PROGRESSIVE POLICY INSTITUTE

Policy Report
October 2004

Radio Frequency Identification

Little Devices Making Big Waves

by Julie Hutto and Robert D. Atkinson

The Internet gave computers around the world a single network for sharing data. Now, the emerging technology of radio frequency identification (RFID) promises to create a vast network of *things*—wirelessly linking together everything from animals in migration for scientific research, to building movements in earthquakes, to the vast array of products that businesses make, retailers sell, and consumers buy. In its simplest form, RFID technology can take the form of a tag, potentially costing just pennies, much like the standard barcode tags on products in the supermarket. The difference is that while it takes a laser to scan a standard barcode and read its Universal Product Code (UPC), an RFID tag stores its identifying code on a tiny microchip and transmits it wirelessly to a reader device. That design allows more tags to be scanned at once from further away, and it allows individual items—not just types of items—to be assigned unique identifying codes.

The advent of standard barcodes brought tremendous efficiency gains in the distribution and retail industries, and RFID devices now hold even greater promise. Wal-Mart and other industry leaders have begun to introduce RFID technology into their supply chains, the Food and Drug Administration has recommended their ubiquitous use on pharmaceuticals, and the Department of Defense plans to boost its use of the tags this year.[1] The potential benefits to the economy and consumers are vast: RFID tags may facilitate dramatically reduced supply-chain costs, better inventory management, automated store checkout, reduced theft, more accurate and efficient product recall, improved counterfeit drug prevention, and a host of other benefits.

Yet despite the tremendous potential benefits of RFID technology, privacy advocates worry it could lead to more detailed tracking of the products we buy, maybe even to the level of taking inventory of what is in our homes and what is on our person at any given time. Arguing that stores, corporations, and even libraries will use the technology to spy on people, RFID critics have threatened boycotts to derail the

Julie Hutto is a policy assistant at the Progressive Policy Institute.
Robert D. Atkinson is vice president of PPI and director of its Technology & New Economy Project.

"One person with a belief is a social power equal to ninety-nine who have only interests."
—John Stuart Mill

The Progressive Policy Institute

The Progressive Policy Institute is a catalyst for political change and renewal. Its mission is to modernize progressive politics and governance for the 21st century. Moving beyond the left-right debates of the last century, PPI is a prolific source of the Third Way thinking that is reshaping politics both in the United States and around the world.

PPI invents new ways to advance enduring progressive principles: equal opportunity, mutual responsibility, civic enterprise, public sector reform, national strength, and collective security. Its "progressive market strategy" embraces economic innovation, fiscal discipline, and open markets, while also equipping working families with new tools for success. Its signature policy blueprints include national service, community policing, and a social compact that requires and rewards work; new public schools based on accountability, choice, and customization; a networked government that uses information technology to break down bureaucratic barriers; pollution trading markets and other steps toward a clean energy economy; a citizen-centered approach to universal health care and a progressive internationalism that commits America's strength to the defense of liberal democracy.

Rejecting tired dogmas, PPI brings a spirit of radical pragmatism and experimentation to the challenge of restoring our collective problem-solving capacities—and thereby reviving public confidence in what progressive governance can accomplish.

The Progressive Policy Institute is a project of the Third Way Foundation.
www.ppionline.org

PPI
PROGRESSIVE POLICY INSTITUTE

technology's adoption. In response, a number of companies have postponed item-level RFID programs and lawmakers in several states and the U.S. Congress have introduced legislation that, if passed, would curtail the use of RFID technology.[2]

Yet the privacy alarms being raised are at best premature and at worst hypothetical and impractical. Because this is such a promising yet nascent technological application, PPI believes that the call for RFID legislation is not yet warranted. Instead, industry should continue its efforts to educate customers about RFID technology and to notify them when they purchase items with RFID tags. Government, in turn, should actively monitor industry efforts to develop and abide by a set of RFID self-regulatory best practices that includes notification.

What is RFID?

