BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 4, Number 7 July 2004

Articles

Case Report

News

www.bnai.com

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

CNIL held that obtaining data about third parties in this way without the knowledge of the e-mail recipients was contrary to Article 25 of the Law of January 6, 1978 which prohibits the collection of personal data through methods which are fraudulent, underhand or covert.

In the decision, CNIL warns French companies and the French public that if they use this software they will be in breach of French law and could be liable for up to five years imprisonment and a fine of EUR300,000 (£200,000).

This is another example of the development of highly invasive software which allows the covert monitoring and collection of information by electronic means thereby potentially infringing personal privacy. Rampell Software also makes a number of other software products which allow covert monitoring including one which allows the user to see everything that happens on his or her PC from anywhere in the world including who is using it and what they are doing on it.

Although at first sight being able to track whether or not an e-mail has been opened seems a useful tool, the amount of information collected by the "DidTheyReadIt" software clearly goes a long way beyond this, allowing the sender to find out additional information about the recipient which he or she might not want disclosed. This is certainly the finding of the French Data Protection Authority and anyone thinking of using software of a similar sort should consider the privacy and data protection implications very carefully – and avoid its use if they or any recipients are located in France.

The CNIL decision is available in French at:

www.cnil.fr/index.php?id=1602&news[uid]=177&cHash=5f39b9474d

By Andrew Johnston, an Associate in the IT and E-Commerce Group of Eversheds LLP; e-mail: andrewjohnston@eversheds.com

Technology

RFID Tags and Privacy

By Jim Harper, a lawyer in Washington, D.C. and Editor of the privacy advocacy website, Privacilla.org,. Jim also runs public policy consulting firm PolicyCounsel.Com and has previously served as counsel to the U.S. House Judiciary and the U.S. Senate Governmental Affairs Committee.

Radio frequency identification (RFID) technology promises many consumer benefits. With RFID, goods on trucks, in trains, and in warehouses can be inventoried without unloading and digging through pallets and packaging. Embedded in or attached to consumer products, RFID can improve customer convenience by permitting receipt-free returns and suppressing post-sale theft. As a personal identification device, RFID already enables keycard holders to quickly enter secure buildings and pass through toll gates.

But, as new communications and information storage technologies often do, RFID has also raised a variety of privacy concerns. Responding to the call of activist groups, state legislators have begun pushing legislation, and the U.S. Federal Trade Commission and U.S. Congress have instituted hearings to consider whether this nascent technology should be regulated.

As yet, RFID tags have seen limited deployments, so there is little real-world experience on which to ground discussions of the merits or demerits of regulation. As RFID technology comes into full use, various social forces will constrain it more suitably than would government regulation. RFID users face economic incentives and consumer preferences that will direct the technology's evolution in harmony with consumer interests. Meanwhile, consumers' easy access to defensive techniques and counter-technologies will complement existing laws that already protect privacy.

An unlikely threat to privacy, RFID technology will help producers, marketers, and retailers take major steps toward better understanding – and therefore better serving – the entire mix of consumer interests. Legislation to restrict the technology would be premature given the social forces that will shepherd RFID's comfortable assimilation into commercial and consumer society. Prompt deployment of, and experimentation with, RFID would best serve the interests of the public and the economy.

Understanding RFID

Before grappling with its policy implications, it is important to understand RFID technology, its limitations, and its significant advantages over predecessors like bar codes and static ID cards. RFID (sometimes also called dedicated short range communication, or DSRC) uses the radio frequency portion of the electromagnetic spectrum to uniquely identify objects. Good old radio communications and new efficiencies in fabrication and miniaturisation go into RFID devices that can help organise the production and delivery of goods, and enable personal identification in efficient new ways.

RFID is poised for use as an alternative to bar codes, those boxes of vertical bars and spaces that represent numbers and other symbols. The most familiar example of a bar code is the Uniform Product Code found on most consumer goods today. RFID is already used in some identification cards, in transportation access cards, and in the shipping and logistics industry.

