The Virginia Joint Commission
JCOTS
on Technology and Science

RFID
Radio Frequency Identification
Overview and Implications

I. Introduction

Radio Frequency Identification (RFID) is an extraordinary technology and its public and private utilization is growing exponentially. The adoption of RFID is revolutionizing how businesses monitor their supply chains and the government's ability to supply services and provide for homeland security. The technology offers greater abilities for the government to increase efficiency and businesses to analyze inventory and security controls than traditional methods. The adoption of RFID tags is increasing in all areas of life. As consumer awareness of the presence of RFID rises, so to will the privacy concerns associated with radio frequency identifications' ability to locate and track individual items. The present and future use of RFID yields continuing benefits to consumers, manufacturers, and government. However, the use of RFID also raises debate among privacy advocates regarding individual privacy concerns of the technology's applications.

This overview defines Radio Frequency Identification and explains its present and future applications. The memorandum will also outline policies that have been considered, both federally and in states, to address the privacy concerns raised by the technologies public and commercial adoption and implementation.

II. RFID Technology Overview

A. History of RFID

RFID was first widely used in World War II as a mechanism for the British air defense radar to determine which aircraft were friendly and which were foe. The aircraft would receive a radar signal from a ground station and would reply with a series of pulses which then would be recognized as a friendly aircraft. This system is the predecessor to today's friend or foe identification system used by the American military.[1] It has since developed into a technology which is easily adaptive to commercial and public use.

[1] Bill Glover & Himanshu Bhatt, *RFID Essentials* 59 (2006).

B. RFID Characteristics

1. Physical Characteristics

RFID tags are composed of an antenna and a chip. The tag may be housed in plastic card, called a “contactless smart card” or paper labels called “smart labels." Glass vials can contain tags which can be heat tempered or adaptive to placement in liquids.

2. Power Source

- *Passive tags* do not contain a power source and cannot initiate communication with a reader. A passive tag obtains the energy necessary to communicate completely from the reader. Passive tags are the least expensive of available tags and are the most abundant. Passive tags are used in building access cards and in tracking goods through the supply chain. Current readability range is approximately ten feet but may vary significantly depending on the size of antenna and reader.

- *Semi-passive tags* contain their own power source but require a reader’s radio signal to initiate communication. The tags onboard power allows the ability to detect by sensors and store environmental factors, such as moisture and temperature. This environmental data is referred to as “smart dust”. Tags utilizing smart dust currently cost $100 but reportedly may drop to below $10 in a few years. [2] Not all semi-passive tags utilize sensors to create smart dust.

- *Active tags* contain a battery and do not require a reader in order to acquire the energy necessary to communicate. Tags that contain batteries may communicate from longer distances, up to 750 feet. These tags send a continuous signal and are the most expensive tags. Active tags are used for toll passes, such as the "E-Z Pass," and generally the use must justify the increased cost of the more expensive active tag.

3. Technical Explanation of Components

- The **chip** stores information about the individual product to which it is attached. The information can vary in its specificity depending on the storage capability of the RFID tag. Generally, in commercial use RFID chips contain an Electronic Products Code. The storage of product information on an RFID is analogous to the Universal Product Code (UPC), or barcode. Both UPCs and EPCs allow

[2] STAFF OF THE FED. TRADE COMM’N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 6 (2005), http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

retailers to readily identify products by using computerized equipment to speed up transactional efficiency. Line of sight is needed to read a UPC's bar code, such as in the grocery store checkout. RFID may be read remotely, without line of sight, at varying distances depending on the size of the antenna.

- A chip requires an **antenna** so that the data may be retrieved. The antenna acts as a conduit between the chip and the reader. Antennas vary in size depending upon the range required for the particular use. The composition of a chip and an antenna is commonly referred to as the **tag**.

- The use of an RFID tag requires a **reader**, also called interrogators, which send out radio waves in a certain frequency to the tag. The radio waves signal the RFID tag to respond with the information contained on the chip. The antenna picks up the radio frequency energy which it converts to electrical energy. The electrical energy then powers the chip and allows it to communicate its identity to the reader by differentiating the resistance on the antenna in its reply signal. The signal is similar to Morse code.[3]

  Readers vary in size according to their use. A reader may be stationary or portable. RFID readers can process hundreds of items at the same time, unlike UPC readers, making RFID much more efficient. The reader acts as an intermediary between the tag and a network. After receiving a reply, the reader will then need network interface capability and a database to decipher the chip's information into language capable of human understanding.