An RFID tag uses a tiny computer chip to store information about a product or an item in the form of a uniquely numbered code, an Electronic Product Code (EPC). An EPC is quite like a Universal Product Code (UPC) on a standard barcode. But while standard barcodes are read with lasers, RFID readers use radio waves to read information from RFID tags. Because the EPC is a unique 96-bit number, it can correspond to more information in a database, which allows each specific item to be identified (such as a particular shaver), not just a type of product. An RFID tag will generally not have a power supply of its own. In that way, it is passive, like a copier machine on sleep mode. When its tiny antenna picks up a radio signal

from an electronic reader, the radio wave energy sent by the reader provides the power for the tag to reply.[3] The awoken tag emits the information contained in its chip, allowing the reader to identify it. RFID technology is a great improvement over labor-intensive barcodes for several reasons. RFID readers: 1) have a larger read range of up to a few feet; 2) do not have to be within line of sight of the products; and 3) can identify multiple items at once.

RFID technology is already a part of the landscape in cell phones, car security, and ID badges used to access commercial buildings and parking structures all over America. In fact, the technology has actually been around since World War II, but RFID devices can now fit on a microchip barely noticeable to consumers, and cost just pennies when produced in large quantities. As a result, many new and important uses for the tags have emerged and countless others will likely be discovered. For example, some ranchers have experimented with putting RFID tags on cattle to monitor the potential spread of mad cow disease. If an outbreak were to hit the United States, an RFID tag on the packaging of beef could identify the producer and the animal it came from. In another application, pet owners have implanted RFID chips in some 50 million pets nationwide to better identify lost animals. The passes that speed customers through tollbooths and metro turnstiles also use the technology. But the real economic benefits will come when RFID is ubiquitous in commercial supply chains.

RFID tags are not yet on individual products, like shavers or lipsticks, and until the costs fall far enough and technical issues are resolved, they probably will not be. That could take several years. However, large retailers such as Wal-Mart have started to require that their suppliers put them on the packaging of large pallets and cases of goods to better monitor the progress of shipments. For example, as a pallet is shipped from a factory, put on a truck, moved to a warehouse, and delivered to a particular store, the pallet is automatically tracked each step along the way, significantly increasing efficiency and reducing costs. Because products and packaging are all different shapes and sizes, it would be too costly or time-consuming to track all goods with barcodes. But with RFID tags, companies can scan in bulk and at greater distances. One analyst estimates that if RFID tags were widely deployed, retailers could reduce standing inventories by 5 percent, warehouse labor by 7.5 percent, and product losses by 1 percent of sales.[5] These would be significant savings in an economy in which retail trade totaled $1.09 trillion in 2002.[6] And the savings would not just be in the commercial sector. Governmental adoption of RFID could lead to significant savings and other benefits. Finally, RFID could also help boost the prospects of the IT industry itself as companies buy chips, software, and readers.[7]

It is important to note that these benefits will accrue to consumers. A key strategy of RFID opponents is to argue that the costs in the form of potential lost privacy are great and they are all borne by the consumer, while the benefits accrue solely to businesses. But if this were true, then as retailers used new

Figure 1

An RFID tag attached to the back of a box behind the traditional barcode. See EPC logo above the label.[4]

technology over the last 50 years to boost productivity, their profits should have soared. In reality, fierce competition requires retailers to quickly pass marginal savings on to consumers.

While companies cannot currently afford to tag individual products with RFID technology, as costs fall, many products—especially ones costing more than a few dollars—will likely be tagged, either in the packaging or in the product itself. The former option would allow consumers the choice of discarding the RFID tags just as they would a stick-on barcode label. The later option would not allow for easy removal, but would open up further uses for the tags.

In either case, RFID tags would allow customers to walk their shopping carts by an electronic reader that would tally up the total cost of their purchases and charge them, spitting out a receipt. Stores could do a much better job of preventing popular items from going out of stock so consumers do not have to settle for second choices, or make additional trips to find what they need. With barcodes, inventory management is still a labor-intensive and costly endeavor; RFID tags would allow more of it to be automated.[8] Moreover, RFID-tagged goods would lead to lower prices because they prevent backroom theft and shoplifting more effectively, two major expenses for retailers.[9] Currently, some popular anti-theft devices use radio frequency technology by simply triggering an alarm system at the exit, but RFID tags, with their identifying EPC, can help stores to better track and understand theft patterns. RFID tags could help ensure product quality, allowing expired perishable goods to be removed more quickly from shelves.

