

RFID

Prepared by the NECCC RFID Work Group



NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

Copyright © 2005 by National Electronic Commerce Coordinating Council

NECCC
2401 Regency Road
Suite 302
Lexington, KY 40503
(859) 276-1147
www.ec3.org

Made in the United States of America.



NECCC is a consortium of national organizations and public and private sector leaders identifying best practices for strategic change within government.

Alliance partners are:

National Association of State Auditors, Comptrollers and Treasurers
National Association of Secretaries of State
National Institute of Governmental Purchasing

NECCC also works in partnership with these affiliate organizations:

Association of Government Accountants
Information Technology Association of America
National Automated Clearing House Association
National Association of Government Archives and Records Administrators
National Association of State Treasurers

Table of Contents

- Introduction..... 1**
- Overview..... 2**
- RFID: How Does It Work?..... 3**
- ROI and RFID: Business Cases..... 5**
- What Does the Future Hold for RFID?..... 7**
- The Role of Policymakers in RFID..... 12**
 - Model Cases..... 12
 - Existing Proposed Legislation..... 12
 - Existing Applicable Laws..... 13
 - Appropriate Levels of Government Regulations..... 15
 - Technology Policy Principles..... 15
- The Role of Industry in RFID..... 16**
 - Enact and Abide by Strict Privacy and Information Handling Guidelines..... 16
- Conclusion..... 20**
- Appendix A..... 21**
- Endnotes..... 25**

Written by:

Michael J. Tavilla, Association for Competitive Technology

With:

Eveanna Barry, NASACT/NECCC

Dan Combs, Global Identity Solutions

Daniel J. Greenwood, MIT Media Lab

Clark Kelso

David Lewis, Waterville Consulting

Mike Malik, Delaware Department of Information Technology

Stephen Mendonca, The MarketQuest Group

Richard J.H. Varn, RJV Consulting

Dr. Harsh Verma

Introduction

Radio Frequency Identification technologies permit the identification of an object wirelessly across a distance. In commerce, the technology has been used as a smarter, more efficient bar code. Employers, governments and others are also using the technology for more effective and convenient access control or authorization of people by including it on objects like employee badges, automatic toll paying devices and eventually on passports. As this technology becomes more widely deployed in every sector of the economy, it is creating significant cost savings, new revenue opportunities and enhanced services. Some applications, such as those involving use of RFID enabled objects held by people, raise privacy and other civil liberties questions. Should people be able to refuse, disable or opt out of using this technology to avoid potentially being tracked or monitored without their knowledge or consent? Should this technology be mandatory on passports and drivers licenses to aid law enforcement, intelligence and other government workers in protecting and serving the public? Is the positive economic impact of this technology as a bar code replacement on crates, products and other objects so significant that government should create specific incentives for its adoption and use? How will our society be different once this technology is ubiquitously used – who will benefit, how might current expectations change, what costs might develop, and what role, if any, will policy makers play?

This paper will provide general overview information about RFID technology, how it is being used and some preliminary thoughts on its relevance for government. There are many stakeholders with different interests in RFID technology. It is likely that industry will seek to use this technology to control costs, achieve new efficiencies by better tracking of goods and transportation systems and to make additional value by creating business models, innovating processes or inventing new kinds of products or services. Even within a given enterprise, however, the interests will vary depending on the organizational vantage point of any given individual. For instance, within a state government, a purchasing officer may seek to develop some metrics for assessing best value, based on the various types of RFID implementations (active, passive, shorter or longer ranges, etc.) and to draft check lists for agencies to follow to assure the technology is utilized in a way that is consistent with internal privacy, fair information practices and other relevant standards. A regulator, on the other hand, may seek to develop ways to audit the logs of RFID-aware systems as another tool for evaluating what has actually happened with people, places and things in the regulated business or industry. By contrast, a legislator may be interested in creating a study task force to assess whether the potential privacy issues are adequately addressed by existing state law or whether new law may be needed to fill possible gaps. Finally, a program manager or line worker will likely be motivated to leverage this technology to provide the same or a higher level of service at less cost, in less time, yielding greater relevant information, or by enhancing other efficiencies or quality of delivery.

Overview

RFID: The “EZ-Pass” of goods in the marketplace, from producer through to consumer.

Just as drivers have grown to depend upon electronic toll collection (EZ-Pass) technology to breeze through toll booths, manufacturers, retailers, and other government agencies envision similar benefits in RFID technology, ultimately increasing choices and lowering costs. These small tags can be affixed to goods at the bulk or unit level to convey information such as product type (like a Universal Product Code), production date, and other data relevant to the movement of goods from the manufacturer to store shelves and on to consumers.

Wal-Mart, far and away the world's largest retailer with \$285 billion in sales, is driving adoption in the commercial supply chain by requiring suppliers to use RFID tags. This biggest of big-box retailers seeks to manage distribution, warehouse, and in-store inventories to lower logistical costs, translating into lower costs and a more dependable supply of goods for consumers. The general concepts and principles used to locate packaged goods in a retail context can be used for inventory/materials control in production as well. A manufacturer may use RFID to insure the necessary components are present to assemble the products on projected production schedules for tomorrow or next week. Yet RFID's potential goes well beyond retail, inventory, packaged goods, and other commercial applications. For example, the U.S. Department of Defense (DoD) makes extensive use of RFID tags to track goods and military materiel used by the armed forces around the globe -- all to ensure proper battle readiness and support.

RFID can also be used to identify individuals. A common example is employee identification cards that can control access and (optionally) pinpoint the location of the employee while in the workplace. Consider the extraordinary value of the technology if a doctor or nurse within a hospital had the ability to identify those closest to respond to “code red” situations and administer life-saving critical care. RFID is also being used in patient wrist bands to facilitate accurate identification and recording of patient-related data such as prescriptions. The integrated use of RFID technology in the healthcare field to identify patients, providers, medicines, supplies, and medical equipment offers the potential for more consistent care at a lower cost. However, it is the very use of RFID for individual identification, particularly in documents like driver's licenses and passports, that has raised some of the greatest privacy concerns.

There is little question that RFID has improved the operations of governments, manufacturers, and retailers as well as provided benefits to individual consumers. Although we are in the earliest stages of widespread adoption and deployment, important regulatory and business-side questions remain unanswered.