RFID Components

RFID systems consist of three components in two combinations: a transceiver (transmitter/receiver) and antenna are usually combined as an RFID *reader*. A transponder (transmitter/responder) and antenna are combined to make an RFID *tag*. An RFID tag is read when the reader emits a radio signal that activates the transponder, which sends data back to the transceiver.

There are two types of transponders, which correlate to the two major types of RFID tags.

- *Passive* transponders and RFID tags have no energy source of their own, relying on the energy given off by the reader for the power to respond. Cheaper, passive RFID tags are the most likely to be used for consumer goods.
- An *active* transponder or tag has an internal power source, which it uses to generate a signal in response to a reader. Active transponders are more expensive than passive ones. They can communicate over miles like ordinary radio communications. They are commonly used in navigation systems for commercial and private aircraft.[1]

Frequencies Affect Capability and Cost

Low-frequency RFID systems (30 KHz to 500 KHz) have short transmission ranges of generally less than six feet. High-frequency RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer longer transmission ranges. In general, RFID systems are more expensive if they operate on higher frequencies.

Different frequencies also have characteristics that make them more or less useful for particular applications. Low-frequency RFID systems use less power and are better able to penetrate non-metallic substances. They are ideal for scanning objects with high-water content, such as fruit and liquids. Higher frequencies typically offer better range and can transfer data faster but they use more power and are less likely to pass through materials. Higher frequencies are useful for air-to-air and air-to-ground communications.

Chips and Data

The RFID tag stores data on a tiny computer chip. The cheapest and most common chip will be the read-only chip, which is likely to carry only a serial number. More expensive "read-write" chips allow new information to be added to the tag or written over existing information when the tag is within range of a reader. Writeable chips will be useful in some specialised applications such as maintaining maintenance records for vehicles or appliances, but they are more expensive than read-only chips and impractical for tracking less expensive items.

Once an RFID tag has returned data to the RFID reader, the data is then used in whatever way appropriate for the task at hand. Probably, the most common RFID systems will relate the serial numbers from read-only tags to other relevant and useful information in secure databases. RFID may be used to implement and record the sale of a consumer good at a checkout stand, to allow a keycard holder to enter a building, or for dozens of other purposes.

Advantages of RFID

Two advantages to RFID over bar codes are apparent. First, they do not require direct contact or a line of sight for scanning. Secondly, they can identify items individually rather than generically, which creates many interesting possibilities.

Scanning Without a Line of Sight Eases Inventory Tracking

When goods are purchased in grocery stores today, bar codes must be directly presented to a laser scanner in order to register. Clerks must turn products around and hold the bar codes, flat and clean, up to a reader. RFID scanning of products requires none of this; products will need only to be brought within the appropriate distance of a reader. Likely, future shoppers will walk through checkout lanes (or arches), registering their purchases and payment methods instantly, and never wait in line or interact with clerks.

The dominant early application of RFID in the consumer goods context will probably not be individual item labelling. Rather, early applications will track boxes, cartons, cases, and pallets of goods on trucks, in trains, and in warehouses. Today, an extraordinary amount of waste occurs when goods sit on loading docks spoiling, when they are shipped to the wrong locations, or when they sit idly in warehouses.

In April 2004, RFID tags debuted at Wal-Mart on pallets and containers of consumer products, and the company's remaining suppliers are expected to employ tags for inventory flow control over the coming years.[2] Thanks to RFID, inventorying can be done without unloading items and digging through pallets.

RFID systems can tell manufacturers very quickly when and where items have been sold so they can promptly manufacture and ship replacements. When RFID is used to squeeze waste and inefficiency out of the supply chain, the savings will be passed on to consumers and investors.

Individually Identifiable Items Mean Enhanced Safety and Convenience

The other advantage of RFID is its ability to identify items individually rather than generically. The typical RFID tag may contain about two kilobytes of data, which is enough for an individualised numeric code that identifies the tag distinctly from all others in the world.

