ACLU
AMERICAN CIVIL LIBERTIES UNION
of NORTHERN CALIFORNIA
FOUNDATION

DRAFT PAPER: DO NOT DISTRIBUTE OR CITE WITHOUT PERMISSION OF AUTHOR

Rights "Chipped" Away:

RFID and Identification Documents

Nicole A. Ozer[1]

Introduction

In January 2005, parents from a small town named Sutter, California, an hour North of Sacramento, sent a letter to the offices of the ACLU of Northern California. Their daughters had come home from their public middle school with new identification badges

[1] Nicole A. Ozer is the Technology and Civil Liberties Director at the ACLU of Northern California. The opinions expressed in this article are not necessarily that of the ACLU or the ACLU of Northern California. Special thanks to Valerie Small-Navarro, ACLU Sacramento Legislative Office, Michele Tatro, Lee Tien, Electronic Frontier Foundation, California State Senator Joe Simitian, Rei Onishi, Legislative Aide (former), Office of California State Senator Joe Simitian, David Molnar, Department of Computer Science, University of California- Berkeley, Lenny Goldberg, Lenny Goldberg and Associates, and Beth Givens, Privacy Rights Clearinghouse. Many of the ideas and information in this policy paper have been developed over the course of two years of work with these extraordinary individuals on the Identity Information Protection Act. First introduced in the California State Legislature in February 2005, the bill was the first legislation in the nation to address RFID technology in identification documents.

that appeared to have computer chips embedded inside. The parents had questions and reached out to the ACLU to try to get some answers. These parents had no idea what that letter would mean, how far that letter would go, how it would impact their family, their town, and the national debate over personal privacy in post 9/11 America.[2] ACLU stories often start like that. And like many ACLU stories, this one is far from over. The letter from these parents unleashed a firestorm over the privacy and security implications of a technology called Radio Frequency Identification (RFID). First used during World War II to differentiate between friend and foe aircraft, it emerged in the commercial sector in the 1970s to track products as they moved through the manufacturing sector and then to tag and track cattle and other livestock. Prior to 9/11, it had only been used to identify individuals on a relatively small scale, mostly for building entry and road toll collection systems. But, in the past six years, RFID technology has been increasingly considered for

[2] For more information about Sutter, please see ACLU-NC Press Release, February 7, 2005 *available at:*

Privacy Rights Are At Risk – Parents and Civil Liberties Groups Urge School District to Terminate Use of Tracking Devices, ACLU of Northern California, *at* http://www.aclunc.org/news/press_releases/privacy_rights_are_at_risk_-_parents_and_civil_liberties_groups_urge_school_district_to_terminate_use_of_tracking_devices.shtml (last visited Jan. 8, 2007).

See also ACLU-NC Press Release, February 16, 2005, *available at*:

Victory for Students, Parents and Civil Liberties Groups – Company Announces it will End Tracking Pilot Program, ACLU of Northern California, *at* http://www.aclunc.org/news/press_releases/victory_for_students,_parents_and_civil_liberties_groups_-_company_announces_it_will_end_tracking_pilot_program.shtml (last visited Jan. 8, 2007).

The Sutter story was covered extensively in the local, national, and international press.

Kim Zetter, *School RFID Plan Gets an F*, Wired News, *at* http://www.wired.com/news/privacy/0,1848,66554,00.html; http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/02/10/BAGG0B8I4D1.DTL (last visited Jan. 8, 2007).

use in government- issued identification documents like passports, drivers' licenses, and student badges. This technology, which had been quietly creeping into the lives of Americans, was blasted into the public spotlight by these two unassuming sets of parents who had a few straightforward questions and concerns about the privacy and security impact of RFID technology in their children's school badges- questions and concerns that had not been adequately answered by the school or the company selling the new technology. In the past few years, these questions and concerns have not abated, but come into greater focus as government oversight organizations such as the Government Accountability Office ("GAO") and the Privacy Integrity Committee of the Department of Homeland Security, politicians, researchers, and industry organizations have looked more carefully at risks of RFID and fostered critical debate about whether it is an appropriate technology for use in government-issued identification documents.

The ACLU of Northern California has been a leader in generating public and legislative attention to the privacy, personal safety, and financial security risks associated with the use of RFID technology in government-issued identification documents.[3] This policy paper will discuss RFID technology, its vulnerabilities, and its impact on civil liberties and consumer privacy. It will also discuss the development and current status of RFID legislation that is moving though the California legislature and serving as a model for other state action.

[3] See ACLU of Northern California RFID webpage at http://www.aclunc.org/issues/technology/dont_chip_our_rights_away!.shtml (last visited Jan. 8, 2007).

RFID- What is it?

RFID is a generic term for technologies that use radio waves to automatically identify people or objects from a distance of several inches to hundreds of feet. In the past few years, as major newspapers and radio stations have reported about the privacy and security concerns of RFID, spurred in large part by the Sutter story and the rollout of RFID in passports, the term has moved from obscurity to relative known in the minds of many Americans.[4] Along with increased knowledge has also come increased skepticism about whether RFID technology adequately protects an individual's privacy and security.[5] So much so, that some manufacturers and government agencies have tried to distance themselves from the bad publicity that has been garnered by some RFID

[4] "The number of U.S. consumers who are aware of RFID technology is growing steadily, but so are negative perceptions of the technology—especially among women."

"Since the first survey of the series, conducted in September, distrust over the use of RFID has increased and TV and radio news surpassed the Internet as the most common way people learn about RFID."

See RFID Consumer Buzz report, based on a quantitative survey of more than 7,000 consumers and on focus groups involving 40 of the respondents conducted during December 2004 and January 2005. *Available at*

Mary Catherine O'Connor, *Surveys Reveal Dubious Consumers*, RFID Journal, *at* http://www.rfidjournal.com/article/articleview/1409/1/1/ (last visited Jan. 8, 2007).

[5] "The legislation [Identity Information Protection Act] also tells the general public that RFID is too risky—a growing perception already shaping the overall market for RFID products."

Doug Farry, *Act Now! RFID providers and users can influence public policies that impact the RFID industry*, RFID Journal, *at* http://www.rfidjournal.com/article/articleview/2768/1/128/ (last visited Jan. 8, 2007).

products. A crop of new names for the technology has been developed, with segments of the industry re-branded as "smart cards," "smart chips," and "contactless integrated technology."[6] However, regardless of name, all segments of the RFID market are based on the same core technology. RFID tags are comprised of tiny computer chips with antennas that can be encoded with information, such as someone's name or social security number or in the case of commercial use, the type of product or its origin. These chips, some as small as a grain of rice, are then embedded in documents and objects.[7] When an RFID reader is in the area, the chip transmits its stored information to the reader by sending it a radio signal. The chips do not alert anyone that it is transmitting this information or to what reader this information has been sent. On top of this foundational

[6] Gene J. Koprowski, *Wireless Industry Defends RFID for Passports*, Tech News World, *at* http://www.technewsworld.com/story/42349.html (last visited Jan. 8, 2007).

The Department of State is not calling the passports RFID-enabled; rather, it calls them "contactless smart-cards…DHS avoids the term 'RF' [radio frequency] like the plague…"

RFID Tags and Contactless Smart Card Technology: Comparing and Contrasting Applications and Capabilities, Smart Card Alliance, *at* http://www.smartcardalliance.org/pages/publications-rfid-vs-contactless (last visited Jan. 8, 2007).

"Smart Card Alliance members developed this document to compare and contrast the applications and capabilities of the two technologies. The differences are important to keep in mind as the various forms of RF chip technology become pervasive in the market."

[7] The Hitachi "Mu chip" is .4 mm square -small enough to be embedded in paper.

Electronic Numbering of Products and Documents using the "µ-chip" (or mu-chip) supported by a Networked Database unleashes new Business and Life Style Applications that facilitate innovative Manufacturing, Distribution, Consumption, Tracking and Recycling operations, Hitachi, *at* http://www.hitachi.co.jp/Prod/mu-chip/ (last visited Jan. 8, 2007).

technology lie several permutations of RFID tags- "passive" tags, "active" tags, and "smart" tags.

"Passive" tags are so termed because they have no internal power source and perform no actions until they are awakened by receiving energy waves in the radio signal emitted by a reader. Studies from the United States Department of State have shown that tags envisioned to be read from a few inches can actually be awakened and read at distances of more than 20 feet, with others scientists demonstrating that they can be read at greater than 69 feet.[8] Since these tags have no internal battery, they can be small, easy to embed, quite cheap to produce, and can successfully operate for a long period of time.

"Active" tags have their own battery source. They do not have to wait to be awakened by a reader, but are capable of initiating communication with a reader and continually broadcasting their stored information. They also have a much longer read range of several

[8] *Radio Frequency Identification Technology in the Federal Government*, GAO, *at* http://www.gao.gov/new.items/d05551.pdf (6) (last visited January 8, 2007).

Scientists from Los Angeles-based Flexilis showed at DefCon in 2005 that passive RFID chips can be read at up to 69 feet.

Brian Krebs, Leaving *Las Vegas: So Long DefCon and Blackhat*, Washington Post, *at* http://blog.washingtonpost.com/securityfix/2005/08/leaving_las_vegas_so_long_defc.html (last visited January 8, 2007).

Testing conducted by the U.S. State Department showed that smart cards with passive chips that had an intended read range of only 4 inches could actually be read from a distance six times as far — 24 inches — and could theoretically be read from more than 3 feet away. It has also been reported that readers can "eavesdrop" on legitimate reader-to-card communications from a distance of 30 feet.

hundred feet- some of up to 750 feet depending on battery power. The batteries in these tags normally last several years.[9]

Some tags are called "smart" because they possess the technological capability to include some forms of security protection for transmission of sensitive data. These chips are sophisticated enough to allow the layering of data protection processes, such as cryptography and authentication,[10] on top of the core radio frequency technology actions performed by the chip. However, these tags are only as "smart" as the decision makers who decide what types of protections should be built onto these chips and how effective these protections actually are against privacy and security attacks. [11]

The Very Real Worries of the Sutter Parents and the Public

> "There are more than 200 million of these security devices [RFID] used worldwide with not an instance of a security breach."

[9] *Radio Frequency Identification Technology in the Federal Government*, GAO, *at* http://www.gao.gov/new.items/d05551.pdf (last visited January 8, 2007).

[10] Very generally, cryptography is the procedure to translate data written in plain text into ciphertext, coded text that requires access to a key or password to be able to read the information. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

[11] *See* next section for discussion of some of the vulnerabilities of "smart" tags.

—Roxanne Gould, Senior Vice President, CA Government & Public Affairs, American Electronics Association (AeA)[12]

While industry representatives may claim that RFID technology is secure, the facts over many years tell a very different story. The privacy and security vulnerabilities of RFID-embedded identification documents and products have been shown by government offices, independent researchers, and motivated criminals.

Mass-Distributed Building Entry card System Cracked

In February 2007, IO Active, a small computer security firm based in Seattle, Washington, showed just how easy it was to read and clone the information encoded on the building entry cards used at many public and private buildings across the nation. [13] At the RSA Conference, Chris Paget, IO Active's Director of Research and Development demonstrated how a handheld device the size of a standard cell-phone, costing $20 in parts, could read the personal information encoded on the RFID chips used in HID Global ProxCards. [14] With the push of a button on the same device, the personal

[12] *Orange County Register*, August 7, 2005.