Among the most pressing:

- 1) *What will industry practices be (particularly standards) for implementation?*
- 2) *How will governments handling consumer data ensure the proper level of privacy and security?*
- 3) *What is government's role in oversight of the personnel and business issues that come with widespread adoption of RFID?*

This white paper will explain in detail how RFID technology functions, explore present and future applications for RFID, and examine the policy and regulatory implications that arise with its adoption in particular industry and business settings.

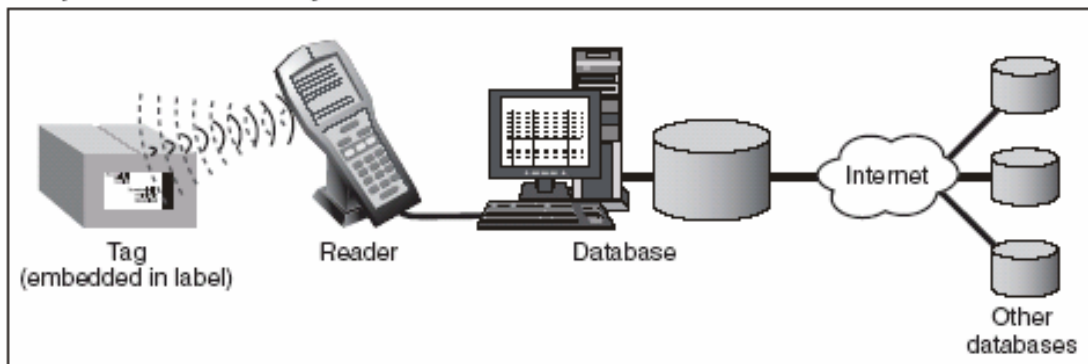
RFID: How Does It Work?

RFID tags, sometimes referred to as “smart labels,” were once used only in limited ways to track cattle herds or manage vast government inventories. Now, however, the technology has evolved and has already been used for a myriad of applications that have a positive impact on manufacturing, corporate supply chains, and at the level of everyday consumers and citizens.

The basic components of an RFID system are the tag, a reader, and a database that maintains product information (See Figure 1). Basically, a pallet of products or an individual item can contain a tag. A reader identifies the tag, reads the information it contains, and queries a database that in turn provides information about the product. The Internet enables the transmission of this data.

Figure 1

Components of an RFID System



Source: GAO.

RFID provides a method of identifying unique items or entities using radio waves. Typically, a reader communicates with a tag, which holds some specific digital information in a microchip. There are also some chipless forms of RFID tags that use material to reflect back a portion of the radio waves beamed at them.

The Electronic Product Code (EPC), in conjunction with RFID, provides a method of automatic identification and tracking of objects. RFID technology has an advantage over bar-coding in that it allows the client to uniquely identify each individual object as well as identify objects within the vicinity that are not within sight.

RFID in combination with the EPC system can help computers automatically and uniquely identify everyday objects. Enabling computers to automatically recognize and identify everyday objects will enable those computers to track and trace the objects, trigger events, and even perform actions on the objects themselves. The application of RFID and EPC technologies will provide enterprises with an unprecedented real-time view of the location and integrity of their global assets and inventories and will enable significant gains in operational efficiency. Other business benefits include improved labor efficiencies, better inventory management across the supply chain, improved product integrity, reduced shrinkage, and other benefits.

RFID tags are generally found as part of a standard label affixed to a box, package, or shipping container and can be of two varieties: *active* and *passive*.

- **Active RFID.** This type of tag has an internal power source, or battery, that constantly powers the device and enables radio transmissions to reach the reader. The benefits of active RFID include a stronger signal strength resulting from its native power source that thereby enables greater possible ranges from tag to reader. Active RFID tags have no power constraints and may have communication ranges of 100 meters (approximately 328 feet) or more. But given the greater complexity, costs are higher for active RFID tags. Active RFID tags are appreciably more expensive than their passive tag cousins, currently priced at \$1 or more per unit.
- **Passive RFID.** Passive RFID tags gain their power from the radio frequency transmission of the reader, at the moment of scan, and then respond with the necessary information. Passive RFID requires a stronger signal from the reader to provide the power necessary for a response and its return signal is weaker than an active return signal. Passive RFID signal range is generally limited to three meters (approximately ten feet) or less. Currently, passive RFID tags cost approximately \$0.20 per unit.

ROI and RFID: Business Cases

Specific technical aspects aside, the primary aim of any RFID implementation is to increase efficiency and yield measurable benefits, monetarily, in labor-savings, etc., and show a return on investment from the technology for the organization, agency, or business. As mentioned earlier, there are numerous examples of current, present-day RFID deployments that are bearing tangible benefits for governments, businesses, and other entities that need to keep track of goods and other units of material.

- **United States Department of Defense.** DoD has been making use of large-scale RFID deployments since the first Gulf War in the 1990s. The department, a massive mover of equipment domestically and across the globe, has realized efficiencies unheard of just a generation ago. At a recent event on Capitol Hill examining RFID, a DoD official said that the department has reduced duplicate or incorrect shipments of goods dramatically. RFID technology helps ensure that military vehicles and supplies get where they are going when they need to be there, ending a downward spiral of events where duplicate units may be sent where they are not needed, thereby depriving needy forces of those units.¹ And even though, regrettably, government departments sometimes are not hotbeds of technological innovation, DoD is the exception. The department has pioneered use of the Iridium network of global satellites, which it already uses for other communications. These tags transmit unique identification numbers, date and time information, and current position to within 3.5 feet. That capability will change DoD's RFID network from one that provides information on where shipments of equipment have been to one that is closer to a real-time understanding of where equipment is actually located.²
- **United States Department of Agriculture.** In 2004, the USDA announced that it would embark on a \$19 million dollar project to be alerted about and respond to intentional or unintentional animal disease outbreaks. Ultimately, this National Animal Identification System (NAIS) could track 100 million animals and manage a disease outbreak to preserve healthy livestock and maintain a safe food supply.³ Bovine spongiform encephalopathy, better known as “mad cow disease,” tops the list of those diseases on priority watch by the agency. Another is chronic wasting disease, a related ailment that affects deer and elk. In accordance, USDA officials have shipped 26,000 RFID tags this year to states to help prevent the spread of these diseases to domesticated herds.⁴
- **Virginia Beach, Virginia.** This southern Virginia ocean-side city recently invested \$1.5 million on an RFID system for its public libraries. RFID tags have replaced easily damaged barcodes that were previously used to track book inventories. The tags have increased returns, freed librarians from repetitive tasks, and doubled checkout speed. Librarians no longer have to visually scan shelves for misplaced books—they may simply wave a wand across a shelf to detect missing items.⁵ State and

local governments can also deploy RFID in other ways. For example, toll collection on roads and bridges, identification of inmates at state prisons, county jails, juvenile facilities and mental health facilities, identification of patients cared for in government- run hospitals, clinics or medical facilities, and for identification for access to secure public buildings.