RFID tags permanently embedded in individual products could provide a host of benefits to consumers at home. For example, they could help with product recall by enabling consumers to have their specific product scanned to see if it is subject to a recall. Since RFID tags would uniquely identify products, a recall could zero in on a particular defective batch of goods, for instance, instead of recalling an entire product line. In more futuristic scenarios, RFID tags could help consumers by monitoring food supplies, automatically generating shopping lists of items that have been consumed, and automatically giving the microwave cooking instructions on a product.

These latter benefits are years away and, indeed, use in the supply chain is just beginning. Though Wal-Mart announced in the summer of 2003 that it would require some of its suppliers to put RFID tags on all shipments sent to its Dallas distribution center, one study found that only 25 percent of these suppliers might be able comply with that request by January of 2005.[10] Companies have had several technical problems implementing RFID, such as the failure of electronic readers to read all the tags present, or accurately read RFID tags through metal or liquid. To introduce RFID technology, companies face high start-up costs, including $1,000 per electronic reader, which contributes to hesitation in adopting the technology. Even greater cost is incurred in integrating RFID data into other company systems to reap the benefits from RFID data. However, as the technology is deployed, costs are expected to go down and effective use is expected to rise.

Premature Objections to RFID Technology

Despite the fact that the great promise of RFID technology is still years away, privacy groups are already using hypothetical scenarios of possible RFID abuses to fan public fears in an attempt to mobilize an anti-RFID public relations campaign. They invoke images of citizen tracking to provoke strong reactions from consumers.[11]

In November 2003, a coalition of groups including the American Civil Liberties Union, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and led by the Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN),[12] released

a "Position Statement on the Use of RFID on Consumer Products," which called for a "moratorium" on RFID technology to allow a full assessment of the impact of the technology.[13] Other advocacy groups have launched highly visible consumer boycotts that have successfully caused several big companies to delay their RFID plans.[14] Privacy advocates have also unsuccessfully tried to convince the San Francisco library system to abandon its proposal to put RFID tags on its library books, a measure that would allow libraries to cut costs significantly and in turn spend more money on books and/or extend service hours. RFID opponents sought to block the library system's use of RFID tags not only because they feared greater "tracking" and discovery of personal reading habits, but out of apprehension that if libraries adopted the technology it would become more legitimate in the eyes of the public and thus spread to commercial and other governmental applications.[15] Opponents seem willing to object to RFID use by government and the private sector even if it means forgoing lower prices for consumers and more efficient public services for citizens.

These kinds of advocacy campaigns have led a number of state lawmakers to propose legislation to regulate the use of RFID technology. Utah's "Right to Know Act" and similar legislation introduced in California and Missouri—and possibly more states in the near future—seek to preempt privacy violations.[16] In addition, the "Opt Out of ID Chips Act" was introduced in the U.S. Congress in June 2004, and has been referred to committee. Some members of Congress have in turn begun to publicly discuss and raise warnings about RFID.[17]

Privacy advocates argue that RFID, which some refer to as barcodes on steroids, would violate consumer privacy in three types of situations: (1) tracking consumer behavior in stores; (2) collecting information about purchases that could link personal information with purchased goods; and (3) collecting information outside of stores when rogue and hidden RFID readers might identify what someone has stashed away in her purse. Each fear is overblown.[18]

In-store tracking: Privacy advocates worry that retailers will track consumers in their stores, either by tracking the things on their person or by using "smart shelves"—shelves with readers attached to them—to monitor consumers as they simply browse around a store, before they have even bought anything. Privacy advocates point to field tests in Oklahoma and others in Massachusetts that were planned but cancelled in which the removal of an item from a smart shelf triggered a surveillance camera to take a photo. Companies might do this as part of their existing programs to better understand in-store consumer behavior so they can in turn do such things as better place products and deter theft. But this sort of targeted monitoring is no different from regular video surveillance in stores, which courts have consistently ruled is legal and does not violate privacy, and which stores keep private. Moreover, privacy advocates do not complain when store employees monitor this type of consumer behavior surreptitiously, or when a security guard keeps an eye on the store and makes sure no one puts a product into their pocket. The reality is that, as with surveillance cameras, consumers will get used to RFID technology over time and will develop appropriate expectations about the level of privacy they have in stores.