[13] http://www.infoworld.com/video/archives/2007/02/rsa_ioactive.html (video of Chris Paget demonstrating the RFID cloner at the RSA Security Conference).

[14] http://www.infoworld.com/article/07/02/28/HNblackhatrfid_1.html; see also http://blog.washingtonpost.com/securityfix/2007/02/legal_threat_silences_rfid_sec.html?nav=rss_blog; http://www.securityfocus.com/news/11444

Following the RSA Conference, IOActive planned to give a presentation at the Black Hat Computer Security Conference in Washington, D.C. demonstrating the cloner and information on the RFID cards could then be copied and re-transmitted, “spoofing” the existence of an entry card and gaining access to the very buildings or information that the RFID chips were intended to protect from unauthorized access. Paget explained, “[a]s the system stands at the moment, I could walk past someone on the street, maybe stand next to them in an elevator, and I could grab their card id and get into the building.”[15]

British E-passports Cracked

In November 2006, the technology protections on three million British e-passports was cracked by software written in less than 48 hours and an RFID reader bought for about $500.[16] While the British Home Office had adopted the Triple-Data encryption standard (3 DES) to try to prevent conversations between the passport and the reader, researchers found that the “secret key” to open up the secure chip was actually published on the face of the passport – the passport number, date of birth, and expiration date.[17] Once this not

releasing schematics about how it was built. When HID learned of its intended briefing, it contacted IOActive, and demanded that the company refrain from presenting their findings at the Black Hat Convention on the basis that "such presentation will subject you to further liability for infringement of HID's intellectual property."[14] With the help of the ACLU of Northern California, IOActive gave a modified presentation that successfully highlighted the vulnerabilities of insecure RFID technology. See Press Release, ACLU of Northern California, HID Threatens Patent Lawsuit, Silences Important RFID Presentation at National Conference (Feb. 28, 2007) *available at* http://www.aclunc.org/news/press_releases/hid_threatens_patent_lawsuit,_silences_important_rfid_presentation_at_national_conference.shtml.

[15] Paul Roberts, *RSA: Door cards – the enterprise’s weakest link*, INFOWORLD, Feb. 13, 2007, http://www.infoworld.com/video/archives/2007/02/rsa_ioactive.html (video of Chris Paget demonstrating the RFID cloner at the RSA Security Conference).

[16] *Cracked It!,* Guardian Unlimited, *at* http://www.guardian.co.uk/idcards/story/0,,1950226,00.html (last visited Jan. 8, 2007).

[17] 3DES uses 112-bit or 168-bit keys.

so secret key was known, the RFID tags in the passports could be read. Within minutes of being read, the information from the passports could be copied and pictures of the holders appeared on a computer screen. The British government could have included a feature in the new e-passport that likely would have prevented this attack. The specification for the international e-passport developed by the International Civil Aviation Association (ICAO) detailed a feature called active authentication that countries could elect to include as part of its technological protection measures. The British government apparently chose not to do so.[18] According to Adam Laurie, the computer expert that helped crack the e-passport, the protections put in place to protect this sensitive information was the equivalent of "installing a solid steel front door to your house and then putting the key under the mat."[19]

[18] ICAO, a little known body run by the United Nations with a mandate for setting international passport standards, was given the responsibility of formulating the security guidelines for all new international e-passports. http://www.icao.int/ (last visited January 9, 2007).

Active Authentication is detailed in the ICAO PKI Technical Report available at http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf (last visited January 9, 2007).

For more information about the history of the e-passport, please see ACLU White Paper: *How the U.S. Ignored International Concerns and Pushed for Radio Chips in Passports Without Security,* Available at http://www.aclu.org/privacy/spying/15780res20050426.html (last visited January 9, 2007).

For more technical information about security and privacy issues of the e-passport, please see Security and Privacy Issues in E-passports, Ari Juels, David Molnar, and David Wagner *available at* http://eprint.iacr.org/2005/095.pdf (last visited January 9, 2007).

[19] Adam Laurie is a computer expert and technical director of the Bunker Secure Hosting, a Kent-based computer security company.

RFID-embedded Credit Cards Cracked

In October 2006, information being transmitted by tens of millions of new RFID-embedded credit cards was intercepted by researchers at the University of Massachusetts-Amherst.[20] Prior to rolling out these new cards to consumers, companies like American Express and J.P. Morgan Chase claimed that the cards incorporated protections to protect sensitive information.[21] However, researchers found that information such as the cardholder's name and other data was being transmitted by the RFID tag without encryption and in plain text. With $150 of readily-obtainable computer and radio components, the researchers developed a reader the size of a couple of paperback books and skimmed and stored the information from the new RFID-embedded credit card.

California Capitol Entry Cards Cracked

In August 2006, security researcher Jonathan Westhues showed the vulnerability of high security areas that rely on RFID-embedded card entry systems.[22] In the shadow of workers installing the final stages of a $2.5 million dollar investment in concrete barricades, posts, and other security measures to secure the California State Capitol,

[20] John Schwartz, Researchers *See Privacy Pitfalls in No-Swipe Credit Cards*, The New York Times, *at* http://www.nytimes.com/2006/10/23/business/23card.html?ex=1319256000&en=76401b1601fc06e3&ei=5090 (last visited Jan. 8, 2007).

[21] American Express said its cards incorporate "128-bit encryption," and J. P. Morgan Chase has said that its cards, which it calls Blink, use "the highest level of encryption allowed by the U.S. government." *See id.*

[22] *Cloning RFID Tags in Sacramento,* ABC 7 News, *at* http://www.youtube.com/watch?v=4jpRFgDPWVA (last visited Jan. 8, 2007).

Westhues read the RFID-embedded entry cards of two California state legislators. In a matter of seconds, the information from the RFID tag popped up on his laptop screen. He transmitted the information from his laptop and with the high security door believing he was Assemblymember Fran Pavley, he gained access to the California State Capitol.[23]

Dutch e-passport Prototype Cracked

In February 2006, the prototype for the RFID Dutch e-passport was cracked on National television.[24] In less than two hours, the information transmitted between the chip and the reader was intercepted, stored, and then cracked. The crack allowed full access to all the information on the passport, including the digitized fingerprint, photograph, and other encrypted and plain text data. Like the British passport, the ease of cracking the protections was due in part to the fact that the "secret key" was not so secret- it was sequentially issued and constructed from information on the face of the passport, including its expiration date and passport number.[25]

[23] *Capitol building to be ringed with barricades*, Silicon Valley/San Jose Business Journal, *at* http://www.bizjournals.com/sanjose/stories/2002/03/18/daily35.html (last visited Jan. 8, 2007).

In 2002, the Legislature voted to allocate funds for the Capitol building to be ringed with barricades. This work was completed in 2006.

[24] Thomas Ricker, Dutch *RFID e-passport cracked, US next?*, engadget, *at* http://www.engadget.com/2006/02/03/dutch-rfid-e-passport-cracked-us-next/ (last visited Jan. 8, 2007).

[25] The Dutch e-passport, also based on the ICAO standard, also failed to incorporate additional optional technological protections such as active authentication. *See* earlier discussion of British e-passport crack for more information.

VeriChip Human-Implantable RFID Cracked

In February 2006, the VeriChip, an RFID-tag approved by the Federal Drug Administration (FDA) for implantation into humans, was cracked by Jonathan Westhues in less than two hours.[26] While the VeriChip corporate website still claims that its tags are "safe," "secure," and "cannot be counterfeited," Westhues was able to read and clone the chip in the arm of a *Wired News* reporter in mere hours with a reader the size of an MP3 player and an antenna about five inches long.[27] While RFID technology has "ever increasing processing speeds, wider reading ranges, and larger memory capacities,"[28] the VeriChip has not become harder to read and clone. Since first cracking the VeriChip, Westhues has shown that even smaller technology, costing as little as $20, and requiring little skill to assemble, can be used to read and clone the chip.[29] There are currently over 4,000 VeriChip systems installed worldwide for use in the healthcare, security, and

[26] Annalee Newitz, *The RFID Hacking Underground*, WIRED, *at* http://www.wired.com/wired/archive/14.05/rfid_pr.html; (last visited Jan. 8, 2007).

Susan Kuchinskas, *The New Chip-erati*, internetnews.com, *at* http://www.internetnews.com/security/article.php/3582971 (last visited Jan. 8, 2007).

[27] The VeriChip corporate website claims that "unlike conventional forms of identification, the VeriChip™ cannot be…counterfeited. It is safe, secure…" http://www.verichipcorp.com/content/company/rfidtags (last visited Jan. 8, 2007).

[28] *See* http://www.verichipcorp.com/content/company/rfid101 (last visited Jan. 8, 2007).

[29] For information on Jonathan Westhues' work, *see* http://cq.cx/vchdiy.pl (last visited Jan. 8, 2007).

government sectors.[30] Once the VeriChip is read and cloned, the copy could be used for whatever purpose was intended for the initial chip, whether it be identifying a patient or accessing a secured location.

RFID Gas Cards and Car Keys Cracked

In 2005, researchers at Johns Hopkins University cracked the security protecting the RFID devices widely deployed in automatic Exxon Mobil gasoline purchasing passes and in automobile anti-theft devices. [31] Using a home-brewed device costing a few hundred dollars, the researchers successful cracked the encryption code on the Texas Instruments chips in 30 minutes. Once they had the code, they used a laptop and a simple RFID device to fill-up with gas for free. The work at Johns Hopkins also revealed the security vulnerabilities of anti-theft car devices that use similar chips. Passive RFID tags are placed in keys that are authenticated by the steering column- if the RFID is not present, the car is not supposed to start. But, these chips were also easily cracked. This research was a surprise to many car owners, but probably not for many car thieves. Police believe that car thieves often successfully steal expensive cars, such as two of soccer star David Beckham's custom-designed anti-theft BMW's, by using software to spoof the RFID

[30] *See* http://www.verichipcorp.com/company.html (last visited Jan. 8, 2007).

[31] Peter Weiss, *Outsmarting the Electronic Gatekeeper*: Code breakers beat security scheme of car locks, gas pumps, Science News Online, *at* http://www.sciencenews.org/articles/20050205/fob8.asp (last visited Jan. 8, 2007).

system.[32] The security researchers see the ease of cracking these RFID deployments as "a sign that the backers of the RFID industry are being short-sighted by trying to roll out more uses for RFID devices before their security and privacy issues are addressed."[33]

Impact of RFID on Civil Liberties and Consumer Privacy

"RFID technology secures our privacy, prevents theft, and saves lives."

- AeA Website, January 2, 2007 [34]

The truth is that there is widespread evidence and accompanying concern about the impact of RFID technology on privacy, financial security, and personal and public safety. These concerns are not limited to organizations that advocate for civil rights, such as the ACLU of Northern California, but are shared by government organizations such as the Government Accountability Office, by elected representatives, independent researchers who specialize in RFID technology, and even by segments of the technology industry itself.[35]

[32] Robert Vamosi, *Gone in 60 seconds-- the high tech version,* CNET News.Com, *at* http://news.com.com/2100-7349_3-6069287.html (last visited Jan. 8, 2007).

[33] Jack M. Germain, *RFID Technology Faced with Privacy Considerations*, E Commerce Times, *at* http://www.ecommercetimes.com/story/44406.html (last visited Jan. 8, 2007).