  - *Tunnel readers* use an enclosure that houses antennas which direct their radio frequency waves at the tags. The enclosure usually is in the form of a conveyor belt. Tunnels are highly efficient in commercial use on assembly lines or packaging conveyors, because they allow management to identify the location of a particular good in its production.[4]

  - *Handheld readers* are similar to UPC readers in the super market but as previously discussed, do not require line of sight. Many RFID handhelds are capable of reading UPC codes. Handhelds may communicate to a database wirelessly or by radio frequency modems.[5]

  - *Forklift readers* are currently available. A forklift reader may be highly useful in the distribution chain by both wholesalers and manufacturers. A reader can read hundreds of tags in seconds, greatly reducing the need for manual participation, thus lowering overhead and increasing speed.[6]

---

[3] *See* Glover, *supra* note 1, at 37.
[4] *Id*. at 114.
[5] *Id.* at 115.
[6] *Id.*

- *Smart Shelves* allow real time inventory of retailer items. A retailer may equip shelves with readers which query on a constant interval. A database keeps track of events that signify that a product has moved. The database can then report to a manager when product levels reach a critical quantity that requires an order from the manufacturer. Smart Shelves can also be utilized in detecting expiration dates and product recalls.[7]

4. Data Storage

RFID tag storage capacity varies greatly depending on the size and power source of the tag. Another factor dictating storage ability is whether the RFID is "read-only" or "read/write capable". A read-only tag has the data permanently stored in the chip when it is manufactured. A read/write capable tag can have new data saved to its chip after it has been made. Read-only tags are less costly and have a longer read range. Chips, besides storing an Electronic Products Code, may store biometric data such as fingerprints or photographs. The following section discusses varying tag storage capacities.

- One-Bit Electronic Article Surveillance tags (EAS) are used by retailers for theft prevention. An EAS tag is a rudimentary RFID device that communicates to the reader either a one or a zero that signals when a tag is present or absent. If a tag is detected a database is signaled that triggers an alarm to alert staff that an object is being taken out of the store. EAS tags are always passive and are incapable of memory storage. The tags are inexpensive and are abundantly used by retailers.[8]

- The U.S. Department of Defense recently ordered active tags capable of storing up to 256 bytes of storage. Tags with such a large capacity of storage can be used to store large quantities of information such as an object's previous locations, photographs, or electronic signatures.[9]

Typical Characteristics of RFID Tags

	Passive Tags	**Semipassive Tags**	**Active Tags**
Power supply	external (from reader)	internal battery	internal battery
Read Range	up to 20 feet	up to 100 feet	up to 750 feet
Type of Memory	mostly read-only	read-write	read-write
Cost	$.20 to several dollars	$2 to $10	$20 or more
Life of tag	up to 20 years	2 to 7 years	5 to 10 years

Source: GAO[10]

[7] *Id.*
[8] *Id.* at 68.
[9] *Id.*
[10] OVERNMENT ACCOUNTABILITY OFFICE, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION IN THE FEDERAL GOVERNMENT 8 (2005), http://www.gao.gov/new.items/d05551.pdf.

III. RFID Applications

A. Commercial Use

1. Loss Prevention

RFID tags can prevent counterfeiting because the serial number within the tag is individual to the specific good and will not be registered as the genuine product.[11] A manufacturer can determine that a theft occurred and the location of the incident in the chain of delivery. Retailers also use RFID tags to stop shoplifters. As discussed below, the Food and Drug Administration has asked drug manufacturers to use the technology to proscribe counterfeiting of pharmaceuticals.

2. Inventory Monitoring

By using tunnel, handheld and smart shelf readers the commercial dependence on manual labor to input shipments and arrivals is lowered drastically. The speed and efficiency of the supply chain will increase exponentially by the universal adoption of RFID. In the case of a product recall, RFID tags also allow manufacturers to determine exactly which products delivered to retailers must be recalled. The ability to narrow a recall to a few goods produced sequentially greatly reduces the costs associated with recalling entire product lines.

Retailers and manufacturers use RFID to have an unobstructed view of their supply chain.[12] In 2003, an investment firm stated that Wal-Mart could save $8.35 billion per year by completely utilizing the capabilities of RFID.[13] The company currently has over 300 of its suppliers tagging products.[14] Wal-Mart predicted in 2006 that over 1,000 of its stores and 600 suppliers would utilize the technology by January of 2007.[15] Out-of-stock tagged items are replenished three times faster then non-equipped items.[16] Perishable goods are being monitored by RFID tags to make sure fruits are sold when ripe. The mandated use of RFID technology now includes companies such as Target and Rite-Aid.[17]

---

[11] Gal Eschet, *FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification*, 45 Jurimetrics 301, 307 (2005).
[12] *Id.* at 302.
[13] Mark Roberti, *Analysis: RFID—Wal-Mart's Network Effect*, CIO INSIGHT (Sept. 15, 2003), *available at* http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.
[14] Marc Songini, *Wal-Mart Details its RFID Journey*, Computerworld Software (March 2, 2006), *available at* http://www.computerworld.com/industrytopics/retail/story/0,10801,109132,00.html.
[15] *Id.*
[16] *Id.*
[17] For a demonstration of the use of RFID tags in distribution and inventory monitoring *see* EPCglobal, The EPCglobal Network Demonstration (2004), *available at* http://www.epcglobalinc.org/about/media_centre/EPCglobal_Network_Demo.pdf.