Tracking personal information: Of all the concerns over RFID, the notion that it enables stores to better link purchases to personally identifiable information (PII) is perhaps the most misguided. Privacy advocates claim that when a consumer swipes her credit card (or library card) at the checkout counter, the store will then link her personal information with the item she has just purchased and even save her name on the RFID tag. Yet the only differences between RFID and standard barcodes with respect to tracking PII is that products with RFID are read wirelessly while products with barcodes are read

with laser scanners, and instead of a store knowing that you bought a Sony Walkman, they now know exactly which Walkman you bought. With both RFID and barcodes, product information is collected, and in both cases, if consumers pay with a credit card or use a loyalty card, the store obtains information on what a particular person buys. Stores have been doing this for as long as credit cards and barcodes have existed, and it does not seem to bother the vast majority of consumers for the simple reason that there is little or no consumer harm involved. Even so, many federal and state laws, such as the Fair Credit Reporting Act, Health Insurance Portability and Accountability Act (HIPPA), and the Gramm-Leach-Billey Act, already regulate the use and reuse of much of this information. The fastest way for a retail company to lose business would be to disclose the personally sensitive buying patterns of their customers. For the small number of consumers who are worried about their privacy, there is a simple answer: Pay with cash and do not use a loyalty card. It is unlikely that stores would embed PII on the RFID tag itself at the time of purchase for the simple reason that it would scare away customers. Moreover, RFID tags do not store personal information largely because to do so would significantly raise the costs of the readers and chips without significantly adding to their value.[19]

Out-of-store rogue tracking: Privacy advocates worry that if consumer goods contain RFID chips, then all sorts of unauthorized tracking will occur—from strangers with access to an electronic reader discovering that someone is carrying a bottle of Prozac, to a representative from a market research firm driving by houses and reading the products in the homes, or even in trash cans. The position statement on RFID technology issued by CASPIAN and others warns that companies will use the RFID tags to track all your physical movements and purchasing habits.[20] These overblown claims against RFID, in which the technology becomes a magnifying glass into people's personal lives, either overestimate the technology or ignore applicable laws. Credit card companies already log all of your purchases, which can be used to piece together your movement, and nobody gets full access except police with a warrant. Rogue scanning seems unlikely. RFID tags, if left active, can only be read from a few feet away and cannot be read through metal, water, or most walls. A would-be privacy invader would have to buy a reader to gather information that has, if even accessible, limited gossip value. If a retailer or marketer tried to invade personal privacy and read tags intrusively, who would want to buy from them? The market or civil suits would end such practices. Furthermore, companies can encrypt the tags, which would make it next to impossible for electronic readers other than their own to detect and read their RFID tags.[21]

As far as house-scanning goes, readers have to be at a relatively close range to the product, so someone with an electronic reader could not get information about the products inside someone's home from the street. Moreover, in most public settings, it would be difficult to engage in surreptitious rogue tracking (especially if readers were placed in fixed locations), or to actually identify who was carrying what products.

The chain of events needed for rogue scanning to occur—a live tag still attached, a reader in very close proximity used without a person's notice, and access to product code information—suggests the likelihood is small.

This is not to say that there are not legitimate consumer privacy issues involved in the use of RFID technology, or that only a small share of consumers has concerns.[22] In particular, PPI believes that consumers should ideally have a right to know that the product they have purchased contains an RFID tag, and they should have a choice to discard or deactivate the tags after they leave the store. In order to respond to these two legitimate concerns, industry has already initiated a process of self-regulation that acknowledges and addresses the issues of notice