- **Wal-Mart.** Due to its sheer size and global market reach, Wal-Mart effectively issued an industry-wide mandate for suppliers of consumer packaged goods when it committed to RFID technology in its operations. As of January 1, 2005, 137 of Wal-Mart's suppliers (the largest 100 suppliers and 37 volunteers) were tagging cases and pallets going to three of their distribution centers. Wal-Mart estimates that 65 percent of goods during this initial stage of deployment were tagged and read. As these percentages increase, the company hopes that goods will flow properly at the warehouse level, that proper inventory will be maintained in stores, and that even the in-store pick-up for online orders can be improved. Unintended positive consequences have also emerged; having pallets of goods out of aisles during peak shopping times, thereby not obstructing consumer access to shelves, should make shopping easier and improve sales.⁶

- **Las Vegas-McCarran Airport.** Unlike Denver International Airport, which suffered numerous high-profile failures of its automated non-RFID baggage system in the late 1990s, Las Vegas McCarran has enjoyed considerable success in getting RFID-tagged baggage to travelers at airport carousels. Being one of the world's busiest airports, with a single IT infrastructure to manage baggage, McCarran was a prime candidate to bet on RFID. Old-style barcodes had a reading accuracy rate of approximately 85-89 percent as compared to 99.7 percent for RFID tags. The older barcode technology resulted in 6,000 mishandled bags a day.⁷ This lost or delayed luggage cost airlines an average of \$100 per passenger, including courier services to get luggage to the passengers or fees to replace items. Today, the airport cites savings of hundreds of thousands of dollars each year with its higher accuracy rate.⁸

- **National Seaports.** More than 17,000 containers, or roughly 80 percent of all U.S. imports, enter the United States by ship each year, yet U.S. customs and security officials open and inspect less than two percent of containers arriving at seaports. The inability to check all of the containers represents a gaping hole in the nation's domestic security. Government officials worry that terrorists could exploit lax security at ports and smuggle weapons of mass destruction into the country. Recently, a council comprised of port operators, logistics technology providers, former U.S. military leaders, and public officials, launched the first phase of a project called Smart and Secure Trade Lanes (SST) to demonstrate how RFID could be used to secure and track containers and safeguard international shipping lanes. Initial trials tracked the shipment of 818 containers carrying real goods leaving three overseas ports (Hong Kong, Rotterdam and Singapore) and arriving at one U.S. port (Seattle-

Tacoma). The project monitored a total of 18 different trade lanes and was able to track 100 percent of the containers end to end and was found to have correct and accurate container, route and manifest data. In addition, savings were realized of approximately \$300-\$500 per container in administrative, theft/loss, and other handling-related costs.⁹

- **Hospital Infant Protection.** A technology already installed in over 900 U.S. hospitals is an RFID-based infant protection system called “Hugs” that thwarts infant abductions and eliminates accidental infant mismatching. Each infant wears a tag on his or her wrist or ankle that contains an RF transmitter. Hospital exit points are electronically monitored to detect unauthorized removal of an infant. Since 1983, there have been 233 infant abductions in the United States, half of which originated at healthcare facilities. In July 2005, this system alarm sounded at a facility when an infant was removed from a hospital’s seventh-floor nursery. Nurses and staff responded to the “Code Pink” alert, and security officials recovered the infant unharmed and safely returned him to the maternity ward. Infant mismatching at hospitals can be eliminated as well. Regrettably, without RFID, mismatching incidents occurred roughly 20,000 times a year according to the Journal of Healthcare Protection Management.¹⁰
- **Amusement Parks.** Amusement parks in California and Tennessee allow visitors to track their parties in real-time through a product offered by SafeTZone Technologies, Corp. This firm’s RFID-based device is watch-sized and worn on the wrist. Should members of a group get separated from each other, they can visit a kiosk and scan the “bracelet” for information about where the rest of their party is located. Technologies such as this will empower parents, youth group leaders, spouses and park employees with immediate visual awareness of the whereabouts of children, students, or significant others.¹¹

What Does the Future Hold for RFID?

While there have been real initial successes in the use of RFID technologies, the long-term potential benefits are immense. To date, RFID has demonstrated brighter prospects for companies wishing to gain process efficiency and transparency, as well as to identify additional business potential. Major retailers have reorganized their shipping and receiving around RFID technologies. Concurrently, the market is responding positively with a new crop of product offerings from major information technology providers like HP, IBM, Microsoft and Oracle.

The next wave of RFID offerings will set higher standards of intensity and robustness. Customers will soon see RFID solutions based on advanced middleware and architecture, which will accelerate the trend towards standardized applications and business processes across industry verticals. Some vendors are

preparing to offer managed services that will support RFID implementations throughout the customer cycle, including network integration, consulting, IP transport, hosting, storage and security.

While the bulk of today's RFID software is aimed at inventory or asset tracking, the industry has set its sights a bit further as well. The impact of more affordable and standard applications will place RFID at multiple points in the supply chain, even to the point of connecting parts, products, machines and transport mechanisms. Some providers already offer high-speed readers and printers that comply with RFID/EPC codes. Such systems will greatly streamline the process of advance shipping and invoicing.

As indicated, there are a myriad of applications in various industry verticals of the overall economy that are possible and just being realized (See Figure 2). Specific examples of future substantial impact include:

- **The advanced administration of healthcare services.** Everyone is burdened by high costs of healthcare: consumers, businesses and governments. Given that much of this cost is in paper-laden, offline processes, RFID can be an integral part of the redevelopment of America's health care system. Beyond tracking newborns, RFID can be used to track hospital supplies and medicines and even improve and speed patient care. Patients can now be outfitted with an RFID-enabled wrist band, which before only held the text of the name and ward of the patient. These RFID tags could be programmed to identify the patient to caregivers with greater detail, alerting them to information about special meal requirements, medicine/allergy information, and other vital information about condition. Although it may make privacy advocates moan, some have even championed the eventual use of implantable RFID tags implanted just under the skin to mitigate the risk of lost or damaged tags worn on the wrist. Even former U.S. Department of Health and Human Services Chief Tommy Thompson is a believer. He plans to be implanted with an RFID tag manufactured by VeriChip, a subsidiary of a company on whose board he serves.
- **Pharmaceuticals.** RFID will help ensure the safety and integrity of the global supply of life-sustaining drugs and medicines. A troubling recent trend is the increased production of counterfeit drugs that may be ineffective, merely placebos, or actually lethal. Sales of counterfeit prescription drugs are expected to nearly double by 2010, reaching \$75 billion by the end of the decade, according to a new study from the Center for Medicines in the Public Interest. At that pace, counterfeit sales would surpass the annual sales growth of legitimate pharmaceuticals. For example, counterfeit drug sales for 2005 will reach nearly \$39 billion. The U.S. Food and Drug Administration (FDA) is promoting track-and-trace technology such as RFID as a deterrent to drug counterfeiting, diversion and theft. RFID tags can be attached to foil packs and other containers of medicine to authenticate that they are genuine, effective and safe. The issue is also global in scope. According to

a government-owned Chinese newspaper, the *Shenzhen Evening News*, approximately 192,000 people died in China in 2001 because of fake drugs. Since 2001, Johnson & Johnson has established 38 criminal cases against different factories that copied its products in China. In the U.S. in recent years, drug-maker Novartis has assisted in over 200 counterfeiting investigations in 33 countries.¹²

- **Consumer retail outlets.** While only used now on a very limited, trial basis by some retailers, the benefits RFID can provide everyday consumers in their shopping experiences is immense. Imagine a grocery store where items are scanned as they are placed in the cart and when shopping is completed, there is no need to wait in a check-out line. Or when shopping for clothing, RFID tags contained in items you may have already picked up for purchase, can help direct the shopper to complementary items. Both would ease the customer experience in locating the products they need and speed the payment and purchasing process.

How industry and government will use RFID in the next five years			
Application (Specific Sector)	Major Category (Asset Management/ Logistics/Security)	Description (General Description of Usage)	Potential Benefit (Possible gains of implementation)
Automotive	Asset management, security	The TREAD ACT is a federal mandate requiring the tire industry to develop a mechanism to track tire recalls. The AIAG RFID group is currently working on RFID standards for tires.	Provides a more accurate picture of where tires have been sold. Lowers the risk of litigation for manufacturer.

How industry and government will use RFID in the next five years

Application (Specific Sector)	Major Category (Asset Management/ Logistics/Security)	Description (General Description of Usage)	Potential Benefit (Possible gains of implementation)
U.S. Department of Defense	Asset management, logistics	DoD mandates RFID usage by its suppliers.	Increases the efficiency of the supply chain.
Agriculture	Asset management	One of the first applications of RFID was to identify animals.	Increases the efficiency of livestock handling
Oil and Petroleum	Asset management	IDTAG is used in the drill pipe identification process, where it is embedded into the pipe under the metal surface to address the pipe wear problem.	Allows drilling companies to minimize pipe breaks, maximize pipe life, and keep accurate pipe inventory records.
Gas Production	Asset management, logistics	RFID tag embedded into the metal collar of the bottle or container or alternatively securely clipped onto the collar with a plastic carrier to identify gas bottle	Solves logistical problems in the supply and distribution of industrial gas to customers.
Education	Asset management, logistics	RFID tagging for library use to check books and other media inventories.	Allows for "Smart-shelf" and increased efficiency of staff and systems.
Airlines	Asset management, logistics	Tracking of bags from airport check-in counters, where the RFID tags are attached, until they are dropped off at the baggage carousel at the customer's destination.	Solves luggage mishandling for airline customers.
IPFMA FDA NACDS	Logistics, security	International Federation of Pharmaceutical Manufacturer's Association (IPFMA) proposing RFID for tracking, management, and manufacturing of drugs.	Track drugs and limit counterfeiting and theft.
Pharmaceuticals	Logistics	The tracking of theft-prone drugs (Oxycontin, Viagra, Sudafed) – following FDA guidelines for RFID pilot programs.	Track-and-trace protection for drugs. Reduces counterfeiting and theft that cost the industry \$30B/year.

How industry and government will use RFID in the next five years

Application (Specific Sector)	Major Category (Asset Management/ Logistics/Security)	Description (General Description of Usage)	Potential Benefit (Possible gains of implementation)
Medical	Logistics	Monitoring the precise location of people (e.g., patients, staff and visitors) and/or equipment like IV pumps, laptops and record events associated with their location.	Link the patient with life-saving key drugs, personnel administering the drugs, biometric measurements, etc.
Credit-Card, Financial Systems, Transportation	Logistics, security	Credit cards with embedded RFID chips. In Asia, contactless payment methods for public transit systems are common.	Increases the efficiency of electronic payment systems.
Transportation	Logistics, security	Non-stop systems for security, parking, and access control for hands-free control to ensure only authorized vehicles have entry.	Provides access data for administering periodic access charges or parking fees.
Transportation	Logistics, security	Highway toll collection systems for E-Z Pass and FastPass systems.	Saves time and increases traffic-flow by allowing vehicles to pass through a scan point without stopping.
European Central Bank U.S. Mint	Security	Embed RFID in notes to discourage counterfeiting.	Discourage counterfeiting.
DOT TSA	Security	Operation Safe Commerce - identifies existing vulnerabilities in the supply chain and develops improved methods for ensuring the security of cargo entering and leaving the United States.	Lowers risk of WMD/other dangerous or illegal materials of entering the U.S.
Government	Security	Electronic Article Surveillance (EAS) to identify items as they pass through a gated area.	Generates an alert of unauthorized removal of items from data centers.
Retail	Supply chain/asset management	Tags for clothing (Benetton), razors (Gillette/Tesco), shipping palettes, cartons (WalMart), shelf items (7-Eleven).	Lowers retailers' costs, improve inventory management, enhance service to customers.

The Role of Policymakers in RFID

Model Cases

RFID, by virtue of the technology itself, raises no public policy issues. Only when it is used, or potentially misused in some contexts, do issues arise. And the issues will differ, sometimes to a large degree, depending on that context. A key policy issue that has attracted attention is the possibility of tracking individuals without their knowledge or consent, while other policy issues include economic development and national security. As with any important enabling technology, policy makers must look to this young market with care and a sense of diligent stewardship. By finding a balanced approach to rule making and policy, legislators, regulators and other policy makers can foster a strong market for these technologies while guiding usage that protects the public and ensures national security.

