PUBLIC LAW RESEARCH INSTITUTE
UNIVERSITY OF CALIFORNIA HASTINGS COLLEGE OF THE LAW

RFID and Privacy

by

Mariko Yoshihara, Hastings Class of 2008

PLRI Working Paper Series
April 2007

Public Law Research Institute
UC Hastings College of the Law
100 McAllister Street, Suite 405

(415) 565-4671
(415 565-4884 (fax)
www.uchastings.edu/plri

About the Public Law Research Institute

The Public Law Research Institute was organized in 1983 at UC Hastings College of the Law to research legal issues of importance to California's state and local governments. In 2003, the Institute was incorporated into Hastings' Center for State and Local Government Law. PLRI Reports and PLRI Working Papers are written by Hastings faculty, or by Hastings students working under close faculty supervision, and with the assistance of the outstanding reference staff of the Hastings library.

From its inception, the Institute has operated under two basic principles. The first is that law students can – and, as an indispensable part of their legal education, should – contribute substantially to the solution of important problems facing state and local governments. The second is that Hastings College of the Law, founded as the law department of the University of California in 1878 to serve the interests of the people of California, has an important role to play in the search for solutions to the problems Californians currently face.

Additional copies of this paper or other papers in this series can be obtained by contacting the Public Law Research Institute at Hastings College of the Law, 100 McAllister Street, Suite 405, San Francisco, California, 94102-4978, or via email, plri@uchastings.edu.

David J. Jung
Professor of Law and Director

Joanna Weinberg
Adjunct Professor of Law

Steven Bonorris
Research Fellow in Public Law

Annie Lo
Academic Program Coordinator

RFID and Privacy

by Mariko Yoshihara*

Introduction

As the use of Radio Frequency Identification (RFID) technology becomes increasingly prevalent, concern about individual privacy becomes a more pressing issue. This Working Paper explores some of the current legislation and proposals that seek to protect consumer privacy and security in response to the potential issues accompanying RFID technology.

Background

RFID technology is an automated system of wireless data capture, consisting of two parts: the tag (or transponder) and the reader.[1] The tag is a silicon chip that contains information, usually a unique numerical identifier, transmitted by an attached antenna to the RFID reader through radio waves.[2] Depending on the radio frequency and power source, readers can pick up the radio waves at a range between three and thirty feet,[3] and read the stored digital information on the chip. RFID tags can be embedded in products, government-issued ID cards, credit cards, toll devices and even people. The privacy issues are particularly acute, as consumers can be unaware of the very presence of a tiny RFID tag as well as the fact that personal information can be transmitted at any time.

The precursors of RFID technology were first widely used during World War II to help identify ally or enemy planes.[4] Due to its efficiency and falling cost, RFID technology soon expanded into the commercial sector. Compared to magnetic strips or barcodes, which usually contain only generic, category-levels of information, RFID tags can carry significantly more data, be reprogrammed with new data, and also be read faster, from farther away, without being in a direct line of sight.[5]

---

* Mariko Yoshihara is a member of the Hastings class of 2008. This working paper was written under the supervision of Steven Bonorris, and edited by Annie Lo.

[1] G.A.O.-05-0551, at 5 (2005).

[2] *Id.*

[3] Department of Homeland Security, "Comments of the Electronic Privacy Information Center," *available at* http://www.epic.org/privacy/us-visit/comm120605.pdf [last visited March 14, 2007].

[4] "The History of RFID Technology," http://www.rfidjournal.com/article/articleview/1338/1/129/ [last visited March 8, 2007].

[5] "General RFID Information," http://www.rfidjournal.com/faq/16/50 [last visited March 14, 2007].

RFID tags come in a range of forms, and can vary in storage capacity, memory type, radio frequency, and power capability. Depending on the design and capability of the RFID tag, costs per tag can range from 20 cents to several dollars.[6] As RFID technology matures, its costs are decreasing rapidly, smoothing the way for more ubiquitous use of RFID systems. The most common type of RFID tag is passive and read-only, which means it derives its power from radio waves transmitted by the reader and contains, at a minimum, a unique serial number identifying the object to which it is attached. This type of tag is commonly attached to objects, pallets, or cases, and used for inventory control. RFID tags may also be active or semi-passive. Active tags contain a power source and transmitter that initiates communication with a reader, and usually have read/write capabilities. Examples of active tags are those used for toll passes, such as EZ Pass in the San Francisco Bay Area. Semi-passive tags do not communicate with a reader, but instead, use a battery to perform other functions, such as to power the internal electronics or write information obtained from monitoring a sensor.