[34] RFID: Security, Privacy, and Good Public Policy, AEA, at http://www.aeanet.org/publications/idjj_rfid_grad_overview.asp (last visited January 8, 2007).

[35] Neville Pattinson, director of Technology & Government at Axalto Inc. of Austin, Texas, commented at the June 7, 2006 DHS Data Privacy and Integrity Advisory

Impact on Privacy and Anonymity

Tracking: The use of RFID technology in identification documents threatens to drastically reduce privacy rights because of its potential to be used for anonymous and invisible tracking. Any information that is transmitted remotely from the RFID tag — whether that is a name, social security number, or other random number- permits tracking of the movements and activities of an individual. With tests revealing that RFID tags can actually be read at a distance of many feet, an individual's ID may be read surreptitiously as he or she walks through a doorway or hallway, sits at the airport, stands at a political rally, or visits a doctor's office or a gun show. RFID readers will also continue to get more powerful, with greater read ranges fitting into smaller devices, making them even more portable and easier to conceal. [36]

Profiling: The use of RFID technology in identification documents also lays the groundwork for even more widespread profiling of individuals. Profiling functions to

Committee that "It's inappropriate to use RFID technology for tracking and authenticating identities of people," He further noted, "You can think of RFID as an insecure barcode with an antenna." See

Kim Cameron, *Homeland Security Privacy Office Slams RFID Technology*, Kim Cameron's Identity Weblog, *at* http://www.identityblog.com/?p=451 (last visited Jan. 8, 2007).

[36] Online tutorials exist for counterfeiting RFID cards and RFID readers the size of cell phones can be purchased online for just a few hundred dollars. http://cq.cx/prox.pl for an online tutorial. A quick Internet search for RFID card readers will reveal many readers priced at just a few hundred dollars that attach to your mobile device.

create a picture of a person's private affairs or to attempt to predict future activities by aggregating a person's movements or transactions over a period of time. The deployment of RFID technology in government identification documents and the existence of ubiquitous readers would enable the gathering of immense amounts of data. The aggregation of such data will enable the government, and potentially third parties who are also deploying RFID readers, to have intimate details of private lives, including personal information such as medical predispositions or personal health histories.

RFID-enabled profiling is already being deployed in the commercial sector. For example, amusement parks are already using RFID tags to determine what attractions are most popular.[37] At Legoland in Denmark, the park rents RFID bracelets to parents, marketing them as a tool for parents to find their children if they get lost. But, meanwhile, the parks also collect the data from the RFID tags to determine how families use the park, such as "gaug[ing] consumer interest in new rides, even new Lego building sets." [38] Much more sophisticated systems that use mobile phones are now being deployed. The RFID reader phones are designed to read tags that people come into contact with that are embedded in retail stores or in the products being sold in those stores. When the phone reads the tags, the software running on the phones sends out information such as the stores that people

[37] Legoland RFID Tracks Lost Kids, Collects Data, available at http://www.crmbuyer.com/story/Legoland-RFID-Tracks-Lost-Kids-Collects-Data-37694.html (last visited Jan. 8, 2007); See also http://online.wsj.com/article/SB111401226549812066.html (last visited Jan. 8, 2007).

[38] See http://www.crmbuyer.com/story/Legoland-RFID-Tracks-Lost-Kids-Collects-Data-37694.html;

visited. “Then the system infers people's behaviors and deliver[s] information based on the inference results."[39]

Tracking and Profiling Concerns Expressed by Diverse Groups

Concerns about how RFID technology could be used for inappropriate tracking and profiling were brought to the attention of Congress by the GAO in May 2005 in its report: *Information Security- Radio Frequency Identification Technology in the Federal Government*.[40] The GAO found that “the use of tags and databases raises important security considerations related to the confidentiality, integrity, and availability of the data in the tags, in the databases, and in how this information is being protected. Key privacy concerns include tracking an individual’s movements and profiling an individual’s habits, among others.” [41]

The GAO continued by stating that “[a]mong the key privacy issues are notifying consumers of the use or existence of the technology; tracking an individual's movements; profiling an individual's habits, tastes and predilections; and allowing for secondary uses

[39] *RFID in Japan*, ubiks.net, *at* http://ubiks.net/local/blog/jmt/archives3/005739.html (last visited Jan. 8, 2007).

[40] *Radio Frequency Identification Technology in the Federal Government*, GAO, *at* http://www.gao.gov/new.items/d05551.pdf (last visited January 8, 2007).

[41] *See id.*

of information." [42] The GAO expanded on its concerns with tracking and profiling. It cautioned that:

> the widespread adoption of the technology can contribute to the increased occurrence of these privacy issues…tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated. [43]

Similar concerns about both tracking and profiling were also detailed to the Department of Homeland Security in 2006 by its Data Privacy and Integrity Advisory Committee (Privacy Advisory Committee). [44] In its Final Report released in December 2006, it warned of several concerns with the use of RFID in identification documents. It wrote that RFID-embedded identification documents might enable unauthorized access to information through skimming and eavesdropping, that information transmitted might be reused or leveraged for a second purpose without the knowledge or consent of individuals, and that such RFID-enabled systems had the potential to allow "widespread

[42] *Id.* at 3.

[43] *Id.* at 22.

[44] The Privacy Advisory Committee was created to advise the Secretary of the Department of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues relevant to DHS that affect individual privacy, data integrity and data interoperability and other privacy related issues. See http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm for more information and activities of the Privacy Advisory Committee.

Privacy Office – DHS Data Privacy and Integrity Advisory Committee, Homeland Security, *at* http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm (last visited Jan. 8, 2007).

surveillance of individuals…without their knowledge or consent."[45] In its Draft Report, the Committee found that RFID "appears to offer little benefit when compared to the consequences it brings for privacy and data integrity," and recommended that "RFID be disfavored for identifying and tracking human beings."[46] In its Final Report, released in December, 2006, it set forth a host of criteria for agencies to consider when deciding whether to use RFID technology in identification documents, including whether another type of technology could accomplish the goals with less privacy and security risks.[47]

The Institute of Electrical and Electronics Engineers, a nonprofit group representing more than 220,000 United States electrical, electronics, computer, and software engineers, has also expressed serious worry about the privacy and tracking issues associated with the use of RFID in identification documents.[48] In its Position Paper adopted by the Board of

[45] Report No. 2006-02: *The Use of RFID for Human Identity Verification, DHS*, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf (1-2, 6-7) (last visited Jan. 8, 2007).

[46] *The Use of RFID for Human Identification, DHS*, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf (7) (last visited Jan. 8, 2007).

[47] *Report No. 2006-02: The Use of RFID for Human Identity Verification, DHS*, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf (12) (last visited Jan. 8, 2007).

[48] "This statement was developed by the Committee on Communications and Information Policy of the IEEE-United States of America (IEEE-USA) and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA is an organizational unit of The Institute of Electrical and Electronics Engineers, Inc., created in 1973 to advance the public good and promote the careers and public policy interests of the more than 220,000 electrical, electronics, computer and software engineers who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE or its other organizational units." *Available at* http://www.ieeeusa.org/policy/positions/rfid.html (last visited January 8, 2007).

Directors in 2006, the group stated that “RFID systems present a unique technical and policy challenge because they allow data to be collected inconspicuously, remotely, and by unknown, unauthorized, or unintended entities.” It advised that “the security provisions for data acquired using RFID technology must adequately address the fact that data can be collected at a distance, inconspicuously and even unintentionally.” The IEEE was also very concerned about information being used for secondary purposes unrelated to the original reason for carrying or using the RFID embedded card, without the knowledge of the card holder. “Because data in an RFID network has little human intervention and is acquired immediately during a transaction and can even be acquired following a transaction, the data aggregation and use for purposes other than those intended are possibilities that must also be addressed.” [49]

Industry representatives have also formally expressed worries that some forms of RFID technology significantly threaten privacy. In its letter to the State Department, the Smart Card Alliance, a major “smart” chip industry group, explained that EPC 2 Global tags, a basic form of RFID technology that lacks multilayered additional protections “and was designed to track packages and products is not the appropriate technology to use for securing human identification systems.” [50] The Smart Card Alliance confirmed that

[49] *Developing National Policies on the Deployment of Radio Frequency Identification (RFID) Technology*, IEEE USA, *at* http://www.ieeeusa.org/policy/positions/rfid.html (last visited January 8, 2007).

[50] Comments on the Smart Card Alliance to the Department of State, October 3, 2006 available at http://www.smartcardalliance.org/resources/pdf/Smart_Card_Alliance_Response_Passport_Card_Final.pdf (last visited January 8, 2006).

RFID tags such as this, “release their identifiers…to any compatible reader, with no ability to authorize that the reader is allowed to access the information prior to releasing the data.” [51] The RFID technology being considered by the federal government for use in the passport card “does not support the necessary security safeguards to…prevent the citizen's unique reference number from being tracked when it is outside of its protective sleeve." [52] The Smart Card Alliance concluded by stating that “while these vulnerabilities may not be critical in a supply chain application because the information contained on the tags is not sensitive, they are serious issues for any human identification application.”[53]

The AeA and leading technology companies have also echoed the concerns that core RFID technology does not adequately protect privacy. [54] In a 2006 letter to the State

[51] *RFID tags?,* Smart Card Alliance, *at* http://www.smartcardalliance.org/pages/publications-epc-gen2-faq#6 (last visited Jan. 8, 2007).

[52] The Smart Card Alliance is a membership organization that includes over 150 U.S.-based and international organizations covering the full spectrum of the industry- suppliers, integrators and end user groups. http://www.smartcardalliance.org/ (last visited Jan. 8, 2006).

Proposed Passport Card With RFID Technology Bad News for Privacy and Security, Says Smart Card Alliance, Market Wire, *at* http://www.marketwire.com/mw/release_html_b1?release_id=174725 (last visited Jan. 8, 2007).

[53] *Id.*

[54] January 30, 2006 letter to the State Department and the Department of Homeland Security regarding what type of machine readable technology should be deployed in the new Western Hemisphere Travel Initiative Card. Letter signed by AeA, Anteon International Corporation, Axalto Inc., Gemplus Corporation, Giesecke & Devrient Cardtech, Inc, Infineon Technologies, Oberthur Card Systems of American, Philips Electronics North America, and Texas Instruments, Inc.

Department and Department of Homeland Security regarding what type of machine readable technology should be deployed in the new Western Hemisphere Travel Initiative Card, the trade organization and companies explained that basic RFID that was designed for identifying pallets of goods and allowing rapid inventory tracking is "inappropriate for personal identification applications." Such RFID technology has a very long read range, on the "order of 30 feet or more," and would "perversely maximize the possibility…of an illicit actor 'tracking" a person at very long ranges." [55] The information on the tag could also be "surreptitiously skim[med]." [56] The letter urged the government agencies to reconsider whether to use basic RFID technology because its use "would potentially threaten individual U.S. citizen privacy." [57]

Elected officials are also becoming increasingly alarmed about the implications of RFID technology used in identification documents. Senator Clinton submitted a letter to the State Department expressing her distress that the administration has not fully considered the data security and privacy concerns of a proposed border-crossing identification card that would contain RFID technology.[58] Senator John Sununu (R-NH) and Senator Daniel

RE: Privacy and Security Concerns with the use of EPCglobal UHF Generation 2 technology in the Western Hemisphere Travel Initiative Card Program, aeanet.org, *at* http://www.aeanet.org/governmentaffairs/AeA_Letter_Jan_30_2006.asp (last visited Jan. 8, 2007).