and choice. Both of the major manufacturers of RFID tags have developed RFID privacy policies, as have the retailers who plan to use them, including the EPCglobal network, a member-driven organization of industry leaders using RFID that includes Wal-Mart, Procter & Gamble, and Hewlett Packard.[23] Early on, EPCglobal developed a set of guidelines to address RFID privacy issues that focuses on four areas of concern: notification, choice, education, and security.[24] Retail suppliers already implementing RFID have developed a protocol whereby they attach a recognizable EPC logo next to the RFID tags indicating to the consumer that once he purchases a product he can remove and discard the tag. In addition, stores distribute flyers explaining to consumers what RFID tags are and how they can tell if there is one on the product they want to purchase. EPCglobal members are also committed to giving consumers the option of keeping or discarding RFID tags after they purchase a tagged item. The policy stops short of guaranteeing that tags will be disposable or that stores will deactivate them at checkout, but it serves as a steppingstone to further consideration of the issue.

It is also important to realize that RFID technology is still at an early stage, and like so many other IT applications, implementation policies and improvements in the technology could address many of these privacy concerns.[25] For example, some privacy advocates argue that the voluntary approach to removing tags does not go far enough; they propose that stores be required to disable tags at check out. To "kill" an RFID tag, the store could have another code that, if sent to the RFID tag, would deactivate it, rendering it unusable. The "kill-tag" requirement, however, is not necessarily the most effective approach. Many consumers may want to keep their tags active to use them in the ways mentioned above, as well as for receipt-less returns. Moreover, RFID tags could facilitate societal benefits, such as product recalls or identification of discarded goods containing toxic materials. Stores could choose to offer these services routinely or provide in-store locations to do it.

Another way to deactivate RFID tags is with blocker devices. RSA Security Inc. has developed an RFID jammer tag, virtually the same size as an RFID chip, which prevents a nearby electronic reader from accessing an RFID tag. If held near the tag, the jammer prevents a reader from activating the tag and retrieving the information stored on its chip. RSA is also working on an RFID chip with a privacy code included, which could be enabled to protect the information on it.

While technologies and policies could provide solutions, it is important to not let assumptions about what could be, no matter how far-fetched or impractical, raise privacy issues that in turn stop the use of RFID technologies. It is simply too early to determine what the RFID practices will be, let alone which ones are likely to become real privacy problems. Moreover, some of these purported solutions may turn out to be unneeded and unwanted and could significantly increase the costs of RFID and reduce the economic benefits. For example, if consumers were allowed to deactivate tags before check out, as some have advocated, their goods would have to be scanned manually by a clerk, thereby raising labor costs. Stores would likely pass those costs along in the form of higher prices for all customers, even those not concerned about RFID technology.[26]

What To Do

1. Given the fact that RFID is in its initial stages of deployment at the case and box level, and that the privacy harms envisioned are largely speculative, PPI believes that any legislation related to RFID is premature, and could inadvisably limit RFID use.

Legislating before real harms are identified increases the likelihood of overreaching and curbing uses of RFID tags that do not threaten

privacy, thus locking out some of the exciting potential applications of RFID. For instance, an early version of legislation in California would have required stores to deactivate RFID tags before the tagged product left the store and would have required affirmative consumer consent before using the tags. Such an "opt in" requirement would likely derail RFID use completely. Similarly, legislation called for by privacy advocates to regulate data aggregation and data sharing, which would require consumer choice and access and security standards, is not needed. As discussed above, stores have been collecting information on the products consumers buy for at least two decades and for the vast majority of products, the process remains an accepted part of American commerce.

It is too soon to consider legislation to prevent rogue tracking, given that the threat remains completely speculative. If it turns out that rogue tracking presents a real risk to privacy, however, the best response would be to outlaw it, the way that other intrusive activities in the wireless space have been outlawed (such as hidden video cameras in bathrooms, monitoring of cell phone conversations, and the like).

2. While PPI does not believe protective legislation is warranted at this time, Congress should monitor state legislative activities with the eye toward passing legislation to preempt restrictive and conflicting RFID legislation.