As demonstrated earlier, RFID can be used in a variety of ways, and depending on the use, various public policy issues arise. For example, the privacy issues differ when RFID is used to monitor location of products or animals versus the privacy issues if humans are monitored. The use of RFID on identity cards, such as passports or a drivers licenses, will raise more policy issues if there are no safeguards or protections in place. Perhaps one of the most important protections that can be used is limiting the data transmitted by RFID on personal effects (such as identity documents or clothing) to redact any personally identifiable information (PII). For example, if the RFID tag only transmitted a randomly generated unique ID, as opposed to the person's name and address, then privacy risks can be limited. In addition, whether the tag is active or passive, and the read range of the tag should be considered when assessing the severity of privacy issues.

At this stage, it is doubtful that state legislation is an appropriate tool to affect deep or specific technology requirements in the development of the market for RFID. This section seeks to illuminate some of the factors and principles that policymakers should keep in mind when deciding what actions to take and when, with respect to RFID.

Existing Proposed Legislation

Responding to worried constituents, state legislators across the nation have already proposed new legislation that would limit the use of RFID technologies in businesses, schools, governments and other applications (See Appendix A). This initial response, similar to other state legislative reactions to new technologies, varies widely from state to state and is disproportionately applied. Some bills seek to require only labeling and notice that RFID is in use, while the state of California's approach would most

tightly regulate the technology itself, including prohibitions of certain applications and technology-specific security requirements.

These bills are offered for informational purposes, but not necessarily as an endorsement. Rather, at this point in time, it is felt that a light regulatory touch and more study is the best approach by legislatures. More information on recommended approaches appears at the end of this section.

Existing Applicable Laws

Numerous federal and state laws have focused on principles and policies about data access, accuracy, security, integrity, use, re-use, sale, storage, expungement, redaction, notice, education, choice, etc. These laws often directly or indirectly address the computer chips, transmissions, systems, storage, data, documents and databases to be used or created for RFID systems. Therefore, they already form a legal framework for the issue surrounding RFID and must be examined first for applicability to issues, concerns or actual problems stemming from RFID plans and deployments.

For example, all states have laws against fraud and theft. Most of these have been reviewed to ensure they cover specific kinds of technology-related forms of fraud and theft. Among these crime statutes are broad-based statutes like those prohibiting computer crimes. These statutes were adopted in response to such problems as computer hacking, data theft and computer viruses. These statutes ban unauthorized access to or theft from computer networks, computers and data storage. These statutes define computers, storage, data and networks generally so that even an RFID chip is considered a computer, part of a network and a data storage device. Therefore, since many of these state statutes, as witnessed in California, generally address bad acts and are not limited to a specific kind of computer technology, they apply to many of the potential problems and abuses of RFID already (See Figure 4).

Figure 4: State of California Laws That Already Apply To RFID

§§502.1 Prohibits access or use of computer chips and data without permission.

§§502.6 Prohibits card skimming.

§§502.8 Prohibits possession of equipment that surreptitiously intercepts electronic serial numbers or mobile identification numbers.

§§530.5-8 Addresses identity theft in that it prohibits obtaining personal information and using it for any unlawful purpose.

§§13848 Creates a High Technology Theft Apprehension Prosecution Program Trust Fund to help deter, investigate and prosecute high technology related crimes.

§§637.7 Prohibits tracking: “No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.”

§§1798 of the California Civil Code (The Information Practices Act of 1977) regulates the use of personal and other information by government.

For those jurisdictions that have made technology specific laws, they are in need of regular review to ensure that they keep pace with new technologies or are made more generic. For example, a review of California’s card skimming law shows that it needs updating as it only addresses magnetic stripes. In another example, Utah recently reviewed its laws on unauthorized access to networks and added wireless networks as it previously only addressed wire line networks.

The federal government, unlike many European countries, has chosen not to have a single comprehensive privacy law. Instead, there are numerous broad-based and subject-matter-specific privacy and access laws that address public and private information. Recently passed or amended acts such as the Fair Credit Reporting Act (FCRA), the Graham-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA) are designed to address the use and misuse of private information no matter whether RFID or another technology is used. Often a new technology, such as RFID, is singled out as a “poster child” for addressing a larger privacy, access, integrity or security issues.

In crafting information technology policy, policy makers must correctly identify the issues they intend to address. Moreover, these issues, while related, are often used interchangeably even though they are distinct. These issues would include:

- Data mining and matching of personal, private, and public data.
- Unauthorized data use and access.
- Illegal surveillance and tracking, privacy invasion, or other misuse of information by governments and/or private parties.
- Ensuring fair and accurate treatment of persons based on their real history as represented by documents and data.
- Criminal use of personal data for financial gain or which causes financial harm including identity theft
- Annoying or invasive marketing.
- Job loss from technology.

Appropriate Level of Government Regulation

Federalism and Regulation of Issues Involving Use of RFID

In the federal system of government, there are multiple jurisdictions at which legislation or regulation can be enacted. Choosing the appropriate level for regulatory action is critical. Selecting too narrow and local a level for regulation can leave serious problems unresolved. Conversely, selecting too broad and high a level for regulation can stifle and interfere with innovation.

As a general rule, the level of regulation should be aligned with the scope of the particular problem that requires a resolution. If an issue or problem tends to be local in nature, local regulation is to be preferred. If an issue or problem tends to be national or global in scope, federal oversight may be required. At the same time, consideration must be given to whether local or state regulation unduly interferes with other important interests that are federal or global in scope.

For example, RFID technology is being used in national and global commerce to track inventory as it makes its way from manufacturing plants to retail stores. Attempting to regulate these uses at the local or state level is very likely to interfere with important interests in efficient and effective commerce.

RFID technology may find uses in patient care through such devices as RFID-enabled wrist bands. While this may appear to be an area for state regulation, the appropriate use of health related information is now a field of regulation substantially dominated by federal law.

By contrast, the use of RFID technology with respect to such issues as toll-road collections or security systems in buildings has a more local flavor or character, suggesting that, if there is to be regulation at all, it should be more at the local and state level than at the federal level.

Technology Policy Principles

Once the technology has matured, and there are more widely adopted examples of usage, governments must be adaptable and reconsider some of these principles when warranted. For now, however, the following principles must guide legislative and regulatory actions on RFID:

- **Technology-agnosticism:** Avoid technology-specific regulations, favoring technology-neutral approaches that address the underlying behavior and outcomes.

- **Uniformity:** Avoid following approaches that conflict from one state to the next.