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] Alice Lipowicz, *Clinton: Pass card initiative needs 'rigorous' review,* GCN, *at* http://www.gcn.com/online/vol1_no1/42815-1.html (last visited Jan. 8, 2007).

Akaka (D-Hawaii) have also introduced legislation to address the expressed technological implications of potential widespread use of RFID technology in ID documents like drivers' licenses and the security risks associated with databases that might be built as a result. [59] State representatives around the country have introduced more than 50 bills in 30 states addressing privacy and security implications of RFID technology use by the government or commercial sectors. [60]

Insecure RFID Technology Interferes with Constitutional Rights

Groups from across the sectors are right to express alarm about the use of insecure RFID technology in government identification documents. Its use will have a widespread impact on privacy and free speech rights. Such rights are not aspirational, but are guaranteed by both the United States Constitutions and further augmented by many state constitutions.

Insecure RFID Impacts Privacy Rights

[59] Renee Boucher Ferguson, *Senators Question Use of RFID in E- Passports, National ID Cards,* eWeek.com, *at* http://www.eweek.com/article2/0,1759,2073670,00.asp?kc=EWRSS03119TX1K00 (last visited Jan. 8, 2007).

[60] *RFID State Legislative Activity*, ALEC, *at* http://www.heartland.org/pdf/20144.pdf (last visited Jan. 8, 2007).

Privacy rights are guaranteed by the Fourth Amendment to the United States Constitution and many state constitutional provisions.[61] The Fourth Amendment promises all Americans a zone of control around their bodies and possessions that the government cannot enter without reasonable cause. This zone of control extends far beyond the front door of a home- also protecting places or things that a "person seeks to preserve as private, even in an area accessible to the public."[62] The use of insecure RFID technology in government identification documents interferes with Fourth Amendment rights by facilitating unreasonable searches.

.

Insecure RFID in Government IDs Facilitates Unreasonable Search

The use of insecure RFID in government identification documents facilitates unreasonable search. A search violates the Fourth Amendment if the government violates a subjective expectation of privacy that society recognizes as reasonable.[63] The

[61] Fourth Amendment. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The states of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington have explicit constitutional privacy provisions. For the text of the provisions, see http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm (last visited May 25, 2007). The District of Columbia also includes an explicit privacy provision in its code. See D.C. Code, 2001 Ed. Art. I. §4.

The California privacy provision will be discussed later in more depth.

[62] Katz v. United States, 389 U.S. 347, 351 (1967) (reversing Court's ruling in Olmstead v. United States, 277 U.S. 438 (1928) and holding that wiretap of public telephone violated Fourth Amendment).

[63] *Kyllo v. United States*. 533 U.S. 27, 30 (2001),

inquiry involves two discrete questions: (1) has the individual, by his conduct, exhibited an actual (subjective) expectation of privacy by seeking to preserve something as private; and (2) whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable or justifiable under the circumstances. [64]

Individuals both take actions to preserve the privacy of the personal information on government identification documents and their expectation of privacy over the information on these documents is one that society has long recognized as reasonable. Individuals go to great lengths to preserve the privacy of the personal information on their government identification documents, guarding them safely away from eye view in wallets and purses.[65] This information hidden away cannot be read and recorded by law enforcement with mere observation. Either an individual must be stopped and forced to produce their identification document or technology must be utilized to penetrate an individual's pocket or purse and read this information. Individuals have no reason to think that the information stored on documents away from public view could, or should, be accessed from a distance without their knowledge or consent.

[64] *Katz v. United States*, 389 U.S at 361

[65] The Supreme Court has held in some cases that there is no Fourth Amendment protection over information exposed to the public. *See United States v. Knotts*, 460 U.S. 276, 281 (1983) (tracking car's movements with an electronic beeper did not violate the Fourth Amendment because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). See also *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (aerial photography of chemical company's industrial complex was not a "search" for Fourth Amendment purposes). However, in the circumstances surrounding RFID technology, law enforcement obtains access to identity information that is not exposed to the public and would not otherwise be accessible through naked eye surveillance. Thus, it should be distinguished and found to implicate the Fourth Amendment..

An individual's expectation of privacy over the information on government identification documents is also reasonable and supported both by state law and Supreme Court jurisprudence. Many states have passed statutes which provide the explicit authority to law enforcement to require individuals to display their driver's license for identification purposes.[66] However, initial stops of individuals, which then lead to requests by law enforcement to display identification, must still be based on reasonable suspicion.[67] Thus, the default position is that individuals, absent reasonable suspicion by law enforcement, have control over their personal information and the disclosure of their identity. Other states, such as California, provide even more extensive protection to individuals over the personal information on their identification documents. California law prohibits a business from retaining or using personal information from a driver's license for any other purpose than to satisfy a legal requirement. [68] A liquor merchant can ask to see an individual's license to verify date of birth in order to satisfy the legal requirement to check drinking age, but cannot retain or use any of the other information on a license.

[66] See Va. Code Ann. § 46.2 – 104;
Wash. Rev. Code Ann. §46.20.037(6)
Idaho Code § 49-316

[67] Hiibel v. Sixth Judicial Dist. Court of Nevada, Humboldt County
542 U.S. 177, 184-185 (2004) (interpreting stop and identify statute and finding no Fourth Amendment violation for requiring individual to reveal identity to police officer in course of reasonable stop under Terry v. Ohio, 392 U.S. 1 (1968) (policy may only stop individuals on the public streets and conduct a limited frisk search if they have a particularized, objective, and reasonable basis for believing that criminal activity may be afoot or that a given suspect may be armed and dangerous.").

[68] Cal. Civ. Code § 1798.90.1.

The Supreme Court has long found Fourth Amendment protection for searches that can not be conducted with mere observation, but require physical or technological intrusion. In *Bond v. United States*, the court held that feeling soft luggage was a search, stating that "(p)hysically invasive inspection is simply more intrusive than purely visual inspection."[69] In *Kyllo v. United States*, the Supreme Court found that the use of thermal imaging technology to determine whether illegal activities were occurring inside a home, information that otherwise would require physical intrusion into the home in order to discern, was also a Fourth Amendment search. The Court found that "where…the Government uses a device that is not in general public use, to explore details… that would previously have been unknowable without physical intrusion, the surveillance is a search.").[70] While the home has always been afforded the highest caliber of Fourth Amendment protection, RFID readers, like thermal imagers, use a technology to invade a core area of personal space. The privacy implications of RFID technology in identification documents should be equally considered because it enables the remote and surreptitious reading of information safeguarded in spaces away from public view , creates the potential for identity and location information to be recorded for perpetuity, and facilitates law enforcement actions that are tantamount to an unreasonable stop and enables unreasonable search.

RFID Implicates State Constitutional Protections

[69] 529 U.S. 334, 337 (2000),

[70]Kyllo, 533 U.S. at 40.

In addition to Fourth Amendment concerns, the privacy issues associated with the use of insecure RFID technology in identification documents may also implicate state constitutional protections. For example, the surreptitious monitoring and recording of identity and location that is facilitated by insecure RFID in identification documents is exactly the type of "modern threat" that was the focus of the California Privacy Amendment.[71] . Overwhelmingly approved by the California voters in 1972, the Privacy Initiative was designed specifically to guard against the expansion of government surveillance and data collection. The ballot argument in favor of the proposition cited "the proliferation of government snooping and data collecting that is threatening to destroy our traditional freedoms." In *White v. Davis*, the first California Supreme Court to interpret the privacy amendment, the Court noted that

> …the moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society. The new provision's primary purpose is to afford individuals some measure of protection against this modern threat to personal privacy. [72]

[71] (1975) 13 Cal.3d 757, 774.

[72] (1975) 13 Cal.3d 757, 774.

State constitutional protections like that in California and other states should also be found to safeguard individuals against unreasonable incursions on their privacy due to insecure RFID in identification documents.

Insecure RFID Technology Impacts Rights to Free Speech

The use of insecure RFID technology in identification documents not only impacts our fundamental rights to privacy afforded both by the U.S. Constitution and some state constitutions, but also chills our ability to exercise our rights to free expression by preventing people from remaining anonymous. .Forcing people to carry a government ID with insecure RFID technology is tantamount to requiring people to potentially identify themselves whenever they walk, speak, or meet in public. With insecure RFID in a document that you need to carry on a daily basis, it would be practically impossible to be in a public place without wondering whether the government was monitoring and recording who you were, where you were, and what you were doing. The loss of privacy and anonymity leads to a reduced willingness or opportunity to engage in unfettered speech and an uneasiness about how one's activities might be perceived by others "No matter how innocent one's intentions and actions at any given moment . . . persons would think more carefully before they did things that would become part of the record.[73] Individuals might stop themselves from participating in a political protest or attending a gun show if there was a possibility that their identities and locations were being

[73] Richard Wasserstrom, *Privacy: Some Arguments and Assumptions*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 325-26 (Ferdinand David Schoeman, ed., Cambridge Univ. Press 1984), *cited in* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 243 (2002).

monitored surreptitiously and records maintained about their activities. From political speech to daily activities, once individuals think they could be "observed and recorded, their habits change; they change."[74]

Time and time again, the Supreme Court has prohibited government activities that interfere with the proper exercise of free speech. Laws requiring people to identify themselves when expressing themselves in public are unconstitutional; likewise for requiring identification of a person's association with others or with organizations. Individuals have a right to protest, leaflet, and circulate petitions anonymously,[75] and it is improper to force disclosure of membership lists.[76] Furthermore, courts have ruled that surveillance that targets individuals, intimidates them, or discourages attendance at an organizational activity or membership in an organization is an improper infringement on

[74] Nicholas C. Burbules, *Privacy, Surveillance, and Classroom Communication on the Internet*, ACCESS (1997), *available at* http://faculty.ed.uiuc.edu/burbules/papers/privacy.html (last visited Mar. 23, 2007) *cited in* Slobogin, *supra* note 94 at 244.

[75] Buckley v. Am. Constitution Law Found., 525 U.S. 182 (1999) (striking down Colorado's requirement that petition solicitors to wear an identification badge because it "discourages participation in the petition circulation process by forcing name identification without sufficient cause."); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (striking down an Ohio law prohibiting the distribution of anonymous campaign literature and taking note of "a respected tradition of anonymity in the advocacy of a political cause."); Lamont v. Postmaster General, 381 U.S. 301 (1965) (striking down government measure that required individuals to notify the post office of interest in certain political materials before receiving them in the mail); Talley v. California, 362 U.S. 60 (1960) (striking down a ban on anonymous handbills, noting that "(p)ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws…anonymously."*);*.

[76] NAACP v. Alabama, 357 U.S. 449 (1958) (forbidding the state of Alabama from compelling the NAACP to disclose its membership lists).

free speech and the right of association.[77] As U.S. Supreme Court Justice John Paul Stevens commented in *McIntyre v. Ohio Elections Commission*, in which the court found it unconstitutional to prohibit the distribution of anonymous campaign literature, "(t)he decision in favor of anonymity (is) motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible . . . (it) is an aspect of freedom of speech protected by the First Amendment."[78] The use of insecure RFID in identification documents is inappropriate because of its chilling effect on the exercise of free speech.