Purposes

A. Commercial Use

- **Labor cost savings**
- **Inventory control**
- **Efficiency**
- **Marketing**
- **Theft prevention**

Retailers are interested in RFID technology because it allows them to maintain constant and accurate inventory data at greatly reduced labor costs.[7] In the commercial setting, RFID tags contain an Electronic Product Code (EPC) that can uniquely identify each and every tagged item. By placing an RFID tag on goods, readers at various inventory checkpoints can quickly tally the amount of goods received and ensure that the goods are originals and in the proper location. This would eliminate the need for manual counting and recounting as the goods proceed from the manufacturer to the distribution center. At the store level, retailers can use RFID technology to assess what goods are in high demand and what goods are not selling well, which makes RFID a

[6] "The Cost of RFID Equipment," http://www.rfidjournal.com/faq/20/85 [last visited March 9, 2007].
[7] Most famously, Wal-Mart has required its top hundred vendors to use RFID tags in all their shipments, to improve its supply chain management.

helpful tool in marketing and product placement schemes. Additionally, a retailer can use RFID tags' unique identifiers to ensure that returned items are in fact the ones originally purchased by the consumer. Retailers can also use RFID tags to track lost or stolen goods, or as a theft detection device to be used in-store.

For the consumer, RFID tags can make the process of purchasing products faster and easier. Commercial RFID advocates envision the possibility of a grocery store where customers walk their carts through readers that instantly identify the products in the cart, compute the amount due, and charge RFID-enabled credit cards. In addition to promoting customer convenience, this would also reduce the number of cashiers required at retail stores. RFID technology could also recommend products to the consumer based on an item of interest or the shopper's prior purchases, during a shopper's visit.

B. Governmental Use

- **Inventory control**
- **Government-issued identification cards / documents**
- **Correctional facility management**
- **Toll collecting**
- **Hospital / patient management**

Various federal agencies currently use RFID technology to track and identify sensitive objects such as radioactive material, shipments, or weapons.[8] In addition, the federal government seeks to implement new electronic, RFID-embedded passports, which would link personal information electronically from individual passports to a central database.[9] The federal government also recently tested a program that embeds RFID technology into the Arrival-Departure forms of travelers to the United States. By automatically tracking the exit and entry of travelers while having instantaneous access to their personal information, RFID technology could make processing these individuals significantly more efficient, and further ensure the security of U.S. borders. However, the Department of Homeland Security has more recently

[8] The Department of Defense is moving towards requiring its major suppliers to use pallet-level RFID tags.
[9] Department of Homeland Security, "Comments of the Electronic Privacy Information Center," *available at* http://www.epic.org/privacy/us-visit/comm120605.pdf [last visited March 14, 2007].

indicated that it is unlikely to move forward with the program due to privacy and security flaws.[10]

Other government uses of RFID technology include tags in correctional facilities, toll collection devices, and hospitals. Several states use RFID technology to track and monitor prison inmates.[11] By programming each inmate's tag, RFID technology facilitates the restriction of inmates to certain sections of the prison, as well as the separation of certain inmates by tracking their physical proximity to one another. In addition, the database could store and keep records on inmate movement or the length of time the inmate has spent in the library or on the job. RFID technology is also widely used for toll collection, e.g. EZ-Pass and Fast Pass, where an RFID tag is placed inside the vehicle, scanned by a reader inside the toll booth, and then linked to the customer's account. RFID technology is also gaining popularity in hospitals because of its ability to track the status and exact location of patients, staff, and essential equipment.[12]

A controversial use of RFID technology may soon be imposed by the Department of Homeland Security's regulations. Under the federal Real ID Act, every state government-issued identification card will be embedded with an RFID tag. The system would link the identification card to an external database that contains a digital picture and the personal information of the cardholder for verification purposes, thus reducing the efficacy of counterfeit IDs. Law enforcement officers could read the information on the ID card from a safe distance. The external database could also contain information such as an arrest warrant or an expired visa linked to that particular person.