Livestock and pets are monitored by RFID tags to indicate their medical records and shot and drug history. The tags are typically attached to the cattle's ear and are re-used. RFID use can also be correlated with a database which stores information such as daily diet and in the case of cattle milk output. This offers farmers the ability to determine top producers and apportion the correct amount of food and water to ensure the highest production of milk.

B. Government Use

1. Federal[18]

The Federal Enhanced Border and Visa Entry Reform Act of 2002 created passports, which electronically store the photograph and identifying information of the passport holder.[19] The RFID technology utilized in e-Passports is a contactless smart card contained in the cover of passports which stores the name, birthdate, country of citizenship, and the image of the individual.[20]

The Food and Drug Administration issued a report in 2004 titled *Combating Counterfeit Drugs* which stated the widespread adoption of RFID tags by pharmaceutical manufacturers could help decrease counterfeit drug cases.[21] The FDA found that adoption of RFID by 2007, as a tracking device, would provide better protection against counterfeiting then other available practices. The FDA stated that the technology acts as an anti-counterfeiting device because authentication technology makes it more difficult to produce a copy of the drug, packaging, and labeling. Tags also provide a way to authenticate these drugs. In early 2004, Wal-Mart began attaching RFID tags to all bottles of controlled substances. The FDA currently measures the adoption of RFID technology by pharmaceutical manufacturers, wholesalers, and retailers. The *FDA Counterfeit Drug Task Force Report: 2006 Update* restated its commitment to utilize the tags to track drugs and discourage counterfeiting. The task force recommended that stakeholders should "move quickly to implement the technology."[22]

---

[18] *See* Appendix I for a GAO table of Federal Agencies' Reported Use or Planned Use of RFID Technology.

[19] A summary of the Enhanced Border Security and Visa Entry Reform Act of 2002 is *available at* http://www.ofr.harvard.edu/additional_resources/Summary_of_Enhanced_Border_Security_Reform_Act_HR3525.pdf.

[20] Marci Meingast *et al., Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport* (2007), *available at* http://www.law.berkeley.edu/clinics/samuelson/projects_papers/Meingast_King_Mulligan_RFID_2007.pdf .

[21] FOOD AND DRUG ADMINISTRATION, COMBATING COUNTERFEIT DRUGS (2004), http://www.fda.gov/oc/initiatives/counterfeit/report02_04.pdf.

[22] FOOD AND DRUG ADMINISTRATION'S COUNTERFEIT DRUG TASKFORCE, FDA COUNTERFEIT DRUG TASK FORCE REPORT: 2006 UPDATE, at 11, http://www.fda.gov/oc/initiatives/counterfeit/report02_04.pdf.

2. State

California uses tamper-proof RFID wristbands in Calipatria State Prison for inmate monitoring. The wristbands allow real-time location of the entire prison population which is stored to a database. If an incident takes place prison officials can access the information on databases and identify and locate which individuals were in the vicinity of the incident. California has reduced property damage, inmate violence and escape attempts by using RFID technology.[23]

Library activities are increasingly monitored by RFID tags which are placed in books. RFID reduces the costs of staffing circulation desks and alerts staff when a book is misplaced. It creates greater efficiency in stocking shelves since the RFID tag may include the Dewey Decimal number thus not requiring the manual affixation of the code. Currently, more than 300 public libraries utilize RFID.[24]

IV. Privacy Concerns

RFID privacy concerns will continue to increase as public and private adoption becomes more widespread. Currently, RFID technology may be cloned (i.e., copied and used to access prohibited areas as the holder of the RFID tag) if biometric or encryption standards are not utilized. However, RFID technology is incapable of pinpointing the location of individuals by Global Positioning System technology. To locate an individual article that contains RFID, the article must be read by an RFID reader and a database must then be accessed to decipher the information contained in the EPC or other information.

RFID privacy concerns can be distinguished between commercial and private invasion. Commercial invasion could occur when tags are used in shopping cards at grocery or clothing stores. Businesses could monitor where an individual traveled in a store by remote readers and access a shopper's purchasing habits. Industry representatives argue that consumers do not have an expectation of privacy because the acceptance of shopping cards waives any privacy concerns associated with businesses' collection of data. Commercial entities also assert that individuals do not have an expectation of confidentiality because they are aware that their spending habits are stored when a shopping card is used. Businesses believe that consumers are willing to accept a small invasion of privacy regarding consumer behavior to allow for the greater benefit of tailored shopping experiences. For example, a business could recognize a consumer's previous purchase and offer a sale on a complimentary good tailored directly to that individual. Representatives of industry feel that if businesses overly invade individual privacy that consumers will change their shopping preferences. Therefore, consumer

---

[23] *See* Eschet, *supra* note 11, at 308. For a description of the FRID system used at Calipatria State Prison *see* Technology System International Inc.'s Web site at http://tsilink.com.
[24] Ricardo Ochoa, *Radio Frequency Identification a Guide for Policy Makers* (December 6-7, 2005), *available at* http://www.ncsl.org/programs/lis/privacy/rfidclose-fall05.htm.

decisions will dictate industry self-regulation to ensure an appropriate balance between individual privacy and business profit.