Liberty and Human Dignity: In addition to privacy and free speech considerations, RFID technology also represents a real threat to the dignity of individuals in our society and reasonable expectations about the inalienable freedoms of individuals. Human beings should not be tagged and tracked like a product or a piece of cattle. By virtue of being human, we have inalienable rights to liberty, rights that are further codified for Americans in our founding documents and in the United Nations Declaration of Human Rights. [79]

[77] *See also* Presbyterian Church (U.S.A.) v. United States, 870 F.2d 518 (9th Cir. 1989) (church suffered harm of diminished membership as a result of surveillance); Olagues v. Russoniello, 797 F.2d 1511 (9th Cir. 1986) (plaintiffs were targets of surveillance).

[78] *McIntyre*, 514 U.S. at 341-42

[79] Article 13 of the UN Declaration of Human Rights: "Everyone has the right to freedom of movement." *All Human Rights for All*, UN.org, *at* http://www.un.org/Overview/rights.html (last visited Jan. 8, 2007).

As the editors of *Scientific American* wrote in response to learning about the use of RFID tags in student badges in Sutter, California:

> [T]aging junior high school kids becomes a form of indoctrination into an emerging surveillance society that young minds should be learning to question … Widespread adoption of human-tracking devices should never be embraced without serious and prolonged discussion at all levels of society.[80]

Personal Safety: The use of RFID technology also has implications for both personal and public safety. If information on identification documents can be skimmed or eavesdropped, a bad actor may use this information for improper purposes. Many people have important interests in keeping information like their names and addresses private. From vulnerable populations like women, children, and crime victims to people with public positions such as judges and doctors who might not want their personal information accessed without their knowledge. Even if the information on an RFID tag is limited to a unique identifier number, a bad actor may gain more information about an individual by using that unique identifier and then accessing a database, by video camera, or by close-range recognition. Subsequent sightings of that identifier number, or stored records of when that identifier number was sighted at a particular place in time, can then be linked to the individual. It is important for individuals to be able to maintain control

[80] *Human Inventory Control*, Editorial, Scientific American, May 2005. Available at http://www.sciam.com/article.cfm?articleID=00093B44-71DB-1264-B1DB83414B7F0000&sc=I100322 (last visited January 8, 2007).

over the disclosure of their personal information and the use of RFID technology in identification documents threatens this ability.

Cloning and Spoofing: The use of RFID technology in identification documents also presents real concerns for public safety. Basic RFID technology enables the reading of information on the chips. Once someone has read this information, they can use it to access unauthorized areas and resources either by spoofing the card and sending out the radio signal with the information from a laptop, as was done by Jonathan Westhues at the Sacramento Capitol, or cloning the card by taking the information and encoding in on another chip in a new card.

According to industry representatives themselves, basic RFID technology does not have the necessary technological protections to "eliminate the risk of terrorists, criminals, or illegal aliens who have a passing resemblance to legitimate cardholders spoofing or counterfeiting…" cards.[81] Basic RFID technology simply "does not support the necessary security safeguards to allow border officials to verify that the passport card is

[81] "Unlike a solution based on EPC Gen 2 technology, the contactless smart card-based solution supports features that can be used to verify the authenticity of the PASS card and eliminate the risk of terrorists, criminals, or illegal aliens who have a passing resemblance to legitimate cardholders spoofing or counterfeiting PASS cards to enter the United States undetected."

Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID, Smart Card Alliance, *at*: http://www.smartcardalliance.org/alliance_activities/whti.cfm (last visited Jan. 8, 2007).

authentic."[82] According to the Smart Card Alliance, these vulnerabilities lead to the possibility of both eavesdropping on the transmissions and tampering with the actual chip to spoof the transmission or clone the card. The data that is read "could be easily written" to a blank tag, creating a duplicate tag. In its letter to the State Department and DHS, discussed *supra*, the AeA and leading technology companies, also explained how RFID is "highly susceptible to forgery" and how "very easily" this can be done. [83]

> A potential illicit hacker could *very easily* read (again, from a distance) the unique ID contained…and *easily* create a duplicate. The scenario can be imagined where a potential terrorist surreptitiously skims the EPC number information…and then *easily* creates a duplicate card which could then be used…." All the potential terrorist need do is be sure that the holder of the fake card resembles the holder of the true WHTI card in order to pass a cursory visual inspection." [84] (emphasis added).

The technology industry itself has admitted that rather than keeping us safer, using a technology that has been shown to be extremely vulnerable to spoofing and cloning and that allows people to move quickly through security checkpoints with only a cursory visual inspection "would potentially undermine critical homeland security border control programs and effectiveness."[85] Succinctly stated by Marc- Anthony Signorino, Director

[82] *Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID*, Smart Card Alliance, *at* http://www.marketwire.com/mw/release_html_b1?release_id=174725 (last visited Jan. 8, 2007).

[83] *Privacy and Security Concerns with the use of EPCglobal UHF Generation 2 technology in the Western Hemisphere Travel Initiative Card Program,* aea.net, *at* http://www.aeanet.org/governmentaffairs/AeA_Letter_Jan_30_2006.asp (last visited Jan. 8, 2007).

[84] *Id.*

[85] *Id.*

and Counsel for Technology Policy, AeA, “ "'If it doesn’t keep the bad guys out, if it’s easily spoofed, then what good is it?'"[86]

Financial Security: The use of RFID technology in identification documents also threatens to further increase incidents of identity theft and reduce the financial security of Americans. As was shown with the recent crack of RFID credit cards, basic RFID technology transmits information that can be picked up by anyone with a compatible reader. If sensitive personal information, such as a person’s name, social security, or account number, is encoded on an RFID chip and not adequately protected with technological features that can resist compromise, the information can be read and used for improper purposes.

Identity theft is already a significant and growing problem in the United States. In 2005-2006, 8.9 million people were victims of identity theft. With average losses of more than $6,000 dollars, total losses of more than $56 billion dollars, and costing people forty hours of time to make claims and resolve losses, identity theft already impacts a significant segment of the American population.[87] So, what advice did the largest study

[86] Michael Arnone, *Beaming Across the Border*, FCW.com, *at* http://www.fcw.com/article94156-04-24-06-Print (last visited Jan. 8, 2007).

[87] The 2006 Identity Fraud Survey Report - released by the Council of Better Business Bureaus and Javelin Strategy & Research was reported to be the largest study ever on identity theft. It found that between 2005-2006, 8.9 million people were victims of identity theft, at an average rate of 6,383, total of $56.6 billion.

on identity theft provide to consumers to try to stem the rise of identity theft? One of its "top tips" was to "keep all sensitive documents, checkbooks and credit cards securely locked away at home and at work." A second tip was to "not release social security or account numbers in response to e-mail, phone or in-person requests." [88] If personal information is encoded on RFID chips, it will be increasingly difficult to maintain control over this information. RFID industry consultants warn that, "[g]iven that RFID tags are made to broadcast information, the possibility of data theft by easily concealable RFID scanners is very real…[t]hese security problems are simply inherent in the technology."[89] Locking up your cards is not going to help if the information encoded on an RFID tag can be read from distance. The study also said that while ID theft is currently a problem, many people can often determine how their information became vulnerable.[90] This is because a majority of identity theft occurs through lost or stolen wallets, credit cards, and check books and so many people can determine when and how their information was accessed by another individual. [91] Since RFID technology does not alert an individual to

New Research Shows Identity Fraud Growth Is Contained and More Control Than They Think, Better Business Bureau Program*, at* http://www.bbbonline.org/IDtheft/safetyQuiz.asp (last visited January 8, 2007).

[88] *Id.*

[89] *RFID Strategy -- RFID Privacy And Security Issues: A look at the evolving state of tag security, Industry Week,* January 09, 2007 Paul Faber *available at* http://www.industryweek.com/ReadArticle.aspx?ArticleID=13371&SectionID=4 (last visited January 9, 2007)

[90] 47% of victims could identify the source of the data compromise. 36% of victims could identify the person who misused their information. *See id.*

[91] In 63% of fraud cases, the point of compromise was either theft by close associates of the consumer (friends, family, neighbors, etc.), lost or stolen wallets, cards and

when it has been read or by what reader, it will likely become harder to determine when information has become vulnerable and be able to track the source of the identity theft.[92]

***Impact of Surveillance Infrastructure*:** In addition to the privacy and security concerns associated with RFID technology in itself, these concerns are magnified with the interplay of this technology with other surveillance infrastructure that is being developed and deployed by the government and being marketed by the private sector. The current debate over RFID technology takes place within the larger context of an extraordinary expansion in the number and pervasiveness of technologies that pinpoint an individual's identity and location — Global Positioning Systems (GPS), cell-site location tracking, and public video-surveillance technologies — as well as the move to create greater federal identification systems and integrated databases through programs such as Real ID, which will create a National ID and a 50-state interlinked database, the new e-passports, the Western Hemisphere Travel Initiative, and travel databases such as the Automated Tracking System (ATS).[93] By accumulating and aggregating countless individual points of data, these technologies, identification systems, and databases threaten to allow the

checkbooks, breached home computers or stolen mail or trash. Trash as a source of data compromise is now less than 1 percent. *See id.*

[92] *New Research Shows Identity Fraud Growth Is Contained and More Control Than They Think,* Better Business Bureau Program*, at* http://www.bbbonline.org/IDtheft/safetyQuiz.asp (last visited Jan. 8, 2007).

[93] For more information about the Real ID Act, *see* www.realnightmare.org (last visited January 8, 2007). For more information about WHTI, *see* http://www.aclu.org/safefree/general/26681prs20060907.html (last visited May 27, 2007). For more information about ATS, *see* http://www.aclunc.org/news/press_releases/government_secretly_tracks_millions_of_americans.shtml (last visited January 8, 2007).

government — and potentially others — to invade the privacy of individuals at an unprecedented scale.