Security and Privacy Considerations

The proliferation of RFID technology has spawned many privacy and security concerns regarding the confidentiality, integrity, security, and availability of the information on the RFID tag databases.

---

[10] "United States Visitor and Immigrant Status Indicator Technology," *available at* http://www.epic.org/privacy/us-visit/ [last visited March 14, 2007].
[11] Claire Swedberg, "L.A. County Jail to Track Inmates," *available at* http://www.rfidjournal.com/article/articleview/1601/1/1/ [last visited March 14, 2007].
[12] Jonathan Collins, "Hospital Gets Ultra-Wideband RFID," *available at* http://www.rfidjournal.com/article/articleview/1088/1/1/ [last visited March 14, 2007].

A. Commercial Use

- **Linkage of items to personal information**
- **Surveillance or monitoring**
- **Consumer profiling**
- **Commodifying consumer information**
- **Consumer awareness**

When RFID tags are used for generic inventory control and tags are placed at the pallet level, there are few privacy concerns because the RFID tag will likely never reach the hands of the consumer. However, in some instances, RFID tags are placed on individual retail items handled and purchased by consumers.

Consumer privacy advocates worry that the unique identifier in RFID tags could link specific objects to their purchasers through credit card information, thus creating a wealth of personally identifiable information and triggering a broader spectrum of privacy concerns. Privacy advocates fear this will lead to an Orwellian society where retailers or third parties can monitor and survey a consumer's movement and behavior through RFID tags.[13] RFID readers selectively placed around the store and linked to a video monitor would allow observation of consumer behavior, as piloted in a Wal-Mart store that filmed shoppers' interaction with a Max Factor lipstick display.[14] RFID readers could also be placed outside of the store premises, harvesting information about the individual's movement well beyond the point of sale, and lasting an indefinite duration.

RFID tags enable the creation of large databases of marketing information for corporations. The correlation of personally identifiable information to the purchase of specific items could create rich profiles of consumers' tastes and preferences; these databases could be sold or traded with other corporations without restriction under current law. Privacy advocates also express concern that consumers are often unaware of the existence or use of RFID technology because the tags can be extremely small, embedded into the products, and operate undetected by consumers. Thus, in contravention of established principles of fair information

[13] "Radio Frequency Identification (RFID) Systems," *available at* http://www.epic.org/privacy/rfid/ [last visited March 14, 2007].
[14] Howard Wolinsky, "P&G, Wal-Mart store did secret test of RFID," *Chicago Sun-Times*, November 9, 2003 Sunday; *see also* Mark Roberti, "The Real Scandal," *available at* http://www.rfidjournal.com/article/articleview/654 [last visited March 14, 2007].

practices, which stress transparency and notice, consumers are often unaware of the potential intrusion into their privacy by RFID technology.

B. Governmental Use

- Linkage of tag to personal information
- Surveillance and monitoring
- Intercepting or stealing personal information

With the expanding use of RFID tags in government-issued items like immigration forms, EZ Pass devices, and perhaps soon, all government-issued identification cards, privacy advocates fear the Big Brother possibilities these tags will create. With a database linking RFID tags to personal information, the federal government could track or put under surveillance particular individuals by using the radio waves in their identification cards. Like the private sector, or possibly in conjunction with the private sector, government officials could use selectively placed RFID readers to trigger surveillance cameras or to monitor the movements of particular individuals. A police officer could potentially hold an RFID reader as motorists pass by on a highway and retrieve each driver's personal information instantaneously through his or her RFID-embedded identification card or EZPass device.[15] Furthermore, there is the risk of theft of personal information by unauthorized readers, either by picking up the radio emissions from RFID tags or by accessing the centralized database of personal information.

Best Practices

In the absence of federal action on the issue of privacy and security concerns raised by this emerging technology, some states have taken the lead in striking a balance between the corporate and governmental interests in RFID tags, and consumer and citizens' legitimate expectations of privacy.[16] Many states have proposed legislation to regulate RFID usage in the

[15] "U.S. Enroute to a Big Brother Society?" *available at* http://www.cbsnews.com/stories/2003/01/15/national/main536711.shtml [last visited March 14, 2007].