The benefits of individualised identification are enormous. In terms of safety, RFID systems will be able to identify when drugs, meat, or other perishable products have expired or outlasted their "sell by" dates. RFID could also assist in recalling defective products. If, for example, tires manufactured at a certain plant on a certain date are recalled, the serial numbers on tags embedded in the sidewall of the tires can be correlated in a database to where and when they were manufactured.

Consumers may enjoy substantial convenience thanks to individualised identification as well. The serial number in an RFID tag on a shirt, for example, may be correlated in a

database to the purchaser and the payment method he or she used. If it does not fit, the purchaser can return it and receive a refund without a receipt.

Such personalisation may also allow RFID tags to significantly suppress theft and the black market for stolen goods. Tags built deep into consumer electronics, shop tools, computers, and the like will act as beacons identifying that an item is stolen. The serial number on the tag could be used to easily and quickly identify the store where it was sold, or the purchaser and owner of the item.

These are just some examples of how RFID's unique attributes – sightless scanning and individual identification – can benefit consumers. And many more imaginative RFID uses will emerge.

Fears Surrounding RFID

The potential power of RFID systems has given rise to concerns about the technology's effect on privacy. There are two routes by which RFID might be used to compromise consumers' privacy: direct and indirect monitoring.

Direct Monitoring of Individuals by Vendors

One fear is that someone in the manufacturing or sales chain will use information gleaned from RFID systems to learn information about or to track a consumer contrary to his or her interests and desires. While linking the serial number on an RFID tag back to the purchaser can have many substantial benefits, misuse of that same linkage may constitute a privacy invasion.

For example, RFID could be used to note a customer's purchases and then learn when the customer returns to the store – or at least when the associated RFID tag (perhaps in clothing) has done so. Conceivably, information like this could be used to develop a dossier about a consumer and his or her activities. The mere collection of too-detailed information may offend consumers' sense of privacy. Use of this information for marketing purposes may offend others, and other broader monitoring may compound the offence.

Questions about direct monitoring parallel longstanding debates about what retailers and marketers may do with consumer information they gather through transactions. This is not a new issue, but an extension of an old one.

Indirect Monitoring By Third Parties

The second way RFID systems may be used to compromise privacy is when an outsider to an RFID network uses the existence of RFID tags to read and collect personally identifiable information contrary to the interests of those monitored. Someone may scan an RFID tag and use further reading of the tag elsewhere as a proxy for the presence of the same individual in the second location. Collecting that information, or subsequently using it in various ways, may compromise privacy and threaten other interests.

For example, union operatives could surreptitiously scan for RFID tags on clothing, ID cards, and so on at the entrance to a right-to-work rally. When an RFID tag's serial number that was scanned at the rally arrives with a person at a union hall, he or she could face retaliation from the union.

Of course, for this method to successfully compromise privacy, it is necessary at some point to identify the person associated with the tag. This type of monitoring would be prone to significant error and it entails many challenges. But it is at least a conceivable way, the technology's opponents argue, that RFID could be used to invade privacy.

Concerns with indirect monitoring using RFID are similar to concerns over monitoring using surveillance cameras. Sometimes it is appropriate; other times it is not. Almost always, it is ineffective at deriving much in the way of useable personal information. Photographic surveillance seems much more powerful than RFID-based surveillance because it captures true personal information – an individual's appearance – on each "scan". RFID-based surveillance will capture the presence of a tag, which may or may not correlate to any individual.