RFID and Government ID Cards:

Even after all the evidence and reports between 2004 and 2006 about the vulnerabilities of RFID technology, including those by the GAO and the DHS Privacy Integrity Committee, and concerns voiced even by portions of the RFID industry about the privacy and security of the technology, the government is still moving forward with plans to embed RFID technology in a range of government identification documents. Fortunately, the work of privacy and civil rights organizations, technologists, and legislators across the country seems to have stopped, or at least stalled, the plan to use RFID in all drivers' licenses pursuant to the Real ID Act. The Department of Homeland's Security draft regulations for Real ID recommended a 2-D barcode that is scanned optically be selected as the common machine readable technology to replace the magnetic strip that is used on many license today.[94] The draft regulations stated that "[t[he integrated contactless chip was not deemed an appropriate technology for this particular document, as there is not an identifiable need for drivers' licenses and identification cards to be routinely read at a

[94] DEPARTMENT OF HOMELAND SECURITY, MINIMUM STANDARDS FOR DRIVER'S LICENSES AND IDENTIFICATION CARDS ACCEPTABLE BY FEDERAL AGENCIES FOR OFFICIAL PURPOSES 30-1 (Feb. 28, 2007) at 76 *available at* http://www.aclu.org/images/general/asset_upload_file993_28735.pdf

distance." [95] However, RFID passports continue to roll out and other RFID-travel documents are in the pipeline.[96]

RFID Passports

Some Americans have already started to receive new RFID-embedded passports and millions more may be forced to carry them in the years to come.[97] The federal government's original plan was to embed all new passports with an RFID chip that had no protections. All the information currently, printed on the face of United States passports, such as names and passport numbers, would be embedded in the chip with no encryption or other privacy or security protections. [98] The United States Government

[95] *Id.*

[96] Real ID's impact on privacy is still overwhelming. The Real ID Act, passed by Congress as a little-known attachment to the Iraq and Tsunami Appropriations Bill, seeks to create a National ID card and national database of information on practically everyone over the age of 16. All National IDs will have both personal information listed on the face of the card and in a uniform machine-readable format. The machine readable format, even if it is a 2D barcode, will make it very efficient for private businesses to make use of the card's infrastructure to create a parallel, private database, one that will be outside the reach of the Privacy Act and contain much more information than government databases. The ACLU has been firm in its opposition to implementation of the Real ID Act. Legislation is moving through the federal government and in more than 28 states to modify the Real ID Act. More information is available at www.realnightmare.org

[97] RFID-embedded passports started issuing on August 16, 2006.
http://www.state.gov/r/pa/prs/ps/2006/70433.htm
Information about the e-passports is available here.
http://travel.state.gov/passport/eppt/epptnew_2807.html

[98] See ACLU White Paper: *How the U.S. Ignored International Concerns and Pushed for Radio Chips in Passports Without Security*, available at

Global Identity Cards, ACLU, *at*
http://www.aclu.org/privacy/spying/15780res20050426.html (last visited Jan. 8, 2007).

tried to quietly dismiss the concerns of other nations and the ACLU about the privacy and security of the new RFID-embedded passports, claiming that the technology was safe and could only be read from a few centimeters away. It only relented when Barry Steinhart, the Director of the Technology Liberty Project at the National ACLU demonstrated at a large conference, in the presence of a State Department official, just how easily data on an RFID tag could be stolen from a distance.[99] Later, the State Department finally agreed to revise its design to include some privacy and security protections. However, the ACLU and computer security experts have told the State Department that the additional protections are still not adequate.[100] As predicted, e-passports issued by other countries under the same international e-passport standards have already been compromised,

[99] *Naked Data: How the U.S. Ignored International Concerns and Pushed for Radio Chips in Passports Without Security*, ACLU, *at* http://www.aclu.org/pdfs/privacy/nakeddata20041124.pdf (last visited Jan. 8, 2007).

[100] The metal shielding that has been woven into the cover to stop the information from being read (RFID technology does not transmit through metal), only works when the passport is closed. The information can potentially be skimmed when the passport needs to be opened. Experts have also raised questions about the technological soundness of the shielding, even when the passport is closed. Experts have also pointed out that there are no protections that prevent tracking. RFID chips can still be identified by unique patterns in their radio exchanges.. And that's just what's been uncovered in the short time these chips have been available; who knows what will be achieved in the 10-year lifespan of the chips now being used? *See*

Are E Passports More Secure?, Wall Street Journal, *at* http://online.wsj.com/public/article/SB115938787873075826-6AbUpMIaJVCS1i_UBVoGrWP867k_20070929.html (last visited Jan. 8, 2007).

see also Bruce Schneier, *Renew Your Passport Now!,* Schneier on Security*, at* http://www.schneier.com/blog/archives/2006/09/renew_your_pass.html (last visited Jan. 8, 2007).

demonstrating that the passports can be cloned and the personal information of millions of Americans will potentially be compromised if they are forced to continue to use them.

Western Hemisphere Travel Initiative

The federal government is also in the process of creating a new RFID-embedded travel document, the People Access Security Service (PASS) card. [101] This new document is being developed pursuant to the Western Hemisphere Travel Initiative (WHTI). WHTI requires that all people traveling between the United States and Mexico, Canada, and the Caribbean, show a passport or other DHS approved document. [102] Starting in January 2007, all air travelers between these regions were required to show a valid passport and the next phase will require all land border travelers to show a passport or the approved document- a PASS card. The Smart Card Alliance, an RFID industry group, has voiced direct concern over the technology being considered for the PASS card.[103].

RFID and Video Surveillance

The further additional coupling of RFID technology in government identification documents combined with ever growing public surveillance systems presents particularly

[101] http://www.intelligententerprise.com/channels/process/showArticle.jhtml?articleID=192600700

[102] For a thorough discussion of WHTI and the privacy and security impact of the PASS card, please see http://www.cagw.org/site/DocServer/WHTI_Report__2_.pdf?docID=1721

[103] http://www.gcn.com/online/vol1_no1/44338-1.html

grave concerns. Public surveillance cameras are proliferating throughout the United States, funded in part by $800 million dollars in grants from the Department of Homeland Security.[104] Camera systems have been approved and instituted in cities throughout the country without guidelines to guard against abuse and, in most circumstances, with little or no public debate. In just a little over two years, the San Francisco "pilot program" of two video surveillance cameras has grown to over sixty cameras, with plans to seek DHS funding in the coming years.[105] Chicago Mayor Richard M. Daley expects cameras to be "on almost every block" of his city by 2016.[106] In the last five years video surveillance has doubled to become a $9.2 billion industry. J.P. Freeman, a security industry consultant estimates that it will grow to $21 billion in 2010 and predicts that "pretty soon, cameras will be like smoke detectors: They'll be everywhere." [107] The coupling of RFID

[104] Martha T. Moore, *Cities Opening More Video Surveillance Eyes,* USA TODAY, July 18, 2005. The article also mentions an additional $1 billion in money available in state grants.

[105] For more information about public video surveillance, see http://www.aclunc.org/issues/technology/say_no_to_video_surveillance.shtml (last visited January 8, 2007).

[106] *Daley: By 2016, cameras on 'almost every block,* Chicago Sun Times, October 12, 2006. *Available at* http://www.suntimes.com/news/metro/92811,CST-NWS-bside12.article (last visited January 8, 2007).

[107] Publicly-available databases accessed by the government, such as Choicepoint, collect and sell data on individuals that include the following categories: claims history data, motor vehicle records, police records, credit information and modeling services...employment background screenings and drug testing administration services, public record searches, vital record services, credential verification, due diligence information, Uniform Commercial Code searches and filings, DNA identification services, authentication services and people and shareholder locator information searches...print fulfillment, teleservices, database and campaign management services..." See EPIC Choicepoint page *available at* http://www.epic.org/privacy/choicepoint/ for more information.

technology with the proliferation of national identification documents means that it is ever more likely that the government will be able confirm the identity of an individual coming into range of a camera and be able to access a wealth of information about that person- likely anything stored in a computerized database- including such things as your motor vehicle and other identification records, your police records and employment history, DNA and drug testing records, and the travel and buying habits of you and your family.[108]

The Symbol of Sutter

The RFID security vulnerabilities that have come to light, the research and policy papers completed by both government agencies and academic institutions, and admissions by segments of the technology industry itself that basic RFID technology allow for tracking of individuals and cloning of the tags, all point to the fact that it is a risky technology to

Choicepoint, Electronic Privacy Information Center, *at* http://www.epic.org/privacy/choicepoint/. (Last visited January 8, 2007)

[108] Publicly-available databases accessed by the government, such as Choicepoint, collect and sell data on individuals that include the following categories: claims history data, motor vehicle records, police records, credit information and modeling services...employment background screenings and drug testing administration services, public record searches, vital record services, credential verification, due diligence information, Uniform Commercial Code searches and filings, DNA identification services, authentication services and people and shareholder locator information searches...print fulfillment, teleservices, database and campaign management services..." See EPIC Choicepoint page *available at* http://www.epic.org/privacy/choicepoint/ for more information.

Choicepoint, Electronic Privacy Information Center, *at* http://www.epic.org/privacy/choicepoint/. (last visited Jan. 8, 2007).

use in identification documents. The public knows it too. Distrust of RFID technology, particularly by the government, is prevalent and growing.[109] However, RFID technology is still being considered for more and more uses by government and the private sector. Why?

Privacy and Security Issues Not Properly Considered

What happened in Sutter is just a microcosm of what is happening on a national level. From small towns to the highest levels of government, the privacy and security issues related to the use of RFID tags in identification documents is not being properly considered. In Sutter, there was never any discussion of the privacy or security issues before the school district decided to force children as young as five years old to carry RFID embedded tags. On the national level, the GAO found that only one of the 16 federal agencies that responded to its survey in 2005-2006 seemed aware that the use of

[109] According to the RFID consumer Buzz report, a quantitative survey of more than 7,000 consumers and also focus groups, conducted during December 2004 and January 2005, “Concerns over the use of RFID technology are still very prevalent, particularly uses by the government.” Further, “the number of U.S. consumers who are aware of RFID technology is growing steadily, but so are negative perceptions of the technology—especially among women….Since the first survey of the series, conducted in September, distrust over the use of RFID has increased and TV and radio news surpassed the Internet as the most common way people learn about RFID.

Mary Catherine O’Connor, *Surveys Reveal Dubious Consumers*, RFID Journal, *at* http://www.rfidjournal.com/article/articleview/1409/1/1/ (last visited Jan. 8, 2007).

RFID technology may give rise to legal issues such as its impact on privacy and tracking.[110]

Concerns Dismissed as Exaggerated and Paranoid

Industry and the government have also often tried to dismiss the concerns of people like the parents in Sutter and of national organizations such as the ACLU, saying that the worries are "often exaggerated" and "unfounded paranoia."[111] While the Sutter school board did not recognize the grave implications of the RFID program, the parents understood them all too clearly and they were right to worry. The ACLU has also been right to worry about the use of RFID in identification documents and unfortunately, rather than our concerns being "exaggerated," they have often been right on target or perhaps not alarmist enough. For example, as discussed *supra*, the efforts by the United

[110] *Radio Frequency Identification Technology in the Federal Government*, GAO, *at* http://www.gao.gov/new.items/d05551.pdf (7) (last visited January 8, 2007).

[111] AeA says the concerns are "often exaggerated." *See*

RFID: Security, Privacy, and Good Public Policy, AEA, at http://www.aeanet.org/publications/idjj_rfid_grad_overview.asp (last visited Jan. 8, 2007).

The parents in Sutter were said to be engaged in "unfounded paranoia." http://www.metroactive.com/papers/metro/09.07.05/rfid-0536.html

Spy Hunter, Metroactive, *at* http://www.metroactive.com/papers/metro/09.07.05/rfid-0536.html (last visited Jan. 8, 2007).

States Government to quietly dismiss the concerns of other nations and the ACLU about the privacy and security of the new RFID-embedded passports.

RFID is Big Money, Relationships Between Industry and Decisionmakers

The best decisions about privacy and security are also less likely to be made when individuals are influenced by money and personal relationships. RFID in identification documents is big money and is expected to grow even larger. According to IDTechEx, the global market for RFID was $1.94 billion dollars in 2005 and is estimated to reach $7.26 billion by 2008. "Driven by demand and new laws," it will likely reach $24.5 billion by 2015. Access cards for the financial, security and safety markets are they key volume applications for RFID technology. [112] Americans are paying for this RFID technology and fueling the growth in the market not just with tax dollars, but also with their privacy, personal safety, and financial security.