[16] Similarly, some thirty-five states have adopted forms of mandatory disclosures to consumers in the event of compromised databases with personally identifiable information, led by California's SB 1386, in the vacuum created by federal inactivity on the issue. "As States Innovate on Issues, Schwarzenegger Blurs the Party Lines," *The New York Times* (January 12, 2007).

commercial setting, but as of yet, none have been signed into law.[17] All states that proposed legislation in the commercial context have, at a minimum, included consumer notice as part of the commercial regulating scheme.[18] Of those states, however, only about half have proposed anything beyond consumer notice.[19] Thus, New York demonstrates a more comprehensive approach to regulating RFID technology and addressing privacy concerns in the consumer context.

This section of the paper discusses exemplars of legislative approaches to the various controversies posed by RFID technology. A discussion of the features of the New York bill serves as a springboard for a wider discussion of the policy concerns implicated. Although it was vetoed, California's SB 768 (Simitian 2006) is the leading example of a security-oriented regulatory effort, aimed at preventing the illicit reading of RFID tags. Other states have pursued different approaches for protecting individuals; for example, Wisconsin has banned the implantation of RFID tags in human beings (AB 290, 2006).

New York and Consumer Protection

In 2006, the New York legislature introduced the Radio Frequency Identification Right to Know Act (RKA), a bill aimed at protecting consumer privacy rights by regulating the increasing use of RFID tags by retailers.[20] Currently, RFID usage in the consumer setting has little restraint, as it is regulated only by non-binding industry guidelines and general privacy laws.[21] The RKA addresses the need to protect consumers from the potential intrusion that RFID technology may have on consumer privacy, such as its potential to track individuals who handle objects with RFID tags and profile consumers without their consent. In response to these potential threats to consumer privacy, along with the increasing use of RFID tags among retailers such as Wal-Mart, Target, and Best Buy, the RKA proposes a comprehensive regulation scheme

[17] *See* 2006 Privacy Legislation Related to Radio Frequency Identification (RFID), http://www.ncsl.org/programs/lis/privacy/rfid06.htm (last updated Sep. 12, 2006).
[18] *See* 2005 Bill Text IL S.B. 2558; 2005 Bill Text MA H.B. 1447; 2006 Bill Text MO S.B. 638; 2005 Bill Text NV A.B. 264; 2005 Bill Text NM H.B. 215; 2005 Bill Text NY A.B. 9504; 2005 Bill Text TN H.B. 300; 2004 Bill Text UT H.B. 251
[19] *See* 2005 Bill Text IL S.B. 2558; 2005 Bill Text MA H.B. 1447; 2005 Bill Text NM H.B. 215; 2005 Bill Text NY A.B. 9504
[20] 2005 Bill Text NY A.B. 9504 (Lexis). The bill was reintroduced in the 2007-2008 legislative session as A.B. 222; A.B. 222 contains the same language as A.B. 9504.
[21] Laura Hildner, "Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level," 41 Harv. C.R.-C.L. L. Rev. 133, 144-145 (2006).

to raise consumer awareness, safeguard against threats to consumer privacy, and create a workable enforcement process by requiring disclosure to consumers of RFID tags, and mandating their deactivation at the point of sale, among other things.

I. Consumer Notice

A. General Notice

Section 2 of the RKA mandates all retailers selling merchandise with RFID tags to post a notice on every cash register informing consumers that: (1) the establishment offers items with RFID tags; (2) state law requires that the RFID tag be removed or disabled before the tagged item leaves the establishment; and (3) the establishment is required to provide customers, on request, with any personal information obtained through the RFID tag while in the establishment.[22]

B. Item-level Notice

Additionally, the RKA requires any item or package with an RFID tag to be labeled with a notice informing the consumer that: (1) the item or package contains or bears an RFID tag, and (2) the RFID tag can transmit unique identification information to an independent reader both before and after purchase of the item. The label must be conspicuous in size and location.[23]

C. Request for Information

The RKA requires the retailer to provide forms for consumers to request all personal information gathered by RFID tags pertaining to that consumer.[24]

II. Deactivation and Removal

Section 3 of the RKA requires the retailer to permanently remove or deactivate the RFID tag at the point of sale, and bear all costs of removal or deactivation. Once removed or deactivated, the retailer cannot reactivate the RFID tag without the express consent of the consumer. Furthermore, the retailer cannot coerce the customer into keeping the RFID tags on their purchased items by stipulating that RFID tag must remain active in order to exchange, return, repair, or service the item.