State regulation of RFID technology is particularly worrisome because, like virtually all public policy issues relating to the IT economy, the implementation of RFID tags is a national issue, since tagged goods cross state borders. One can only imagine the cost and confusion of complying with 50 unique laws. A patchwork system could eat away at the cost and efficiency benefits from RFID. Yet, states have undertaken such regulation before. For example, when barcodes were rolled out in the 1970s, some states passed laws requiring stores to place prices on the individual products, negating the cost savings of barcodes. If there is a role for legislation, it is at the federal, not state, level.

3. To the extent possible, the Department of Defense and other federal agencies using RFID should use commercial standards.[27]

It is important for the federal government not to create a separate RFID standard in conflict with the industry standard being developed by EPCglobal because federal adoption of RFID, particularly in the Defense Department and to some extent within the Department of Homeland Security, will play an important role in driving overall RFID adoption and lead to cost reductions in tags and readers.

4. While we believe that legislation is premature, the Federal Trade Commission should work with industry to encourage best practices and build on EPCglobal's set of standards to construct a more defined industry response to privacy concerns based on notification and choice.

If consumers are to accept RFID technology, industry will need to take privacy issues, particularly notice and choice, seriously. Negative public reaction could threaten RFID to the same degree as restrictive, premature legislation. Meanwhile, as retailers have already planned to do, they should: (1) label RFID-tagged items with a recognizable EPC logo; (2) indicate the location of the tag on the product; and (3) conduct a public information campaign, such as handing out informative flyers or posting signs in stores that have RFID tags. It will also be important for industry to provide notice to consumers when RFID readers are present. However, consumers should not have to sign a notification form, which would eat up the time saved by RFID tags. Ideally,

consumers should have the choice of whether or not to discard or deactivate RFID tags. But unlike notification, which is clear and manageable, the "kill tag" mechanism needs further investigation. As explained above, deactivating an RFID tag might limit its benefit to consumers, raise costs of implementation, and limit innovative applications.[28] While industry should continue to give consumers the choice of deactivating their tags, the government should not mandate that stores kill all RFID tags before they leave the store.

Conclusion

When barcodes and the Internet first appeared, they raised concerns among privacy advocates, but in the long run, both have proven to be extremely beneficial and acceptable to consumers. Moreover, many of the hypothetical scenarios privacy advocates raised did not occur, and other potential dangers were averted during planning and implementation. Indeed, one of the main reasons why the United States is the world leader in information technologies is precisely because we have forged ahead with innovation.

A major technological advancement, RFID tags are poised to stimulate growth; therefore, it is important to embrace them rather than stall or halt them altogether. RFID tags, like barcodes in their own time, could provide quicker and more efficient inventory of consumer goods and myriad other uses outside the retail setting. As RFID tags move into consumer goods, government and industry should cooperate to ensure consumer notification and look into the deactivation of RFID tags, but the government should not impede this very promising technological development.

Endnotes

[1] Brewin, Bob, "Setting the Stage for RFID: DOD to use radio technology at two distribution centers," *Information Week,* September 27, 2004.

[2] Utah's Radio Frequency Identification Right to Know Act, sponsored by state Rep. David Hogue, passed the Utah House of Representatives and is now in the Senate for review: Utah H.B. 251, March 5, 2004, *http://www.le.state.ut.us/~2004/htmdoc/hbillhtm/hb0251.htm*. Regulation of RFID was proposed in the California State Senate, but failed: California S.B. 1834, February 20, 2004, Amended April 1, 2004, *http://info.sen.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040401_amended_sen.pdf*. The Opt Out of ID Chips Act, H.R. 4673, sponsored by U.S. Rep. Gerald D. Kleczka (D-Wisc.), was introduced on June 23, 2004 and was then referred to committee: *http://thomas.loc.gov/cgi-bin/query/D?c108:1:./temp/~c108EwAkUd*.

[3] The security tags used on common everyday products sold in pharmacies also get their power from radio waves but they should not be confused with RFID tags. They are much simpler devices because they contain an integrated circuit instead of a microchip with an identifying code. When a shoplifter tries to leave the store without purchasing an item, the security tag's antenna picks up a signal from a receiver set up at the exit of the store, then sends out its own signal which is picked up by the transponder, triggering the alarm. The alarm does not go off for paying customers because the cashier disables a security tag at check out by blasting it with a strong frequency.