There also appear to be close relationships between the RFID industry and government representatives who are making decisions about new identification documents. Former Secretary of the DHS, Tom Ridge, is now on the board of directors of RFID maker and

[112] *RFID market to reach $7.26Bn in 2008*, IDTechEx, *at* http://www.idtechex.com/products/en/articles/00000169.asp (last visited Jan. 8, 2007).

IDTechEx is a knowledge based company specializing in RFID smart labels, smart packaging and printed electronics. The company gives strictly independent marketing, technical and business advice and services on these subjects

DHS contractor Savi Technology. [113] His work includes telling people that "RFID will make us safer" and that government tests of RFID-embedded passports were a "success" and that the "Feds will safeguard the data gathered." [114] Tommy Thompson, the former Director of Health and Human Services under President Bush, is also now on the board of Applied Digital, the manufacturer of the human implantable RFID tag, VeriChip.[115] While it hardly seems possible, relationships are often even closer in smaller scale deployments. In Sutter, the founders of the company who were deploying RFID in the school, were actually teachers at the high school. They provided the RFID systems for free to the school and gave the school a "donation."[116] The company also promised to give royalties to the school district for future sales of the product to other schools.[117] It also turned out that the attorney for the school district, who provided advice to the school board officials, commented to the press as a representative of the school district, and

[113] *Wireless Industry Defends RFID for Passports, available at* http://www.technewsworld.com/story/42349.html *(last visited January 8, 2007).*

[114] *Id.*

[115] *VeriChip Corporation Appoints Former Secretary of Health & Human Services and Former Governor of Wisconsin Tommy G. Thompson to Its Board of Directors*, ASDX.com, *at* http://www.adsx.com/pressreleases/2005-07-07.html (last visited Jan. 8, 2007).

[116] *School RFID Plan Gets An F* at http://www.wired.com/news/privacy/0,1848,66554,00.html (last visited Jan. 9, 2007)

[117] *Parents Fight Demeaning School Tracking Technology*, News Standard *at* http://newstandardnews.net/content/index.cfm/items/1473 (last visited Jan. 9, 2007)

answered the questions of concerned parents at school board meetings, was also a lobbyist for the RFID company. [118]

It is because the privacy and security issues are overlooked, the concerns that are brought to light are often dismissed, and money and relationships often make good decisions about privacy and security harder to make, that the privacy and security issues of RFID in identification documents should not be "worked out" on a case-by-case basis. If so, they are often "worked out" to the detriment of the privacy, personal safety, and financial security of individuals.

Problems in Need of Solutions:

Legislators are starting to heed the necessity to take action to protect the privacy, personal safety, and financial security of their citizens by introducing RFID bills. In the last several years, over 50 RFID bills have been introduced in over 30 states. [119] One of the most highly publicized bills and one that has been a model for the actions of many other states, is the Identity Information Protection Act. Originally introduced in the 2005-2006 legislative session by California State Senator Joe Simitian (D-Palo Alto) and

[118] It is not clear whether the attorney for the school district, Paul Boylan, was a lobbyist for the Sutter RFID company, InCom, at the time of the initial school board decision and meetings or became a lobbyist for the company several months later. But, during the time he was in Sacramento, lobbying for InCom and against the Identity Information Protection Act, he was still the attorney for the school district.

[119] *RFID State Legislative Activity*, ALEC, *at* http://www.heartland.org/pdf/20144.pdf (last visited Jan. 8, 2007).

recently re-introduced, it creates a comprehensive plan to ensure that there are adequate protections in place for the use of RFID tags in government issued ID documents in California. [120]

Identity Information Protection Act

The Identity Information Protection Act protects all state-issued documents, such as drivers' licenses, government health and other benefit cards, with adequate levels of security to ensure that people are able to decide who and when others can access their information. It also requires that all people are given notice about the technology and the location of the readers.. The bill is a straightforward example of the type of solution discussed by security professionals like those from RSA who have urged that "what is needed…is the adoption of basic controls so no one's privacy is breached," and the IEEE, whose policy statements said that legislation "must" provide "appropriate layered levels of protection and security…as standard policy," and "clear notices regarding what data are collected and how it will be used." [121] The legislation also incorporates the "Best

[120] See www.aclunc.org for full text of the legislation and more information.

[121] Peter Weiss, *Outsmarting the Electronic Gatekeeper*: Code breakers beat security scheme of car locks, gas pumps, Science News Online, *at* http://www.sciencenews.org/articles/20050205/fob8.asp (last visited Jan. 8, 2007).

IEEE USA Position Statement: *Developing National Policies on the Deployment of Radio Frequency Identification (RFID) Technology, February 2006, available at* at http://www.ieeeusa.org/policy/positions/rfid.html (last visited January 8, 2007), Practices" included in the DHS Privacy Integrity Committee Final Report to provide notice, secure readers and data, and avoid secondary uses. [122]

The Identity Information Protection Act was cutting-edge, being the first bill in the nation to address RFID technology in identification documents. However, in essence, it is rather conservative. It is designed simply to ensure that Californians maintain the same level of control that they currently have over the personal information on identification documents like their driver's license. As discussed supra, both California Constitutional and statutory law guarantees privacy and control over such information. Article 1, Section 1 of the California Constitution provides for an inalienable right to privacy[123] and the California Civil Code prohibits a business from retaining or using personal information from a license for any other purpose than to satisfy a legal requirement.[124] California law also prohibits displaying a Social Security number on a license or other identity document [125] [126] and embedding it on a machine-readable magnetic strip.[127]

[122] Report No. 2006-02: *The Use of RFID for Human Identity Verification, DHS*, *at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf (11) (last visited Jan. 8, 2007).

[123] For example, California's state Constitution grants its residents an inherent right to privacy. Cal.Const. Art. 1, § 1. ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

[124] Cal. Civ. Code § 1798.90.1.

[125] Cal. Vehicle Code § 12801(a)

Provisions of the Legislation

The Identity Information Protection Act seeks to help Californians maintain their present level of control, privacy, safety, and security creating basic standards for all government issued identification documents containing RFID tags.[128] Just like a lock on a door to keep things from being stolen, the legislation seeks to put sensible locks on the RFID tags used in identification documents to ensure that personal information is kept safe. The Act creates layered protections for all government issued identification documents.

All Government Documents

The first layer provides that every state-issued ID document must meet three basic standards: (1) tamper resistant features in order to prevent duplication, forgery, or cloning of the ID; (2) authentication process to try to ensure that the identification document was legitimately issued by the issuing entity, is not cloned, and is authorized to be read;[129] and

[126] Cal. Vehicle Code § 1798.85(g).

[127] Cal. Vehicle Code § 12801.

[128] For more information about the Identity Information Protection Act, including the full text of the legislation, please see

Don't Chip Our Rights Away, ACLU of Northern California, *at* http://www.aclunc.org/issues/technology/dont_chip_our_rights_away!.shtml (last visited Jan. 8, 2007).;

see also http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_30&sess=CUR&house=B&author=simitian (last visited Jan. 8, 2007).

[129] See 1798.135 (b) "Authentication" means the process of applying a machine-readable process to data or identification documents, or

(3) notice to all individuals issued an RFID-embedded government ID document about RFID technology, the privacy and security implications, and how they can protect their information. [130]

Multiple Uses, Public Schools, Transport, Public Benefit

Additional layers of protections are built into the legislation when the RFID tag is embedded in identification documents that are used for multiple purposes, for public schools and public transportation, or that confer a public benefit.[131] These types of cards must implement the three basic standards plus one or more of the following protections: (1) a secondary verification and identification procedure that does not use radio waves, (2) a security protection such as mutual authentication; (3) a security protection such as encryption;[132] (4) a security protection such as an access control protocol that enables the holder to exercise direct control over any transmission of the data using radio

both, so as to accomplish either of the following:
(1) Establish that the data and the identification document containing the data were issued by the responsible issuing state or local governmental body.
(2) Ensure that a reader, as defined in subdivision (p), is permitted under California law to access that data or identification document.

[130] See 1798.10(9).

[131] See 1798.10 (7) and (8).

[132] (i) "Encryption" means the protection of data in electronic form in storage or while being transmitted using an encryption algorithm implemented within a cryptographic module that has been adopted or approved by the National Institute of Standards and Technology, the Institute of Electrical and Electronics Engineers, Inc., the Internet Engineering Task Force, the International Organization for Standardization, the Organization for the Advancement of Structured

waves. [133] The additional protections are necessary because such cards are either used by young people or are likely to be needed to be carried on a daily basis because of more constant use.

Encoded with Personal Information

The third, and highest layers of protection, are for identification documents with RFID tags that are encoded with personal information, such as a name, address, or social security number.[134] These RFID-embedded documents must implement the basic standards plus the following five security protections: (1) the ID implements robust encryption to protect against the unauthorized reading of transmitted information; (2) the

Information Standards, or any other similar standards setting body, rendering that data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of that data. That encryption shall include appropriate management and safeguards of those keys to protect the integrity of the encryption.

[133] 1998.10(5) This requirement may be satisfied by the implementation of one or more means including, but not limited to, the following:
(A) An access control protocol requiring the machine-readable or other nonradio frequency reading of information from the identification document prior to each transmission of data using radio waves, without which the identification document will not transmit data using radio waves.
(B) A data-carrying device, such as an integrated circuit or computer chip, that is normally not remotely readable, accessible, or otherwise operational under any circumstances, and only remotely readable, accessible, or operational while being temporarily switched on or otherwise intentionally activated by a person in physical possession of the identification document. The device shall only be remotely readable while the person intentionally enables the identification document to be read.
(C) Another access control protocol that enables the holder to exercise direct control over any transmission of the data using radio waves, not including a detachable shield device or bag.

[134] 1798.10 (3)-(5)

ID implements mutual authentication to ensure as best as possible that only those who are supposed to have access to the data stored on the ID can read it;[135] (3) the ID implements an additional security feature to ensure that the ID cannot be read unless the ID's holder specifically authorizes that reading; (4) the ID's holder is notified of several pieces of information, including (a) that the ID can communicate information using radio waves; (b) that the use of shield devices can help mitigate the privacy and security risks; (c) the location of readers intended to be used to read the ID; and (d) the information that is being collected or stored regarding the individual in a database.

Individually, each of the layered protections are not likely adequate to protect personal information. The RFID industry has admitted that shields are not a realistic solution to the privacy and security concerns and the GAO has found only that "encryption and authentication can help agencies achieve a greater security posture." [136] However, in

[135] (m) Mutual authentication" means a process by which identification documents and authorized readers securely challenge each other to verify authenticity and authorization of both readers and documents before any data is exchanged, except such data as is necessary to carry out mutual authentication. Mutual authentication accomplishes both of the following:
(1) Authorized readers, as defined in subdivision (c), can accurately assess whether the identification document and data stored are issued by the responsible issuing state or local governmental body to an authorized holder.
(2) Authorized identification documents can accurately assess whether a reader accessing them is authorized to read the documents, and authorized to then access data stored on the documents.

[136] *Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID,* Smart Card Alliance, *at*: http://www.smartcardalliance.org/alliance_activities/whti.cfm (last visited Jan. 8, 2007).

> "The requirement for a protective sleeve is also an issue. As drivers are speeding away from the border, they may not always remember to replace the PASS card

concert, these protections may be able to help maintain privacy, personal safety and financial security.