Non-commercial third parties can use personal readers to gain access to data stored on tags to commit crimes. Tag data may be used to gain insight into the contents of a woman's purse or to duplicate the signal given by a tags chip. For example, a mischievous individual could monitor pedestrians on a sidewalk to discover the most advantageous victim by assessing the presence of iPods, types of wallets, car keys, and designer purses. Some individuals have contended that E-passports may also allow criminals or adversaries in other countries to determine a possible victim's nationality and whereabouts. These assertions are countered by the fact that thieves would need high-tech equipment and the ability to access a database that could identify these products or decrypt the information on RFID tags. It seems relatively unlikely that criminals may gain access to such information without high skilled technical expertise.

Unauthorized duplication of a legitimate tag is known as cloning. The cloning of tags is possible and has been demonstrated by Information Technology professionals. Recently, in California, at the request of a state legislator, an individual duplicated a RFID tag signal that allowed restricted access into a government building. Also, tags inserted into humans have been proven vulnerable. The ability to duplicate the signal of tags may require added security measures discussed in the next section.

It is also postulated that government personnel could monitor the whereabouts of an individual under investigation by accessing readers and following the locations of where the suspect is scanned. Tag information could be accessed in criminal investigations to determine what parties where in the vicinity at the time of the crime, allow quicker identification of victims, and locate the whereabouts of stolen goods. Currently, the use of RFID is not so widespread to validate use by government law enforcement, because of the absence of readers in private places and inability of the government to use this technology.

V. Current Privacy Protections

The threats posed by RFID technology have raised many practice solutions to protect the access of information contained within tags. The policies that seek to address privacy concerns pertain to technology and regulations meant to safeguard access to individual tags. The following is a brief description of privacy enhancing technology, commercial self-regulation, and encryption of data stored on the chip.

A. Privacy Enhancing Technologies

Privacy enhancing technologies protect access to data by providing a protection to the readability of tags.

- A *Faraday Cage* is protective sheet of foil or mesh which blocks or greatly reduces the distance and ability of a reader to send Radio Frequency to the RFID tag.[25]

- *Authentication Technology* requires an individual to acquire permission to use a reader and gain the information contained on RFID tags within its zone. This method is not considered reliable due to the acquisition and use of readers by private individuals. Also, inefficient encryption may allow individuals to hack into readers. Readers which require user authentication may still read tags not germane to the purpose of the reader.[26]

- *Tag-Killing Technologies* would disable RFID tags the moment a consumer purchases a product containing a tag. The Massachusetts Institute of a Technology AutoId Center has proposed the policy that after purchase of a good the RFID tags would receive a kill command that would disable the tag's readability. [27] Tag-killing technology is still in its infancy and has yet to be adopted.

B. Fair Information Practices

Fair Information Practices are self-regulations imposed by industry to protect consumers. Many organizations have developed Fair Information Practices to alert customers to the presence of RFID and its uses and abilities. Fair Information Practices generally adhere to similar guidelines utilizing the privacy protections of "notice, choice, access, security, and enforcement."[28]

- The *RFID Bill of Rights* was created in 2002 by Simson Garfinkel as a voluntary framework for commercial deployment of RFID tags.[29] The guidelines adhere to the general principles espoused by organizations interested in consumer privacy.

    a. The right of the consumer to know what items possess RFID tags;
    b. The right to have embedded tags removed, destroyed, or deactivated upon purchase of these items;
    c. The right of the consumer to access the data associated with an RFID tag;
    d. The right to access of service without mandatory use of RFID tags "(e.g. the right to return a product or travel on a particular road),"[30] and:

---

[25] *See* Eschet, *supra* note 11, at 317.
[26] *Id.*
[27] *Id.* at 318.
[28] *Id.* at 324-325.
[29] Simson L. Garfinkel, *An RFID Bill of Rights*, 105 Tech. Rev. 35 (2002).
[30] Simson L. Garfinkel, *Adopting Fair Information Practices to Low Cost RFID Systems* 1, at 4, *available at* http://scrawford.net/courses/RFID%20Bill%20of%20Rights.pdf.

e. The right to know when, where and why the data in RFID tags is accessed and being read.

3. Data Encryption

The use of encryption allows tag using entities to reduce the risk of unauthorized access to sensitive information. Encryption is the process of transforming ordinary data into code form using a key and algorithm. Only authorized users who possess the key may decode the information. The use of encryption can safeguard against unauthorized access to sensitive information. For example, only readers possessing the proper key could access and decode the stored information on a tag's chip.

VI. Current Legislative Initiatives

There are no federal or state statutes which currently address private and commercial spying and tracking actions.[31] The increased use of RFID in the public and private sectors will continue to raise concerns among privacy advocates. Federal laws mandate that federal agencies ensure that private information is not disseminated by the agencies themselves. However, Congress has yet to further this protection to commercial privacy intrusions.