- **Restraint:** First, do not allow every new technology to force a re-examination of every information policy issue. Also, wait until you know how the technology will actually work when deployed. Lastly, even after deployment, the actual intended and unintended consequences of both the technology and a policy response are not clear and caution is urged.
- **Due diligence:** Determine if current laws and policies deal with that technology and its uses and if they are they adequate before any new legislation is considered.
- **Focus:** Narrowly tailor the response to the difference caused by the technology, not the technology itself. Solutions should also be targeted to the problem and actually help solve it. And the use sunset and sunrise clauses will maintain flexibility, adaptability, and trigger protections only if and when problems arise.

The Role of Industry in RFID

Enact and Abide by Strict Privacy and Information Handling Guidelines

Many firms hoping to tap into the emerging market for RFID and related technologies have adopted rigorous principles for an appropriate security and privacy focused deployment of systems. Industry must establish an adequate level of self-regulation, responsible use of technology and business practices that are sensitive to privacy and fair information practices. This is over and beyond whatever laws and other rules may come from government policy makers. Responsible industry practices in other economic sectors has been an effective and enforceable method to achieve privacy or other public interests in lieu of statutes or regulations. In the context of rules governing responsible use of RFID, industry clearly plays an important role.

The types of industry policies and guidelines needed will vary, depending upon the context in which RFID is used. For informational purposes, the following two of RFID privacy guidelines and principles cover use of RFID on people primarily for purposes of authentication (such as on employee badges) and on consumer products, illustrating current practice from the private sector. The first document was recently formalized and announced by ASSA ABLOY Identification Technology Group (ITG).¹³ Responsible firms such as this one know that it is industry's responsibility to help interested parties achieve a balance that safeguards privacy rights while allowing the use of RFID technology to flourish.

All firms must recognize that as technology and the uses for it grow, the issue of privacy protection will

become increasingly important for customers and society at large. These smart firms believe there is an achievable balance that safeguards privacy rights while allowing RFID technology to flourish.

ITG is an example of a firm that has adopted corporate principles and practices regarding privacy and the use of RFID technology. The following bullets comprise the ITG Privacy Principles:

ITG Privacy Principles and Practices for RFID

ITG has adopted corporate principles and practices regarding privacy and the use of RFID technology. This comprehensive set of guidelines establishes a clear corporate philosophy and concrete practices that will enhance ITG efforts in protecting the privacy and security of its' RFID card users.

ITG supports the following business principles and practices in respect to its RFID products and services, in all cases consistent with applicable laws. ITG encourages buyers of our products and services to support the following fair information practices:

- Support industry best practices through self-regulation, certifications, and other methods for protecting the security of personally identifiable information and other private data, and ensure that these practices be auditable and enforceable.
- Support the implementation of security for personally identifiable user information with protection that is proportional to threats to that data.
- Ensure that any personal data stored on our products be subject to review by the user upon request. Personally identifiable information associated with a unique identifier on our products should be subject to reasonable fair information practices.
- Prohibit sharing of personally identifiable information, whether collected on or linked to the tag with other parties without the clear consent of the user.
- Use RFID technology in a responsible manner that only collects necessary personally identifiable information.
- Discourage the use of RFID technologies or services for the purpose of tracking any person without their knowledge and consent.

- Promote user awareness of and consent to the use of an RFID tag on any product or personal effect, its purpose and use, including any data stored on that tag or any change in the intended purpose or use.
- Commit to consumer education for users to make informed and intelligent decisions about the use of RFID products.
- Achieve a workable global RFID standards—this will ultimately lower costs and speed deployment.
- Bring a usable RFID middleware to market. RFID's value is in the real-time data it produces about product characteristics, location, and link in the supply chain. Yet all of this new found data must be managed and used by so-called “middleware” software packages to yield information governments and businesses can act on. Even small scale deployments can produce terabytes of raw data. It's up to industry to develop new and cost-effective ways for governments and businesses to constructively manage and use the data.
- Ensure a strong technological backbone for the RFID network. The business and consumer benefits of RFID will never be realized without proper investment and management of the underlying RFID communications network. This means ensuring the network is entrusted to and managed by a capable administrator who can effectively maintain the critical high-levels of functionality, security, and privacy.

The next document was published by EPC global, and is a set of guidelines intended for use in the supply chain and retail context.

EPCglobal Guidelines on EPC for Consumer Products

The purpose of these Guidelines is to provide a responsible basis for the use of Electronic Product Code™ (EPC) technology for consumer items. Under the auspices of EPCglobal Inc, these Guidelines have been followed since January 1, 2005 and will continue to evolve as advances in EPC and its applications are made and consumer research is conducted. As EPC evolves, so too will new issues. EPC participants are committed to addressing these issues and engaging in a dialogue about them with interested parties.

1. Consumer Notice

Consumers will be given clear notice of the presence of EPC on products or their packaging and will be informed of the use of EPC technology. This notice will be given through the use of an EPC logo or identifier on the products or packaging.

2. Consumer Choice

Consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of the technology, is committed to finding additional efficient, cost effective and reliable alternatives to further enable customer choice.

3. Consumer Education

Consumers will have the opportunity easily to obtain accurate information about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarise consumers with the EPC logo and to help consumers understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines.

4. Record Use, Retention and Security

The Electronic Product Code does not contain, collect or store any personally identifiable information. As with conventional barcode technology, data which is associated with EPC will be collected, used, maintained, stored and protected by the EPCglobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use.

Revised September 2005

The above two policy guidelines and principles documents exemplify approaches by the private sector to set a meaningful framework to address the privacy issues that arise from use of RFID. The issues may vary to some degree depending upon whether RFID technology is used to identify things or primarily to authenticate individuals. The applicable policies and practices may need to be responsive to such contextual differences in the application of RFID technology. As this technology continues to be used more broadly, more such industry leadership will be needed to handle the privacy and other policy implications raised by RFID. In addition, innovative business practices, new technologies that can protect privacy or the ability to use legal pseudonyms, and other hard-coded methods to manifest fair information practices can be developed and deployed by the private sector.

Conclusion

As outlined, RFID offers tremendous benefits to businesses, governments and consumers alike. Yet with this great promise comes the great responsibility of data security and protection as well as sensible and workable deployments of the technology. Any use of RFID with lax data protection principles or a use that employs shoddy technical standards will drive consumers and customers away and attract the regulatory eye of governments. It is the responsibility of private-sector firms to bring effective and usable RFID solutions to market, for customers of the technology to deploy with appropriate security standards in place, and for governments and legislators to address policy questions with restraint. A failure by any one of these actors could derail adoption of this promising technology. If RFID vendors cannot bring useful products to market, if customers of the technology use it in an irresponsible or negligent manner, if governments burden the technology with onerous, unnecessary regulation, or if consumers don't understand both the risks and benefits of RFID, any or all of these factors could unduly limit the technologies extraordinary promise. As one can see, it is crucial that there is a coordinated and cooperative effort among technologists, regulators, legislators, and consumers to work together to ensure RFID can indeed realize its potential in offering benefits to businesses, governments, and the larger society.