III. Information Usage and Storage

Section 4 of the RKA prohibits the retailer from linking any of the consumer's personal information with the information gathered by or contained within the RFID tag, and proscribes

[22] 2005 Bill Text NY A.B. 9504 (Lexis).
[23] *Id.*
[24] *Id.*

the disclosure of any such information to non-party affiliates. Furthermore, the retailer may not use information gathered by or contained within the RFID tag to identify a customer.[25]

IV. Enforcement

If the RKA is violated, the New York Attorney General can seek to enjoin the continuance of the violation. Upon finding a violation, the court may issue an injunction without any proof of injury or damage, grant direct restitution, or impose a civil penalty of no more than five hundred dollars [per violation]. Furthermore, each sale, offering for sale, or item or package in violation of the RKA will constitute separate violations.[26]

V. Commentary

The New York RKA largely conforms to the systems proposed by EPCglobal and the "Position Statement on the Use of RFID on Consumer Products." A nonprofit venture with 400 members of retailers and product vendors such as Wal-Mart and Proctor & Gamble, EPCglobal, has established a system of RFID self-regulation.[27] The guidelines include: consumer notice; consumer choice to remove or disable the RFID tag; consumer education; compliance with any applicable law, and publication of policies regarding retention; use and protection of any personally identifiable information associated with the RFID tag.[28]

Issued and endorsed by various consumer privacy and civil liberties organizations, the "Position Statement on the Use of RFID on Consumer Products ("Position Statement") proposes a framework guided by strong principles of fair information practices, which include: transparency (retailers' RFID policies should be public, goods should be conspicuously labeled, no secret databases or tag reading); consumer education; collection limitation; accountability mechanisms; and security safeguards.[29] The Position Statement encourages retailers to avoid: coercing customers into accepting RFID tags in the products they buy; preventing customers from detecting or disabling RFID tags in their possession; tracking customers without informed

---

[25] *Id.*
[26] *Id.*
[27] *See supra* note 21, 146-147; *see also* http://www.epcglobalinc.org/about/ [last visited March 14, 2007].
[28] EPCglobal, *Guidelines on EPC for Consumer Products*, (September 2005), *available at* http://www.epcglobalinc.org/public/ppsc_guide/ [last visited March 14, 2007].
[29] Electronic Frontier Foundation, *RFID Position Statement on the Use of RFID on Consumer Products* (Nov. 14, 2003), *available at* http://www.eff.org/Privacy/Surveillance/RFID/RFID_Position_Statement.pdf [last visited March 9, 2007]

and written consent; using RFIDs to eliminate or reduce anonymity, i.e. linking RFID tags with personal information.[30]

The RKA encourages consumer awareness and education by requiring open and transparent use of RFID technology, conspicuous labeling that identifies the RFID-embedded item and states its purpose, and the ability to request information obtained by the RFID tag. By requiring the disablement of RFID tags at point of sale and prohibiting the coercion of consumers to keep RFID tags on items, the RKA takes the more restrictive Position Statement approach to prevention of consumer tracking than the EPCglobal approach of consumer choice of disablement or removal (an approach that has been adopted by several other states in their consumer RFID legislation).[31] In particular, the RKA would prevent retailers from using RFID tags to ensure that an item returned for exchange, repair, service, or refund, was in fact the item that was purchased. However, retailers could address this limitation with Section 3(C) of the RKA, which allows the retailer to reactivate the tag after point of sale with the express consent of the consumer. Allowing consumers to choose to reactivate the RFID tag not only provides greater consumer protection (as with most opt-in schemes), in comparison to giving them the choice to deactivate the RFID tag – but retailers can further induce consumers to reactivate tags with financial incentives, just as supermarket loyalty cards present a bargaining away of privacy of purchasing patterns in exchange for grocery discounts. The RKA's prohibition against coercing consumers into keeping the RFID tags active would not likely stand in the way of retailers offering discounts or more generous return policies.