Anti-RFID Advocacy and Inquiry

Reacting against its potential power, a variety of advocates and groups have come to oppose RFID technology. In November 2003, a group of consumer privacy and civil liberties groups issued a three-point position statement arguing for a wide variety of regulatory restrictions on RFID.[3] First, the groups called for RFID systems in the consumer goods context to be indefinitely delayed while a "formal technology assessment" is undertaken. Second, they argued for a welter of regulations on RFID systems. The "strong principles of fair information practices" they called for include a basket of information policies put forward by international bureaucrats in the Organisation for Economic Cooperation and Development and, in addition, amorphous concepts such as "openness," purpose specification, collection limitation, "accountability," and security safeguards. Finally, they called for an outright ban on certain potential practices, such as using RFID "in a fashion to eliminate or reduce anonymity," even though a common use of RFID today is in identification tags and badges.

Heeding the call of the technology's opponents, legislators in a number of states have introduced legislation to restrict RFID, and many more state legislators are considering it. Indulging the pro-regulation groups, the U.S. Federal Trade Commission (FTC) scheduled a June 2004 hearing to "facilitate discussion of core public policy issues and encourage the development of best practices that capitalise on the efficiencies generated by RFID without compromising consumers' privacy and security".[4] The *sub rosa* message is that U.S. federal bureaucrats, whose mission is to prevent fraud, deception, and unfair business practices, are poised to seek prospective regulation if the technology is not used in ways they deem appropriate.

RFID is an exciting new technology, but its capabilities have probably been over-hyped. It will bring substantial efficiencies to the supply chain, but probably not as much as proponents claim. It will give consumers useful conveniences such as receipt-free returns, but probably track people less well than opponents claim.

RFID technology is in an early stage of development. Activists are urging concerns unrelated to real-world experience, with potential harms to consumers unidentified. But substantial benefits from RFID are in the offing. The FTC and state legislatures should avoid intervention. Each of the many "principles" called for by pro-regulation activists may have its place, dictated by the actual interests involved in real implementations of RFID. But discussion of general RFID regulation is premature.

The use of RFID systems will be tempered by a variety of social forces whose influence will come to bear long before government regulation is relevant. Before regulators peer over the shoulder of the RFID community holding a regulatory hammer behind their backs, they should consider these influences and their role in managing technology deployment.

RFID "Regulation" Without New Law

A variety of social forces "regulate" technologies long before there is any need for government interference. The coming deployment of RFID provides an opportunity to study those forces and how they guide a technology toward uses that are optimal for consumers.

These forces fall into several categories, such as economic incentives, consumer preferences, counter-measures, and existing legal protections. While it is impossible to describe how all of these forces will impact RFID systems, examples of their likely operation show that there is no cause for alarm or precipitous government interference.

Economic Forces Guiding RFID Deployment

The businesses that will use RFID exist to respond to the profit motive. Their economic incentives will "regulate" RFID in ways consistent with the interests of consumers.

An assumption underlying most pro-regulatory activism is that corporations are greedy. Hungry for consumer dollars, businesses will collect as much information about consumers as they can and use it to try selling them more and more things. Greed will drive companies to install RFID tags in everything, and place readers everywhere, the argument goes, so sellers can watch consumers' every move, develop psychographic profiles, and wend their way further and further into consumers' lives.

But greed – "self-interest" is the less pejorative term – operates as an equal restriction on vendor behaviour. The purpose of RFID is to increase profitability, so companies will place RFID tags on goods only when this can improve the bottom line. A five-cent chip would not be attached to the wrapper of a fifty-cent candy bar because that 10 percent cost increase would more than eat up the producer's profits.

Self-interest will impact not just the placement, but also the design of RFID tags on consumer goods. RFID tags will be as simple, cheap, and minimally functional as possible to achieve their limited purposes. RFID tags will not be micro-miniaturised computers or have read-write memory – too expensive and wasteful. They will communicate on lower (cheaper) frequencies, which are not conducive to long read-ranges. Secret read-write micro-tags with long-distance capability will show up in consumer products when marketers are wasteful enough to use Formula One cars as delivery vehicles.

Indeed, RFID tags for consumer goods will be optimised for reading at very short distances: Customer satisfaction will fall, and profits will be threatened if, for example, customers are wrongly charged for goods passing near the checkout stand in the hands of other shoppers.