Appendix A

APPENDIX A	
State - Bill #	Massachusetts - H.B. 1447 and S.B. 181
Title	An Act relative to consumer protection and radio frequency identification systems.
Purpose	Requires labels, logos and notices regarding use and purpose of RFID on consumer products and for readers by commercial entities in shopping areas. Requires the ability to remove tags that are not essential to product and limited information on tags to inventory and like purposes.
Summary	Requires commercial entities that place RFID readers in shopping areas to disclose the use and purposes of RFID readers. Also requires use of a logo and a label conspicuously making RFID use and purpose disclosure on products or packaging. Also requires RFID tags that are "not... essential" to the product to be capable of removal by the consumer. Also, limits the data stored or transmitted on RFID tags on products to information necessary for inventory, product return, recall or warranty servicing.
Status	Pending
Definitions	<p>"Radio frequency identification" or "RFID": a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum and that can be used to identify an object, animal, or person.</p> <p>"Radio frequency identification reader" or "RFID reader": an electronic device capable of reading, activating, triggering, or receiving information or data from a radio frequency identification tag.</p> <p>"Radio frequency identification system" or "RFID system": a combination of electronic and other devices including, but not limited to, RFID readers, tags, transmitters, processors, antennae, computers, visual displays and automated checkout systems, which enable the owner or user of the devices to track, monitor, record, identify, process, charge for, surveil, read, encode, decode, or disable a radio frequency identification tag.</p> <p>"Radio frequency identification tag" or "RFID tag": an electronic identifier comprised of electronic tags, electronic product codes, electronic chips, circuits or other triggering devices which contain identification information, data signals or other information related to the product, manufacturer, contents, serial number, date, purchaser, seller, destination, origin, package, carton, material, object or person to which it is attached, embedded or associated, and which information or data is capable of being wirelessly transmitted to or read by an RFID reader or system.</p>
State - Bill #	Maryland - H.B. 354
Title	Commercial Law - Task Force to Study the Use of Radio Frequency Identification Tags by Retailers and Manufacturers
Purpose	Creates a Task Force to study privacy and other issues related to RFID and report on whether legislation is needed.
Summary	Creates a Task Force, appointed by state officials, that shall study and report on the privacy issues raised by the use of radio frequency identification tags by retailers and manufacturers; whether the use of radio frequency identification tags by retailers and manufacturers should be prohibited or restricted; and whether legislation is necessary to regulate the use of radio frequency identification tags by retailers and manufacturers.. Task Force starts on October 1, 2005 and sunsets September 30, 2006.
Status	Pending
Definitions	N/A
State - Bill #	Missouri - S.B. 128
Title	RFID Right to Know Act of 2005
Purpose	Requires a conspicuous label on consumer commodity packaging with RFID disclosing existence of the tag and that the tag can transmit a unique id before and after purchase.
Summary	A consumer commodity or package that contains or bears a radio frequency identification tag or bar code shall bear a label as provided in subsection 4 of this section, and the label shall

	state, at a minimum, that the consumer commodity or package contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and shall be in a conspicuous type-size and location and in print that contrasts with the background against which it appears.
Status	Pending
Definitions	"Radio frequency identification" or "RFID": technologies that use radio waves to automatically identify individual items; "Tag": a microchip that is attached to an antenna and is able to transmit identification information.
State - Bill #	Nevada - A.B. 264
Title	Requires notice to be provided to consumers of retail products which have radio frequency identification tags.
Purpose	Requires manufacturers, retailers and others to ensure label regarding existence of RFID on product prior to sale.
Summary	Anybody who makes or causes an RFID tag to be attached to a consumer product must ensure that the retail product or its package bears a label which notifies consumers of the existence of the radio frequency identification tag, and a retailer selling such a product must ensure the label is affixed prior to sale.
Status	Pending
Definitions	"Radio frequency identification tag" means a device that: 1) Is attached to, embedded in or made part of a retail product or its package; and 2) Uses radio waves or other wireless technology to transmit a unique electronic product code. "Unique electronic product code" means a number or identifier that: 1) Uniquely identifies an individual retail product; 2) Is stored and transmitted electronically; and 3) Is used for the control and management of inventories of retail products.
State - Bill #	New Hampshire - H.B. 203
Title	An Act requiring notice regarding existence of RFID used for tracking
Purpose	Requires written or verbal notice of existence of a tracking device on any product prior to sale.
Summary	Regulates the selling goods with any tracking device in or incorporated into them unless the seller, prior to the sale, informs the consumer verbally or in writing of the existence of the device.
Status	Pending
Definitions	"Device": any item or application that is capable of providing the physical location or tracking the movement of the goods; "device" does not include bar codes or similar visible markings used primarily for product identification.
State - Bill #	New Mexico - House Bill 215
Title	Radio Frequency Identification Right to Know Act
Purpose	Requires businesses purveying tagged items to post notices on their premises and labels on the products of the existence of the tag and how the consumer can request any personal information collected by the business related to the tag. Also, requires removal or deactivation of tag at point of sale with no pressure on consumer to keep tag and prohibits linking personal data with tag data or disclosing personal data to third parties.
Summary	Requires every business in the state that "collects or carries" tagged items must post a specific notice of same, indicating how to file requests for more information. The business must release to a consumer all information gathered on that person when so requested by the person. The business must attach a conspicuous label on all products with a tag. The business must irrevocably remove or deactivate the tag at the point of purchase at it's own expense, and shall not "coerce" consumers into keeping the tags. Neither the business nor its affiliates may use tag information to identify a consumer or disclose directly or through an affiliate personal information about a consumer.
Status	Pending
Definitions	"Personal information": means information that a business can use to identify a person, including the name, address, social security number and financial data of the person; "Radio frequency identification": means identification by technologies that use radio waves or