The states have addressed RFID privacy concerns by different legislative initiatives, but passage of the legislation has generally been unsuccessful. The proposals can be categorized by either requiring removal or disclosure of the presence of tags or prohibiting the use of tags or its linkage to personal information.

A. Federal Law

Radio frequency identification tags are governed by the Federal Trade Commission (FTC). The FTC allows corporations to adopt their own guidelines in the commercial use of consumer information obtained by RFID technology.[32] The FTC has not taken any action or compiled any data regarding the commercial use of RFID.[33]

The United States Government Accountability Office released a report on Information Security titled *Radio Frequency Identification Technology in the Federal Government* in May of 2005.[34] The report discusses the privacy concerns that the federal government must address to comply with the Privacy Act of 1974 and the E-Government

---

[31] Serena G. Stein, Note, *Where Will Consumers Find Privacy Protection from RFIDS? A Case for Federal Legislation*, 2007 Duke L. & Tech. Rev. 0003 at 2, *available at* http://www.law.duke.edu/journals/dltr/articles/pdf/2007DLTR0003.pdf.
[32] *Id.* at 12. Citing, Jonathan Collins, *FTC Asks RFID Users to Self-Regulate*, RFID J., Mar. 10, 2005, http://www.rfidjournal.com/article/view/1437/1/1; *see*, 5 U.S.C. §§ 41-58 (2000) (Federal Trade Commission Act).
[33] *Id.*
[34] *See* GAO, *supra* note 10.

Act of 2002. The Privacy Act protects the retrieval of personal information from use or disclosure once it is collected by the government, regardless of the technology used. The E-Government Act requires government agencies to conduct privacy assessments and evaluate whether collection of data is feasible based on privacy concerns. The federal law only addresses the privacy concerns associated with collection and dissemination of data by federal agencies. Therefore, individuals are not afforded protection of private information attained by third parties or commercial enterprises.

A bipartisan Congressional RFID Caucus has been created by two U.S. Senators, Sen. Byron Dorgan (D-ND) and Sen. John Cornyn (R-TX), to "protect exciting new technologies from premature regulation or legislation in search of a problem."[35] The caucus held two meetings so far in 2007 titled RFID and Innovation: America's Competitive Edge and RFID and Healthcare: Emergency Preparedness and Response. The RFID Technology Council is an informal organization created to support the caucus with the mission of educating Congressional members, the general public and government agencies on the uses and issues related to RFID.[36] Membership to the council is free.

Presently, U.S. Representative Dan Burton has introduced H.R. 2716 which directs the Secretary of Health and Human Services to require the incorporation of counterfeit-resistant technologies into the packaging of prescription drugs.[37] The bill requires the Secretary to incorporate RFID technology or similar track and trace technologies into the packaging of not less than the 30 most counterfeited prescription drugs. The bill is currently in the House Committee on Energy and Commerce.

In 2004, U.S. Representative Gerald Klecza introduced the federal 'Opt Out of ID Chips Act.'[38] The act, if passed, would have required that the presence of RFID tags in commercial transactions be disclosed by including a label and the option to have the tag removed or permanently disabled at the time of purchase. The bill was left in the House Subcommittee on Commerce, Trade and Consumer Protection.

B. State Law

Virginia and other states have proposed legislation that would require labeling of products equipped with tags, prohibit use of RFID for certain government purposes, and limit the information that may be contained on tags.

1. Virginia

Virginia has proposed legislation in the 2004, 2005, and 2007 sessions of the Virginia General Assembly. The legislation has been aimed at requiring disclosure of

[35] *Id.* at 14.
[36] http://www.rfidtechcouncil.org/ (last checked June 25, 2007).
[37] Reducing Fraudulent and Imitation Drugs Act of 2007, H.R. 2716, 110th Cong. (2007).
[38] Opt Out of ID Chips Act, H.R. 4673, 108th Cong. (2004).

RFID use in consumer goods, conducting privacy impact analysis, and restricting the use of information stored on databases related to movement.

In 2007, Delegate Albert Eisenberg proposed HB 2086, the Virginia Radio Frequency Identification Disclosure Act, which, if passed, would have required sellers of consumer goods to disclose the presence of tags by placing a conspicuous label on the good. The bill was passed by in the House Committee on Science and Technology and a letter was sent to JCOTS which resulted in this memorandum. The legislation would subject any person or business who violated the required disclosure of RFID tags to the enforcement provisions of the Virginia Consumer Protection Act of 1977.[39]

HB 1304 (Lingamfelter, 2004), if passed, would have required public bodies to conduct a privacy impact analysis when authorizing or prohibiting the use of RFID and other technologies. The bill would require JCOTS to propose guidelines and policies for public bodies to follow in conducting privacy impact analysis to the governor and 2006 session of the General Assembly. These guidelines and policies would have included the reasons for use of RFID, the impact of its use on civil liberties, and any safeguards that should be used to mitigate negative impacts. The bill was carried over to the 2005 session of the Virginia General Assembly where it was left in the House Committee on Science and Technology.