[4] Image courtesy of Hewlett-Packard.

[5] Lytel, David, "RFID: Investing in the Next Multi-Billion Dollar IT Opportunity," *Precursor*, November 12, 2003.

[6] "Gross-Domestic-Product-by-Industry Accounts, *Bureau of Economic Analysis*, *http://www.bea.doc.gov/bea/pn/GDPbyInd_GO_NAICS.xls*.

[7] One estimate suggests that RFID is the next multibillion IT opportunity, with sales reaching as much as $7 billion per year by 2008. Lytel, *op. cit.* In a recent study, Forrester Research found that 37 percent of "IT decision-makers" expect that even in the next year, RFID deployments will increase. Overby, Christine Spivey, "RFID's Influence on Technology Spending: The Technology Spending And Adoption Plans Of Firms Increasing RFID Efforts," *Forrester Research*, June 1, 2004.

[8] Several stores, including Wal-Mart and the German department store Metro, have experimented with "smart shelves" to monitor shelf inventory. They work by installing an electronic reader near a shelf that periodically scans it to make sure that all of the goods that have not been sold are still there. It allows suppliers to make sure that the shelves remain stocked with their products. If the shelf runs out of a certain product, the electronic reader would communicate electronically to a central database notifying store employees to restock the depleted item.

[9] Better security would lead to tremendous savings since retailers lose $200 billion to theft in the supply chain and $500 billion to counterfeiting each year. Frantz, Mark R., "The Buzz About Emerging RFID," *Retail Info Systems News*, March 27, 2003.

[10] Hines, Matt, "RFID Technology Hits a Wall, Study Says," *CNET.com News*, March 31, 2004, *http://news.com.com/RFID+deadline+hits+a+wall%2C+study+says/2100-1006_3-5182579.html*.

[11] It would be one thing if panicky hypothetical scenarios were coming only from paranoid individuals, but they are coming from leading privacy and civil liberties groups as well. For example, John Gilmore of the Electronic Frontier Foundation has speculated that RFID chips in people's clothes or tires could be used to direct smart missiles targeted at particular people, or be used to have smart bombs in the roadway that would only go off when the particular person's car drives over them: "John Gilmore's Horrific, Dystopian View of an RFID World," *Politech: Politics & Technology*, April 30, 2004, *http://www.politechbot.com/pipermail/politech/2004-April/000652.html*. Barry Steinhardt, director of the Technology and Liberty Program at the ACLU, spun the following scenario in order to whip up fear of RFID: "[Imagine] strolling around the city one evening, you happen upon a sex shop and pause for a moment to snicker at the curious items in the store's window. Then you continue on your way. However, unbeknownst to you, the store's Customer Identification System has detected a radio identification signal emitted by a computer chip in one of your credit cards, and is recording your identity and the date and time of your brief stop. A few weeks later, your spouse is surprised to find in the mail a lurid solicitation from the store mentioning your visit. You've got some explaining to do." Steinhardt, Barry, "Taming the Surveillance Monster," *CIO Magazine*, Fall/Winter 2003, *http://www.cio.com/archive/092203/steinhardt.html*. The problem with all these scenarios is that (1) they are not generally technologically possible; and (2) they are not going to happen, partly because they do not follow the logic of customer relations. For example, a surefire way for adult entertainment stores to lose business is to publicize the names of their customers.

[12] Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) has actively campaigned to stop grocery stores from providing discount cards to consumers, fearing a loss of privacy, *http://www.nocards.org*.

[13] "Position Statement on the Use of RFID on Consumer Products," *CASPIAN*, November 14, 2003, *http://www.privacyrights.org/ar/RFIDposition.htm*.

[14] In the last year and a half, Metro, a German supermarket chain; Benetton, an Italian clothing chain; and Wal-Mart all began to implement RFID, but then pulled back due to public outcry.

[15] "Privacy Risks of Radio Frequency Identification 'Tagging' of Library Books," *Electronic Frontier Foundation*, October 1, 2003, *http://www.eff.org/Privacy/Surveillance/RFID/20031002_sfpl_comments.php*.