	other means to identify consumer goods automatically; and "Tag": means a device that is able to transmit consumer identification information from an item to a business or affiliate.
State - Bill #	Rhode Island - H 5929
Title	Relating to state affairs and government -- Restricting radio frequency identification devices
Purpose	Prohibits state or local government from using RFID to track movement or identity of employees, students or clients or others as condition of a benefit or service.
Summary	No state or municipal agency, or any subdivision thereof, shall use, or request the use of, Radio Frequency Identification Devices (RFID) for the purpose of tracking the movement or identity of any employee, student or client, or of any other individual as a condition of obtaining a benefit or services from such agency.
Status	Pending
Definitions	N/A
State - Bill #	South Dakota - House Bill No. 1114
Title	An Act to restrict the use of radio frequency identification technology in humans.
Purpose	Prohibits requiring a person to receive implant of an RFID chip.
Summary	No person may require the implantation of any radio frequency identification microchip in any other person.
Status	Pending
Definitions	For the purposes of this section, radio frequency identification is technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum and can be used to identify an individual.
State - Bill #	Tennessee - House Bill 300 and Senate Bill 699
Title	A bill requiring conspicuous labeling of goods containing RFID
Purpose	Requires conspicuous labeling of goods containing RFID disclosing existence of RFID and that it can transmit unique information.
Summary	Regulates the selling of any goods containing a radio frequency identification tag that does not bear a label on the good or the good's packaging that: 1) States, at a minimum, that the good or the good's packaging contains or bears a radio frequency identification tag, and that the tag can transmit unique identification information to an independent reader both before and after purchase; and 2) Is in a conspicuous type-size and location, in print that contrasts with the background against which it appears.
Status	Pending
Definitions	"Radio frequency identification" or "RFID": means technologies that use radio waves to automatically identify individual items; "Tag": means a microchip that is attached to an antenna and is able to transmit identification information.
State - Bill #	Utah - H.B. 185
Title	This bill amends the Utah Computer Crimes Act.
Purpose	Amends computer crime law to include RFID.
Summary	A person who without authorization gains or attempts to gain access to and alters, damages, destroys, discloses, or modifies any computer, computer network, computer property, computer system, computer program, computer data or software, and thereby causes damage to another, or obtains money, property, information, or a benefit for any person without legal right, is guilty of a crime, and if the information or benefit is a license or entitlement or confidential, then the crime is a third degree felony. However, it is an affirmative defense to Subsections (1) and (2) that a person obtained access or attempted to obtain access in response to, and for the purpose of protecting against or investigating, a prior attempted or successful breach of security of a computer, computer network, computer property, computer system whose security the person is authorized or entitled to protect, and the access attempted or obtained was no greater than reasonably necessary for that purpose. Furthermore, a person who uses or knowingly allows another person to use any computer, computer network, computer property, or computer system, program, or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other

	things of value by false pretenses, promises, or representations, is guilty of an offense based on the value of the money, property, services, or things of value.
Status	Pending
Definitions	<p>"Computer": means any electronic device or communication facility [with data processing ability] that stores, retrieves, processes, or transmits data.</p> <p>"Computer system": means a set of related, connected or unconnected, devices, software, or other related computer equipment.</p> <p>"Computer network":</p> <p>(a) the interconnection of communication or telecommunication lines between:</p> <p>(i) computers; or</p> <p>(ii) computers and remote terminals[.]; or</p> <p>(b) the interconnection by wireless technology between:</p> <p>(i) computers; or</p> <p>(ii) computers and remote terminals.</p> <p>"Computer property": includes[but is not limited to] electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.</p>
State - Bill #	Texas - H.B. No. 2953
Title	Relating to the identification of public school students through the use of radio frequency identification technology.
Purpose	Prohibits school district from requiring student to use an RFID device for identification, and requires school to provide alternative method of identification to those who object to RFID.
Summary	A school district may not require a student to use an identification device that uses radio frequency identification technology or similar technology to identify the student, transmit information regarding the student, or track the location of the student. A school district that permits the voluntary use of a student identification device described by Subsection (b) shall provide an alternative method of identification for a student if the student's parent or guardian submits timely written objection to the use of radio frequency identification technology.
Status	Pending
Definitions	" Radio frequency identification technology ": means a wireless identification system that uses an electromagnetic radio frequency signal to transmit data between a card, badge, or tag and another device without physical contact.

Endnotes

- ¹ Statements made by Alan Estevez, Assistant Deputy Under Secretary of Defense (Supply Chain Integration), Congressional Internet Caucus Advisory Committee Event, Washington, DC, March 9, 2005.
- ² "DoD Tries Tags That Phone Home," RFID Journal, March 21, 2005.
- ³ USDA Press Release, April 27, 2004.
- ⁴ "RFID's positive identification," Federal Computer Week, April 18, 2005.
- ⁵ "Virginia Beach sees RFID payoff," Federal Computer Week, March 4, 2005.
- ⁶ The Forrester Research Brief, "Wal-Mart's RFID Progress: No Big Bang, But Good Progress," December 16, 2004.
- ⁷ "On Location: McCarran International Airport," Network Computing Magazine, January 22, 2004.
- ⁸ "The life and times of an RFID chip," NetworkWorld, August 1, 2005.
- ⁹ Collins, Jonathan, "Safeguarding Shipping Profitably," 2005.
- ¹⁰ "RFID's Good, Bad & Ugly," *Wireless Week*, July 22, 2005.
- ¹¹ *Orange County Register*, Summer 2005.
- ¹² Testimony of James Christian, VP and Head of Global Corporate Security, Novartis International AG. before the US House of Representatives Subcommittee on Commerce, Trade, and Consumer Protection, House Energy and Commerce Committee, June 15, 2005.
- ¹³ ITG is an ASSA ABLOY business entity made up of separate ASSA ABLOY Group companies focused on current and emerging identification solutions. ITG is based out of ASSA ABLOY's U.S. headquarters in Irvine, California. HID Corporation is the largest manufacturer of contactless access control readers and cards for the security industry, HID has shipped over 200 million credentials to customers worldwide. HID pioneered the development of radio frequency identification (RFID) technology for physical access control. Proximity and iCLASS® technologies can be housed on the same credential and combined with other technologies such as magnetic stripe, barcode, or contact smart chip modules. This provides users the ability to leverage their investment in existing systems while seamlessly upgrading to new technologies and adding new applications. For increased security, users can add a photo ID or anti-counterfeiting element such as a hologram or ultraviolet ink. HID's experience in developing card technologies enables them to play a critical role in the evolution and adoption of contactless smart card technology used for applications such as access control, IT secure authentication, digital cash, the storage of biometric templates, and the storage and retrieval of critical information. For more information on HID, visit www.hidcorp.com.