The 2004 General Assembly session passed SB 148 (Cuccinelli) which restricts the use and access of data generated by electronic toll-collection systems (e.g., Smart Tag). The legislation only allows the information stored on toll databases to be disclosed to a court of competent jurisdiction. The legislation also awards injunctive relief and payment of attorney's fees to a person aggrieved by a violation of the statute.[40]

2. Other States

In 2005, at least 12 states introduced legislation to address privacy concerns related to RFID tag technology. In 2006, the number of states introducing RFID legislative initiatives grew to at least 17.[41] The legislation was particularly concerned with the linkage of personal information to tags. In 2006, three states adopted or enacted RFID legislation: Georgia, New Hampshire, and Wisconsin. California and Rhode Island had RFID legislation vetoed.[42]

In Georgia, H.R.1558 (Representative Setzler, 2006) created the House Study Committee on Biological Privacy. The committee studied the use of biological information and technology by government and private entities and recommended actions and legislation it deemed necessary. Representative Ed Setzler, Chairman of the

[39] Va. Code § 59.1-196.
[40] Va. Code § 33.1-252.2.
[41] For a full description of 2005 introduced legislation and status see Appendix II.
[42] For a full description of 2006 introduced legislation and status see Appendix III.

Committee on Biological Privacy, introduced a bill in 2007 which prohibits entities use of RFID technology in ways which relate to genetic information in issuance of insurance, employment decisions, enrollment decisions by educational institutions, and prohibits implantation of biometric sensors. The bill is currently before the Georgia House of Representatives.

New Hampshire enacted H.B. 203 (Rep Dickinson, 2006) which established a commission on the use of RFID technology. The commission's findings and recommendations are required by November 1, 2007 and the final report is expected on or before November 1, 2008. Wisconsin's Assembly Bill 290 (2005), as passed, prohibits any person from requiring another to undergo implantation of a microchip.[43]

Generally, states have sought to require that the use of RFID be disclosed, removed or deactivated after purchase of goods equipped with the technology, or prohibited linking RFID data to personal information. The legislation has addressed use by governmental agencies and commercial entities. The deficiency in knowledge of the technology's capabilities has led many legislators to propose initiatives which can slow the commercial adoption of RFID. Exaggerated privacy intrusions are among the leading issues that drive these legislative policy initiatives but many of the intrusions either have not yet been realized or are grossly overstated. As discussed above, the technology is in its early stages and both mass falsification of data, by corruption of databases, and commitment of fraudulent acts, by cloning, has yet to occur.

VI. Conclusion

Commercial and governmental adoption of RFID will increase as public and private enterprises realize greater efficiency and profits. The ability to integrate the technology seamlessly in the supply chain and retail sectors of commercial enterprises allows RFID to be both present everywhere and appear nonexistent to consumers. The privacy concerns associated with RFID will escalate as the public becomes more aware of the use of the technology . It is important to understand the capabilities and inabilities of RFID to correctly analyze future policy recommendations.

[43] Wis. Stat. § 146.25 (2005).

Appendix I

Federal Agencies' Reported Use or Planned Use of RFID Technology

Agency	Application
Department of Defense	Logistics support
	Tracking Shipments
Department of Energy	Detection of prohibited articles
	Tracking movement of materials
Department of Health and Human Services	Physical access control
Department of Homeland Security	Border control, immigration and customs (U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)
	Location system
	Smart containers
	Tracking and identification of assets
	Tracking and identification for use in monitoring weapons
	Tracking and identification of baggage on flights
Department of Labor	Tracking and locating case files
Department of State	Electronic passport
Department of Transportation	Electronic screening
Department of the Treasury	Physical and logical access control
	Records management (tracking documents)
Department of Veterans Affairs	Audible prescription reading
	Tracking and routing carriers along conveyor lines
Environmental Protection Agency	Tracking radioactive materials
General Services Administration	Distribution process
	Identification of contents of shipments
	Tracking assets
	Tracking of evidence and artifacts
National Aeronautics and Space Administration	Hazardous material management
Social Security Administration	Warehouse management

Source: GAO, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION IN THE FEDERAL GOVERNMENT 13 (2005).

Appendix II

2005 RFID Legislation of the States

State	Bill number	Requires disclosure	Requires removal or deactivation	Prohibits linking RFID to personal information	Prohibits use	Other
California	S.B. 682 09/09/05 Legislature adjourned 05/16/05 Passed Senate 08/17/05 Placed on Comm. on Appropriations suspense file	Yes, disclosure of device, reader locations, shield devices and reason for reading. Annual updates required.		Yes	In four kinds of mass-distributed identification documents issued by the government: drivers' licenses, K-12 student IDs, government health and benefit cards, and public library cards. This timeout for RFID in these four kinds of mass-distributed IDs is for only three years.	Criminalizes remotely reading the document without the owner's knowledge.
	S.B. 768 09/09/05 Legislature adjourned 05/31/05 Passed Senate 09/08/05 Placed on inactive file on request of Assembly Member.	Yes, disclosure of device, reader locations, shield devices and reason for reading. Annual updates required.		Yes	Same three year timeout as above, but, permits the use of RFID in government-issued IDs. However, in some cases the IDs must meet certain security and privacy requirements. In most cases, the documents cannot remotely transmit information other than a unique personal identifier number	Criminalizes remotely reading the document without the owner's knowledge.
Illinois	H.B. 4088					Provides that a hospital must use a RFID tag in each surgery performed at the hospital. The tag must identify the patient & surgeon, date & type of surgery, the body part