[16] Other states that are considering RFID legislation include Maryland, Massachusetts, and Virginia. To further study the impact of RFID, Maryland has established a task force within its House of Delegates, and the Virginia Joint Commission on Technology and Science (JCOTS) held a hearing to discuss "invasive technologies."

[17] Leahy, Sen. Patrick, "The Dawn of Micro Monitoring: Its Promise, and its Challenges to Privacy and Security," *Conference on "Video Surveillance: Legal and Technological Challenges," Georgetown University Law Center*, March 23, 2004; Schakowsky, Rep. Jan, prepared opening statement for the Subcommittee on Commerce, Trade, and Consumer Protection's Hearing on "Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer," July 14, 2004, *http://www.house.gov/apps/list/press/il09_schakowsky/pr7_14_2004rfid.html*.

[18] Beyond privacy concerns, some argue that RFID tags have negative implications for personal health, electronic waste, and the radio spectrum. Others worry that the tags could interact with medicine inside a tagged pharmaceutical bottle. The privacy concerns, however, dominate the debate over RFID and are the focus of this report.

[19] When you consider that trillions of chips could be used in a year, adding even a few cents to the cost of the chip to allow it to store personally identifiable information (PII), would significantly raise costs.

[20] The statement warns: "when a consumer purchases a product with an EPC-compliant RFID tag, information about the consumer it could be added to the database automatically. Additional information could be logged in the file as the consumer goes about her business. 'Entered the Atlanta courthouse at 12:32. At Mobil Gas Station at 2:14pm'," (RFID Position Statement of Consumer Privacy and Civil Liberties Organization," *Privacy Rights Clearinghouse*, November 20, 2003, *http://www.privacyrights.org/ar/RFIDposition.htm)*. Besides implying that the tags could be easily and surreptitiously read, the scenario of tracking implies that companies would share their databases. In other words, Wal-Mart would share information with Mobil Oil and the Atlanta courthouse and the other places people go in order to compile a massive tracking database. Companies have every incentive to do the opposite. Moreover, if such practices were undertaken, the hue and cry raised would lead to such protests that companies would stop. While it is true that law enforcement could use this information, there are already clear procedures in place governing law enforcement access to and use of this information.

[21] Chachra, Vinod, "Personal Privacy and Use of RFID Technology in Libraries," *VTLS Inc.*, October 31, 2003.

[22] Forrester Research found that "twenty-one percent of U.S. consumers who are aware of RFID tags fear the prospect of companies tracking their purchases." Overby, Christine Spivey, "Commentary: An RFID Code of Conduct," *CNET News.com*, April 16, 2004.

[23] EPCglobal was an offshoot of the Auto-ID Center at MIT, which Kevin Ashton of Procter & Gamble, Sanjay Sarma of MIT, and representatives from Gillette formed in 1999 to develop RFID technology.

[24] "Guidelines on EPC for Consumer Products," *EPCglobal*, 2003, *http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html*.

[25] For example, this has been the case with the Internet privacy standard P3P.

[26] It is not likely that stores would charge a separate fee for those customers who want to manually scan their merchandise, because those sorts of special convenience fees tend to be unpopular.

[27] As to the relative security measures required by the Department of Defense, they could consider added functionality or features for RFID tags placed on sensitive materials.

[28] For example, a "smart refrigerator" that could keep inventory of its contents and print a grocery list of items that have run out.

Find this and other policy reports at **WWW.PPIONLINE.org**, *the official website of the Progressive Policy Institute.*

Now on PPIonline.org:

- ❒ **Technological Innovation Without Big Brother:** Privacy Principles for Government in the Information Age
  Robert D. Atkinson
- ❒ **Meeting the Offshoring Challenge**
  Robert D. Atkinson

Also from the PPI Technology and New Economy Project:

- ❒ **Confronting Digital Piracy**: Intellectual Property Protection in the Internet Era
  Shane Ham and Robert D. Atkinson
- ❒ **Unsatisfactory Progress:** The Bush Administration's Performance on E-Government Initiatives
  Robert D. Atkinson

If you would prefer to receive future reports via email, please contact the PPI Publications Department at **publications@dlcppi.org.**