Also, because they are costly, RFID readers will only appear in places where they can be truly useful for distinct purposes like inventory control and checkout. Corporations are not likely to place RFID readers on street corners, entrances to office buildings, or other public places. For consumer research, readers have been located various places in stores, sometimes networked to cameras, leading to false assumptions that this would become common practice,[5] but it is highly unlikely because of the economics involved.

Even if readers and tags cost nearly nothing, installing readers, powering them, and, most importantly, storing the massive amounts of data they collect will always entail costs. A key role of RFID middleware will be to filter out useless data before computing time and electric power is wasted on processing and storing it. If data is not useful for advancing a particular customer service mission, companies will discard it, incidentally "protecting" consumers from excessive data collection.

In the past, consumer-oriented companies may have had a singular mission to learn more about consumers. RFID-enabled commerce will oblige them to choose carefully what information matters and what does not. Corporations will discard lots of useless consumer data – and they will do so because of "greed."

Jealousy is another corporate trait that prevents – rather than exacerbating – potential privacy problems. A corporation that collects consumer data through RFID will tend to guard such information jealously. The value of data is lost if corporations share it wantonly or if they abandon it to security breaches.

Likewise, for most companies, the design of RFID systems and the data in them will likely be jealously guarded secrets. If correlations between serial numbers and products are openly available, for example, competitors will gain useful intelligence by observing which of their competitors' products their customers buy. A seller of jeans, for example, could recognise the RFID tags from competitors' leather jackets entering its stores and begin selling leather jackets to co-opt the competition.

The serial numbers on RFID tags may be assigned in blocs, as Internet Protocol numbers are today, but companies will be foolish if they assign numbers to their products in blocs. By randomising tag numbers, they will frustrate competitors. They will also frustrate the theorised burglar who allegedly would scan houses with an RFID reader to determine what products are inside.

Wild projections about the capability of RFID in the consumer goods context rely on a distinct lack of clarity about the economic incentives that will affect the design of RFID technology and systems, the deployment of RFID

devices, and the use of RFID-collected data. We can rely on the "greed" and "jealousy" of corporations to protect us from many imagined uses of RFID that cause concern.

Consumer Preferences Counter RFID Abuse

Consumer demand and preferences will greatly influence deployment of RFID systems and use of RFID-derived information. Consumers will be the ultimate arbiter of RFID proliferation and use.

Consumers may demand RFID tags in some circumstances. Expensive electronics components sold with embedded RFID tags can be associated with their owners via the serial number in the tag so that owners stand a better chance of getting their property back if it is stolen or lost.

Consumers may reject RFID tags elsewhere. Shoes seem a particularly inappropriate place for permanent, non-detachable RFID tags. They have one wearer for a long time and so are susceptible to unwanted tracking, a risk that is likely disproportionate to any benefit.

Most commonly, purchasers will probably be indifferent to RFID tags in many goods and many types of packaging. RFID tags on goods that are carried home, used there, and/or discarded have only the remotest privacy implications.

Consumer preferences about RFID extend beyond its presence or absence. Consumers may insist upon RFID tag removal post-sale, either by peeling them off products or by snipping them out. It may be that tags designed to be muted or "killed" at the behest of the consumer will prove most appropriate in some cases. Again, these are decisions to be made in the myriad situations that arise, weighing the threat to privacy against interests like effective theft-prevention systems.

Privacy notices have become something of a fetish of some privacy advocates. Billions of dollars have been spent to deliver privacy notices – for instance in the banking industry – to indifferent consumers. But notice may have a role. After all, a promise about the presence or absence of RFID, or about the use of information generated using RFID, may bind an organisation contractually, subject it to criticism and consumer retaliation when violations occur, and possibly expose the seller to legal enforcement action.