						to be operated on.
Maryland	H.B. 354 04/11/05 Legislature adjourned					Creates a task force to study the use of RFID by retailers and manufacturers.
Mass.	H.B. 1447 S.B. 181 01/26/05 H Referred to the committee on Consumer Protection; Senate concurred	Yes	Yes			Attorney general to promulgate regulations
Missouri	S.B. 128 05/26/05 Legislature adjourned	Yes				
	S.B. 638 2006 Regular Session	Yes				
Nevada	A.B. 264 06/07/05 Legislature adjourned	Yes				
New Hampshire	H.B. 203 02/03/05 Retained in Commerce Committee	Yes				
New Mexico	H.B. 215 03/19/05 Legislature adjourned	Yes	Yes	Yes		
Rhode Island	H.B. 5929 07/15/05 **Vetoed by Governor**				By state or municipal agencies for tracking the movement or identity of an employee, student or client as a condition of obtaining a benefit or services.	

South Dakota	H.B. 1114 03/22/05 Legislature adjourned				In humans (no person may require RFID implantation)	
	H.B. 1136 03/22/05 Legislature adjourned		Yes		Of personal information obtained via RFID without permission	
Tennessee	H.B. 300 S.B. 699 05/28/05 Legislature adjourned	Yes				
Texas	H.B. 2953 05/30/05 Legislature adjourned				For mandatory tracking or identification of public school students.	
	H.B. 2 (1st Called Session) 07/20/05 Special Session adjourned 06/28/05 Passed House 06/30/05 Passed Senate				For mandatory tracking or identification of public school students.	
Utah	H.B. 185 03/11/05 **Signed by Governor**					Clarifies that computer crimes laws apply to wireless networks. Exempts from the Computer Crimes Act certain collections of information through the use of RFID-type technology.
Virginia	H.B. 1304 02/27/05 Legislature adjourned					Requires public bodies to conduct a privacy impact analysis when authorizing or prohibiting the use of invasive technologies, such as RFID

VA cont.	S.B. 107 04/12/04 **Signed by Governor, Chapter 660**					Authorizes research relating to methods of electronic toll collection
	S.B. 148 04/12/04 **Signed by Governor, Chapter 665**					Provides that, with three exceptions, data generated by automated electronic toll-collection systems on use of toll facilities by individually identifiable vehicles can only be disclosed when so required by order of a court
Wisconsin	A.B. 290					Prohibits requiring an individual to undergo the implanting of a microchip
Wyoming	H.B. 258 03/03/05 **Signed by Governor, Chapter 192**					Authorizes telepharmacies to use automated inventory control including RFID

Source: National Conference of State Legislatures

Appendix III

2006 RFID Legislation of the States

State	Bill number	Requires disclosure	Requires removal or deactivation	Prohibits linking RFID data to personal information	Prohibits use	Other
Alabama	S.B. 310	Yes, disclosure of device, reader locations, and shield devices. Annual updates also required.		Yes, except for a personal identifying number, in state, county or municipal government identification documents with listed exceptions including where there is a compelling state interest.		Must implement mutual authentication and encryption techniques
California	A.B. 2561 05/31/06 Passed Assembly 08/24/06 Amended removing RFID relevant portions					Asks the California Research Bureau to submit a report on security and privacy for government-issued, remotely readable identification credentials
	S.B. 433 01/26/06 Passed Senate			Yes	In DMV issued driver's licenses, or identification cards	
	S.B. 682 08/07/06 Amended removing RFID relevant portions 09/27/06 Signed by Governor, Chapter 509	Yes, disclosure of device, reader locations, shield devices and reason for reading. Annual updates also required.		Yes	In four kinds of mass-distributed identification documents issued by the government: drivers' licenses, K-12 student IDs, government health and benefit cards,	Criminalizes remotely reading the document without the owner's knowledge.