Although the RKA requires deactivation at point of sale, it does not address monitoring or surveillance issues associated with the RFID tag prior to sale. Therefore, retailers could use "smart shelf" technology to trigger surveillance when a particular RFID-embedded item is picked up off the shelf in order to assess consumer behavior or control shoplifting. However, with many in-store monitors already installed in retail stores today, smart shelf technology is unlikely to make an impact on consumer in-store privacy . Also, because the information harvested before the point of sale is not tied to the identity of the shopper, the privacy intrusion is minimal.

[30] *Id.*
[31] *See* 2005 Bill Text IL S.B. 2558; 2005 Bill Text MA H.B. 1447

The RKA prevents the retailer from linking RFID information with a consumer's personal information, thus limiting consumer profiling. The limitation on data collection would benefit consumer privacy, but could also hinder retailer marketing tools that use consumer profiles for discounts and promotional offers, reward programs, or customer service programs that make shopping suggestions based on previous or current purchases.

It should further be noted that some of the RKA provisions are somewhat duplicative. For example, Section 4(A) prohibits linking personal information to information gathered by the RFID tag and Section 4(C) prohibits disclosing a consumer's personal information associated with information gathered by the RFID tag. A violation of the first provision is a necessary condition for a violation of the second. By fragmenting the penalties this way, the RKA enforcement scheme can render distinct and comprehensive penalties for violations of the Act. Furthermore, such a scheme establishes an effective accountability mechanism consistent with the Position Statement framework.

The only Position Statement provision that the RKA does not address encourages "security and integrity in transmission, databases, and system access," that is verified by outside third parties and publicly disclosed.[32] The provision would safeguard personal information against interception and theft through RFID technology, and prevent tag reactivation without the consumer's knowledge. The RKA could easily be amended to include such a security safeguard provision, which would inevitably cost the retailer more, but would effectively address a major privacy concern for consumers.

Overall, the RKA addresses the majority of consumer privacy issues: consumer awareness, consumer tracking, disclosure of consumer information, and accountability. Because of the RKA's comprehensive scope and structured enforcement measures, it provides a good model for states to follow when drafting legislation on RFID regulation in the commercial context. However, retailers would be expected to lobby against the passage of the bill, given that it undercuts many of the benefits of RFID technology by greatly reducing the ability of stores to create new databases of consumer purchasing and usage patterns, as well as limiting the use of RFID tags in post-sale control of the returns process.

[32] *RFID Position Statement on the Use of RFID on Consumer Products*, *supra* note 29.

California: Regulating the Security of RFID Technology

In late September 2006, Governor Schwarzenegger vetoed Senate Bill 768, also known as the Identity Information Protection Act of 2006 (IIPA, Simitian).[33] In his veto statement, Governor Schwarzenegger explained that the bill was rejected because of its possible conflict with the federal mandates issued pursuant to the Real ID Act. The IIPA came the closest of any substantive RFID bill to becoming law, and in light of the Real ID Act, should be viewed as an innovative first step at creating a policy framework for regulating RFID technology in the government sector.

I. Bill Summary

a. The IIPA proposed certain security-promoting measures for government-issued identification documents using RFID tags, including:

- Tamper-resistant features
- Mutual authentication process when there may be a transfer of personal information
- Personal information shall be unreadable by third parties through means such as encryption
- Access control protocols for transmission of personal information
- Secondary verification and identification measures to allow the ID holder to opt out of wireless data transmission
- RFID awareness and education for RFID-embedded ID holders
- RFID countermeasures, such as shield devices or switches
- Prohibition on disclosure of or access to any operational system information to unauthorized third parties
- Government accountability measures and criminal penalties

b. The IIPA exempted certain ID holders from these protections, including:

- Those in state prison, county jail, certain juvenile facilities, or under court-ordered electric monitoring at a mental health facility

[33] 2005 Bill Text CA S.B. 768 (Lexis). The bill has been reintroduced for the 2007 legislative session as S.B. 30 and contains the same language as S.B. 768, except for Section 1798.13 of the 2005 bill, which provided for penalties for the unauthorized reading of RFID documents and the parties exempted from said penalties. 2007 Bill Text CA S.B. 30 (Lexis).