Manufacturers and retailers have competitive incentives to stay keenly attuned to consumers' interests in all facets of the product and retailing experience. If activists want to participate constructively in the debate, they should focus on true consumer interests, which encompass more than privacy. Low price, convenience, customer service, quality, customisation, and many other factors, also matter a great deal.

Countermeasures and Self-Help

For privacy-conscious consumers, various self-help techniques exist. In the unlikely event that tag deactivation or easy removal aren't built-in, scissors and razor blades will often be an effective low-tech, anti-RFID weapon. Aluminised Mylar bags are another low-tech RFID countermeasure that blocks the radio signals between readers and tags.

High-technology devices on the drawing boards also will come into use as countermeasures. Blocker tags have been designed to give consumers control of data transmitted to nearby readers.[6]

To counter surreptitious scanning, RFID reader detectors would be simple to design; they need merely pick up signals in the frequency used by RFID and emit a warning. An RFID reader detected at a store would be normal. However, a reader detected at the opera (perhaps) would not. Only a few detectors would be needed to find and "out" retailers who place RFID devices in inappropriate places or try to conceal their use of RFID. Chastising one retailer for such behaviour would chasten them all.

Either consciously or through routine behaviour, people can frustrate attempts to derive information using RFID that conflicts with their preferences. People routinely buy clothing as gifts for others, lose items, and give things to charity. If there ever were a comprehensive RFID scanning system, and if it were tied to purchase records, it would pick up traces of a single person in many different places at once. The value of such data would be minimal, which is why rational economic actors would be unlikely to collect it.

If the natural transfer of possessions across human environments proved insufficient, people could consciously monkey-wrench RFID systems by sewing multiple RFID tags from multiple sources into hats and garments and then trading them. People could easily conceal RFID tags in others' cars and clothing, adding dozens of RFID "zombies" to the streets of our cities and undermining potential surveillance systems.

Techniques for disrupting RFID-based surveillance are numerous. The wide array of countermeasures provides yet another bulwark against use of RFID systems contrary to consumers' interests.

Existing Legal Protections Against RFID Privacy Invasion

Existing law, such as property rights and the common law privacy torts in the United States, already substantially delimit the use of RFID and its potential for abuse. They head off many RFID privacy issues in at least two ways.

First, existing law gives consumers substantial autonomy and control over what goes into their homes, what travels in their cars, and what goes on or in their bodies. Many concerns expressed about RFID omit the almost total power consumers have.

Thanks to property rights, people are under no obligation to allow RFID readers into their homes, though they may certainly want them to simplify grocery shopping and cooking – or to locate RFID tags. Many concerns about RFID presume that RFID readers will somehow be able to inventory the contents of homes. Read ranges will simply not be long enough, RFID readers will not be admitted without the permission of homeowners, and correlations between goods and tags will not be publicly available.

Stories of the potential for human implantation of RFID tags have led to a charged atmosphere of concern. But implantation of an RFID tag into an individual against his or her will would be a tort and probably a crime if done by a private actor, and a violation of constitutional rights and fundamental liberties if done by a public official.

It takes a lot of imagination, and a lack of legal comprehension, to buy into many of the concerns being aired about RFID. The web of laws protecting autonomy and property rights sharply limit the chance that RFID will be used in ways consumers do not want.

A second way that law circumscribes RFID is by outlawing harmful uses of it. The genuine harms that potentially could be done to consumers via RFID are illegal already.

A body of U.S. state law, the privacy torts, bars various invasions of privacy and gives a cause of action to victims no matter what technology was used to collect the information used in an invasion.[7] Various statutes prohibit all variety of harms that may be done with information, whether derived via RFID systems or not. It is illegal (if it is possible) to use RFID in the course of identity fraud, theft, burglary, stalking, murder, or conspiracy to commit any of those crimes. Someone who places an RFID reader surreptitiously on another's property or in another's home must commit trespass, burglary, or both to do it.