CA cont.					and public library cards. This timeout for RFID in these four kinds of mass-distributed IDs is for only three years.	
	S.B. 768 09/07/06 Sent to Governor 09/09/06 Vetoed by Governor	Yes, disclosure of device, reader locations, shield devices and reason for reading. Annual updates also required.		Yes	Same as above	Criminalizes remotely reading the document without the owner's knowledge.
	S.B. 1078 05/31/05 Passed Senate			Yes	In any device issued to a student by a public school, school district, or county office of education	
Florida	H.B. 591 05/01/06 Passed House					Authorizes private companies to operate surveillance under court order (such as for sex offenders). Criminalizes tampering with tracking devices. Authorizes electronic monitoring with RFID within correctional facilities and sets requirements for such systems

	S.B. 450					Authorizes private companies to operate surveillance under court order (such as for sex offenders). Criminalizes tampering with tracking devices.
Georgia	H.R. 1558 03/28/06 Adopted by House					Creates the House Study Committee on Biological Privacy. The committee shall undertake a study of the conditions, needs, issues, and uses of biological information and technology by government and private entities and associated problems and recommend any actions or legislation which the committee deems necessary or appropriate.
Illinois	H.B. 4088					Hospitals must use RFID tags in connection with each surgery performed at the hospital. The tag must identify: (i) the patient and the surgeon, (ii) the date and type of surgery, and (iii) the body part to be operated on.
	H.B. 4259					Provides that no one may encode more than the last 4 digits of a social security number in or on a card or document, including, using a

						chip or other technology, in place of removing the social security number as required by law.
	S.B. 2558	Yes, for any article for sale by a retailer.	Retailers must offer ability to have the circuit removed free of charge.		Prohibits use in any identity document created, mandated, or issued by the government.	Uses the term "Contactless integrated circuits"
Kansas	H.B. 2820					Establishes standards for Drug Pedigrees and sets guidelines for selecting an implementation date for an electronic pedigree system.
	H.R. 6013					States that the "possibility of radio frequency identification tags being placed in national identification cards are a potential invasion of civil liberties" and asks Congress to repeal Real ID Act.
Mass.	H.B. 1447 / S.B. 181	Yes	Yes			Attorney general to promulgate regulations
Michigan	H.R. 239					An initiative to have all cattle in Michigan identified through a radio frequency identification device
Missouri	S.B. 638	Yes				

	S.B. 858 02/09/06 Passed Senate					Prohibits an employer from requiring an employee to have personal identification microchip technology implanted as a condition of employment.
New Hampshire	H.B. 203 05/23/06 Signed by Governor, Chapter 165					Commission on the use of RFID. Requires commission to report its findings and legislative recommendations by November 1, 2007 and submit a final report before Nov. 1, 2008.
NH cont.	H.B. 1738 05/10/06 Signed by Governor, Chapter 107				Prohibits surveillance devices, including RFID devices, to identify ownership of vehicles or their occupants	Provides exceptions.
New Jersey	A.B. 3015 / S.B. 1866	Yes				Prohibits requiring an individual to have an implanted or attached microchip. Prohibits implantation or attachment without written and informed consent. Provides that a person with such a microchip has the right to have it removed at any time. Provides criminal penalties for violations
New York	A.B. 9504	Yes, in establishment and on products.	Yes, free of charge and			Consumer can request all stored

			cannot require RFID tags for exchanges, returns, etc.			information about them from the retailer. Attorney general can enforce.
	A.B. 9505	Yes, on retail products.				Attorney general can enforce.
	A.B. 9506 / S.B. 7974 06/19/06 Passed Assembly					Establishes the radio frequency identification privacy task force.
Ohio	S.B. 349					Prohibits an employer from requiring an employee of the employer to insert into the employee's body a radio frequency identification tag
Oklahoma	H.B. 2605 03/08/06 Passed House					Implements the Oklahoma Animal Identification Program, which may set specifications and standards for the identification technologies used to track and trace animal movements.
	S.B. 1444 02/28/06 Passed Senate 04/19/06 Passed House					Implements the Oklahoma Animal Identification Program, which may set specifications and standards for the identification technologies used to track and trace animal movements.
Rhode Island	H.B. 7432 06/23/06 Vetoed by Governor				Prohibits use by state/local governments i n tracking movement or identity of	Allows civil action for violations. Uses for emergency medical care must be HIPPA compliant.

					employees, students, or clients; or as a condition for obtaining benefits or services. Exceptions for requirements of federal law, department of corrections, an d emergency medical care.	
RI cont.	S.B. 2768 06/23/06 Vetoed by Governor				Prohibits use by state/local governments i n tracking movement or as a condition for obtaining benefits or services, exceptions for requirements of federal law ands emergency response personnel.	Allows civil action for violations. Uses for emergency medical care must be HIPPA compliant.
Tennessee	H.B. 300 / S.B. 699	Yes				
	H.B. 3848 / S.B. 3816		Yes			Use of RFID tags on consumer items can only be used to deter theft
Washington	H.B. 2521	Yes, disclosure of device, reader locations, shield devices and reason for reading.		Yes, except for a personal identifying number	Prohibits use in any identity document created, mandated, or issued the government, exceptions for prisons, toll roads, etc.	Uses the term "Contactless integrated circuits". Criminalizes remote reading without permission.

	H.B. 3125					Establishes a joint task force on RFID technology
Wisconsin	A.B. 290 05/30/06 Signed by Governor, Act 482					Prohibits requiring an individual to undergo the implanting of a microchip.

Source: National Conference of State Legislatures