- On duty law enforcement officers or emergency response personnel
- Patients in the care of a government-operated or government-owned hospital or nursing facility, with limitations
- Those using RFID-embedded IDs for secured access to a public building or parking area

II. Commentary

The IIPA received support from a wide range of groups, including the Electronic Frontier Foundation, the American Civil Liberties Union (ACLU), the Privacy Rights Clearinghouse, AARP, the California Alliance Against Domestic Violence, and the Gun Owners of California.[34] Proponents viewed the IIPA as a comprehensive policy framework of security safeguards that would allow Californians to maintain some control over their personal information and would prevent identity theft, covert tracking, and stalking.[35]

Opponents of the IIPA also viewed it as a step in the right direction from the original proposal of a three year moratorium on RFID technology, but argued that its significant preemptive security measures were premature.[36] The Security Industry Association ("SIA"), a group of 350-plus manufacturers of physical and electronic security equipment, asserted that the IIPA would severely impede the use and development of RFID technology and could lock in a regulatory scheme that would actually be less safe for tomorrow's rapidly evolving technology.[37] The SIA noted that the IIPA scheme contained a host of pitfalls as a result of incomplete fact-finding and lack of input from law enforcement and other government agencies who would be significantly impacted by the IIPA.[38] The SIA argued that the IIPA was too broad and could result in excessive government liability, as well as restrict beneficial uses of RFID technology, such as the locating of 911 victims by law enforcement officers.[39] Although SIA's concerns and recommendations have merit, it is also important to recognize that early adoption of security

[34] Lee Tien, "California Lawmakers Pass Safeguards for Privacy-Leaking RFID Chips" (Aug 31, 2006), *available at* http://www.eff.org/news/archives/2006_08.php [last visited March 14, 2007].
[35] *Id.*
[36] Doug Farry, "Does California's New Legislation Ignore Advantages of RFID?" (Sept 1, 2006), *available at* http://www.mckennalong.com/news-inthe-1862.html [last visited March 14, 2007].
[37] Richard W. Chace in a letter to Senator Joe Simitian, (Aug 3, 2006), *available at* http://rfidlawblog.mckennalong.com/archives/RFIDWG%20Simitianletter%208%203%20FINALSENT.pdf [last visited March 14, 2007].
[38] Chris Kennedy, "SIA Notches Victory in California RFID Battle" (Oct 4, 2006), *available at* http://www.siaonline.org/news/showPR.cfm?ID=1570 [last visited March 14, 2007].
[39] *Id.*

requirements might be the only way to protect citizens from the tremendous threat that insecure applications of RFID technology may have on their right to privacy.[40]

Furthermore, state legislation such as the IIPA should be adopted in light of the Real ID Act. States can formulate a workable policy framework for the regulation of RFID technology while protecting privacy rights and still meeting the federal standards and objectives. It should also be noted that even if states wait for federal mandates, these regulations may be struck down for unconstitutionally conscripting state legislative and executive power in violation of the 10th Amendment.[41] Accordingly, the regulation of state-issued IDs is a power that should be left to the state legislature and executed by state agencies accordingly. States such as Illinois and Washington have proposed legislation that prohibits "contactless integrated circuit" technology in state-issued identification documents,[42] in defiance of eventual federal mandates that will most likely impose the use of such technology. Additionally, Kansas has proposed a resolution expressly calling on Congress to repeal the Real ID Act, noting the danger RFID technology may have on individual civil liberties.[43]

In conclusion, the IIPA addresses the privacy concerns raised by RFID technology while creating a framework that would achieve the Real ID Act's security objectives. Given the inaction of the federal government on this vital issue, state legislatures will continue to attempt to shape and implement a workable regulation scheme. California's IIPA presents a practical first step in the right direction, and provides a model framework for future legislation.

[40] Many current RFID systems use weak, if any, encryption.
[41] *See* New York v. United States, 505 U.S. 144 (U.S. 1992) and Printz v. United States, 521 U.S. 898 (U.S. 1997).
[42] *See* 2005 IL S.B. 2558 and 2005 WA H.B. 2521
[43] Committee on Federal and State Affairs, *House Resolution No. 6013*, Session of 2006, *available at* http://www.kslegislature.org/bills/2006/2006_6013.pdf [last visited March 14, 2007].