The mischief that might be made possible by RFID is already against the law. Ignorance of the law allows many to believe that RFID has outsized power to affect consumers' privacy.

Many concerns about RFID also arise from ignorance about the economic constraints in which the RFID user community will operate. As noted above, vendors will be driven to use cheap, dumb tags useful for tracking inanimate objects in controlled environments, but not good at all for tracking humans in our social environments. While self-help is a worthy, perhaps superior, failsafe should economic constraints on RFID deployments fail, existing law represents the final bulwark against abuse of RFID systems. It punishes wrongdoing and empowers consumer to reject uses of RFID that they do not want.

Consumers will exercise substantial economic sway over how RFID systems will be deployed, though predicting exactly what they will call for is not possible while the technology remains mostly on the horizon. In any event, RFID should not be assumed to have capabilities beyond what the laws of physics and economics will allow. Ill-considered regulation to head off imagined concerns is particularly unwarranted given the legal protections that already exist.

Conclusion

Some privacy activists today embrace a narrow vision of consumer interests. "Privacy," they seem to believe, entails anything that will frustrate marketing and commerce.

True consumers' interests are broader. Along with privacy, consumers want a complex and constantly shifting mix of low prices, convenience, customisation, quality, customer service, and other characteristics in their goods and services. Radio frequency identification technology will help producers, marketers, and retailers better understand and serve the mix of interests consumers have.

The components that go into RFID readers and tags are simple radio communications, but their smaller size and broad deployment enhance the power of the technology and raise concerns about the privacy effects of RFID deployment. These concerns are often premised on unlikely assumptions about where the technology will go and how it will be used.

Any inclination to abuse RFID technology will be hemmed in by a variety of social forces, economic forces being one of the most significant: The typical RFID tag in the consumer goods environment will be cheap, dumb, and not good for much more than tracking inventory.

Consumers, as economic actors, have substantial power to dictate in the give and take of the market how RFID will be used. They will likely demand tags linking to their identities in certain applications – such as consumer electronics – but may object to the presence of RFID tags in other situations. They may demand peel-off tags, or assurances about what a particular tag is doing. In many instances, they will be indifferent, and rationally so.

Regulators, think-tank analysts, and activists should not attempt to dictate RFID policy before real experience has been gained. There must be no moratorium on RFID deployment. There must be no arbitrary bureaucratic "principles" laid in the path of progress. And there must be no outright ban on extensions of RFID technology that may well be beneficial. There must be deployment, experimentation, testing, and study of what consumers really want.

1 An active RFID system recently failed dramatically when Kentucky Governor Ernie Fletcher's plane failed to identify itself as "friendly" to air traffic control in the Washington, D.C. area as he approached for former President Ronald Reagan's funeral, prompting the evacuation of congressional office buildings.

2 See Ann Zimmerman, "Identification Tags Debut at Seven Wal-Mart Stores", *Wall Street Journal*, April 30, 2004.

3 Consumers Against Supermarket Privacy Invasion and Numbering *et al*., RFID Position Statement of Consumer Privacy and Civil Liberties Organizations (Nov. 20, 2003) <*www.privacyrights.org/ar/RFIDposition.htm*>.

4 Federal Trade Commission, *Public Workshop: Radio Frequency Identification: Applications and Implications for Consumers; Notice*, 69 Fed. Reg. 20,523 (Apr. 15, 2004) <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/04-8625.htm>.

5 See, *e.g.,* Jon Dougherty, *Technology Automatically IDs Consumers*, WorldNetDaily.com (July 19, 2003) <*http://worldnetdaily.com/news/article.asp?ARTICLE_ID=33646*>.

6 Ari Juels *et al*., *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, RSA Security (2003) <*www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf*>.

7 *See* Privacilla.org, *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection*, (July 2002) <*www.privacilla.org/releases/Torts_Report.html*>.

An earlier version of this article was published by the Competitive Enterprise Institute, online at www.cei.org.

  WDPR ISSN 1473-3579