online readers should not act upon this information without seeking professional counsel from a trusted advisor. Usage of the this website is subject to the terms set forth at our website: www.rfidlawjournal.com.

[1] As discussed below, will the DoD also lead the way into 'human tracking' applications, or will the legislative and/executive branch take such applications off the table?
[2] The RFID industry needs to take a more active in educating legislatures (both at the state and federal level) about the technology so that, in an effort to 'do something,' the legislators don't destroy a good technology in an effort to regulate conduct.
[3] There is a fairly pivotal assumption: the implantable chip wouldn't expose soldiers to additional risks of detection, etc.

[4] Mining is one of a number of private sector jobs where its use could become a standard condition of employment based on safety reasons.

[5] China is perhaps a poor example, as it is clearly among the countries which will be aggressively adopting the object-based technology within the supply chain.

[6] As a practical matter, the vast majority of expenditures (by both government and private companies) are taking place on the object-based, supply chain side. Even on the supply chain side of the business, this is an early stage industry; with "large" RFID companies hitting $10m in quarterly sales, it is unlikely that much more than small, controlled pilots will be occurring with respect to human tracking applications in the coming few years.

POSTED BY RFID LAW JOURNAL AT 9:39 PM