The Real Costs and Benefits

While the costs of unprotected RFID tags to the privacy, personal safety, and financial security of individuals is astronomical, the costs to implement layered protections such as those in the Identity Information Protection Act are negligible. According to HID Corporation, one of the major vendors of RFID technology in the United States, the cost differential between largely unprotected RFID technology and a "smart card" system that can implement protections such as encryption and authentication is very little. It recently touted that "until now, proximity technology held an important cost advantage over smart cards; but that has changed. Anyone with a budget to put in a standard proximity-based access control system can afford to put in a smart card system instead."[137]

Support Across the Aisles and Up and Down the State

> immediately in its protective sleeve. A cardholder may drive for miles within range of any reader capable of picking up and tracking the information on the card. Some individuals will undoubtedly lose the sleeve."

Radio Frequency Identification Technology in the Federal Government, GAO, *at* http://www.gao.gov/new.items/d05551.pdf (3) (last visited January 8, 2007).

[137] *Smart Cards for Access Control Advantages and Technology Choices,* HID, *at* http://www.hidcorp.com/pdfs/HID_wp_smartcardAC.pdf (last visited Jan. 8, 2007).

The Identity Information Protection Act received widespread support from a broad spectrum of civil rights groups, women's groups, domestic violence prevention groups, business organizations, and conservative organizations from the ACLU to the AARP to La Raza to the Gun Owners of California and the Eagle Forum of California.[138] The legislation also received editorial support from conservative and liberal newspapers up and down the state of California. From the *Orange County Register* that wrote that the bill was "a completely reasonable approach to the issue, one that would make necessary distinctions between beneficial private uses of new technology and mandatory government uses."[139] To the *Los Angeles Times* that wrote that "Simitian is on the right track. Neither government no private industry has given the public much reason to trust their ability to safeguard sensitive personal information."[140] The *Long Beach Press-Telegram* told its readers that "RFID chips are an important innovation. Just as important, [The Identity Information Protection Act] will provide some needed safeguards." [141] While, the *San Francisco Chronicle* wrote that [The Identity Information Protection Act] represents a restrained, reasoned approach to regulating a technology

[138] These groups include the AARP, The California National Organization for Women, California Alliance Against Domestic Violence, California State Parent Teacher Association (PTA), Consumer Federation of California, Privacy Rights Clearinghouse, National Council of La Raza, Asian Americans for Civil Rights and Equality, Eagle Forum of California, Gun Owners of California, the Republican Liberty Caucus, and many more

[139] Editorial, *Orange County Register*, (Aug. 21, 2005)

[140] Editorial, *Los Angeles Times* (Aug. 23, 2005)

[141] Editorial, *Long Beach Press-Telegram* (Aug. 11, 2005)

with potential for abuse.[142] While the AeA had started the 2005 legislative session saying that security breaches were not a worry and opposing the bill, lengthy discussions resulted in both AeA and the Information Technology Association of America (ITAA)[143] reaching a neutral position on the legislation.[144] On the heels of both the facts about vulnerabilities and widespread support from all sides of the aisle and up and down the state, the California Assembly and Senate overwhelmingly passed the Identity Information Protection Act. [145]

Legislators Thinking Ahead, Governor Short-Sighted

With the strong bipartisan passage, California legislators were again on the forefront of crafting important legislation that properly balances the potential benefits of emerging technology while safeguarding privacy and security. However, Governor Schwarzenegger vetoed the legislation in the final hours of the session, eliminating the

[142] Editorial, *San Francisco Chronicle* (Aug. 25, 2005)

[143] ITAA is the nation's largest information technology trade association, representing over 1100 member companies and affiliates. http://www.itaa.org/

[144] The bill's author and sponsors, including the ACLUs of California, EFF, and Privacy Rights Clearinghouse, engaged in hundreds of hours of negotiations over nine months with representatives from AeA and ITAA and member companies, including Cisco, Philips, Infineon, Symbol, HID, and others.

[145] Identity Information Protection Act of 2005 passed the Senate with a strong bipartisan vote of 30-7 and passed out of the Assembly with a strong bi-partisan vote of 49-26 on August 21, 2006. For more information about the Identity Information Protection Act of 2005, including a full legislative history, please visit http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_768&sess=PREV&house=B&author=simitian (last visited Jan. 8, 2007).

opportunity to take a proactive stance in protecting the privacy and security of Californians. In his veto statement, he said that he was instead leaving it up to the federal government to set the technological standards to protect privacy and security in identification documents- the same government that has continually failed to include proper protections on RFID tags.[146] Following the Governor's very short-sighted veto, the Identity Information Protection Act was reintroduced in December 2006, passed the California State Senate with a vote of 33-3 in May 2007, and is continuing to move through the California legislature.[147]

Two Years After Sutter

More than two years after the Sutter story launched a national debate about the use of RFID in identification documents, the concerns remain and the facts are clearer as stories of RFID breaches stack higher and higher, more research has been done, and more reports have been written. Further, government, industry, and public interest groups increasingly agree that without protections, the information encoded on RFID tags is not secure. The bills have been written, the protections are available and cost very little to incorporate. Yet, insecure RFID technology is still being considered for identification

[146] http://www.leginfo.ca.gov/pub/05-06/bill/sen/sb_0751-0800/sb_768_vt_20060930.html. (last visited Jan. 8, 2007).

The Identity Information Protection Act "may impose requirements in California that would contradict the federal mandates soon to be issued."

[147] The legislation was again passed by the California Senate on May 24, 2007, with even stronger bipartisan support. With a vote of 33-2, the legislators sent an emphatic message to Governor Schwarzenegger that the privacy and security of Californians should be protected and the RFID bill should be signed into law. .

documents and there is still not a single RFID law on the books- nothing to protect the privacy, personal safety and financial security of individuals. Now is the time to do something, not wait until there is a privacy and security crisis.

Passing legislation to ensure that there are adequate privacy and security protections are in place on the use of RFID in identification documents does not "ban the technology" or "stifle the technology" or "hinder development" just like passing regulations to put seatbelts in automobiles has not banned, stifled, or hindered that technology.[148] Some form of basic standards to protect individuals is necessary when a technology exists that can lead to significant harm to a great number of people. The industry may not want legislation because "it tells the general public that RFID is too risky." [149] But, individuals

[148] *Editorial: RFID Legislation – Protection or Pause Button?,* AIM Global, *at* http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=433&zoneid=24 (last visited Jan. 8, 2007).

Legislation based on fear hurts progress, All Business, *at* http://www.allbusiness.com/government/advocacy-consumer-protection/484638-1.html. (last visited Jan. 8, 2007).

See RFID: Security, Privacy, and Good Public Policy, AEA, at http://www.aeanet.org/publications/idjj_rfid_grad_overview.asp (last visited January 8, 2007).

[149] Act Now! , RFID providers and users can influence public policies that impact the RFID industry. Doug Farry. Writing about the Identity Information Protect Act, Doug Farry, the *managing director with the government affairs practice of McKenna Long & Aldridge, who lobbied against SB 768, wrote that* The legislation also tells the general public that RFID is too risky—a growing perception already shaping the overall market for RFID products.See

Doug Farry, *Act Now! RFID providers and users can influence public policies that impact the RFID industry*, RFID Journal, *at* http://www.rfidjournal.com/article/articleview/2768/1/128/ (last visited Jan. 8, 2007).

should know the risks and the government should help protect them from these risks. In the case of automobiles, law both mandates protections such as seatbelts and airbags in order to reduce the chance that people get hurt and provides a punishment for bad actors that engage in reckless driving. Likewise, RFID bills are necessary to create basic privacy and safety standards to try to reduce the chance that people's private information will be misused and provide some punishment for bad actors that can be caught.[150] Just like we do not leave auto safety up to the car manufacturers, but instead mandate basic safety standards, the privacy and security of individuals must not be left up to the RFID industry. There need to be basic standards for RFID tags in identification documents. Legislation such as the Identity Information Protection Act is an important step in the right direction.

Basic Standards May Not Be Enough

As important as it is for basic standards to be passed and as hard as many legislators and organizations have worked to pass such laws, they are still just steps. If RFID technology is deployed in mass identification documents, it will be very hard to make these tags safe. Countermeasures are difficult due to security failures, abuse of power, key management difficulties, and the unknown reliability of technological protections.

Security Failures: The ultimate success of using countermeasures to mitigate the threats particularly associated with the use of RFID depends on maintaining the security of the

[150] It is particularly difficult to catch bad actors in the RFID context since RFID tags do not alert an individual that their information has been read or by what reader.

systems. In a mass contactless ID system involving millions of IDs, thousands of authorized persons and readers would need to know the name and personal information that goes with the unique identifier number. Thousands would also need to access the central database where that information was stored; they would need to know how to decrypt the information and so they would need the encryption key; and they would need the authentication key to authenticate the presenter of any ID. With so many secrets known to potentially thousands of people, there would be good reason to doubt whether these secrets could be kept for long. The government has also not had a good history of database security. Countless cases from the last few years of security breaches at such places as Department of Motor Vehicles, Veteran's Affairs, and universities cast serious doubt on whether the government can properly safeguard personal information.[151]

Abuse of Power: Effective countermeasures would also require that all levels of government refrain from abusing a tool that enables them to collect unprecedented quantities of information on people without their knowledge. Since 9/11, there has also been widespread abuse of surveillance powers and disregard of essential privacy laws. From the revelations that the federal government has been engaged in warrantless wiretapping, accessing the private call records of millions of innocent Americans, utilizing secret airline travel tracking systems, and attempting to authorize itself to open postal mail without a warrant, the list goes on and on. Now is not a good time to consider giving the government access to another surreptitious surveillance tool and just hope that it will not be abused.

[151] *A Chronology of Data Breaches*, Privacy Rights Clearinghouses, *at* http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Jan. 8, 2007).

Reliability of Countermeasures: Addressing the security and privacy risks associated with RFID technology in government IDs also uniquely depends on measures such as unique identifier numbers, encryption, and mutual authentication since the core technology is actually developed to transmit information to anyone with a compatible reader without the knowledge or consent of the tag owner. The more layers of technology that are implemented, however, the more complicated the security architecture becomes and more failure opportunities are created. Further, many of these security countermeasures, such as encryption, mutual authentication, basic access control, and shield devices have never been deployed together in a mass contactless ID system. Their effectiveness has not withstood the tests of the real-world. Additionally, deployment of RFID technology in mass distributed identification documents will create an even greater incentive to develop new ways to crack the technology and gain access to identification information. Where there is a strong enough incentive to crack a technology, it will be cracked. As we have seen with smaller-scale RFID breaches in recent years, it is likely that some method for circumventing these protections can and will be devised.

Difficulty of Punishing Wrongdoers: The structure of RFID technology also makes it difficult to catch bad actors if countermeasures should fail. Since RFID technology does not alert you that the information has been read, it will be difficult to ascertain whether the countermeasures have been breached or whether the technology is being misused.

Next Steps

There are many concerns with basic RFID technology and also with the ability of countermeasures to address these risks. In the meantime, other identification technologies — which do not pose the same privacy and security threats — appear to be just as effective as RFID technology in many situations. For example, contact-required smart cards, optical scan cards, the newest generation of magnetic strip cards, and 2-D barcodes can all serve as alternatives to increase efficiency. Since these other forms of machine readable technology do not transmit information unless an individual swipes or displays a card for optical reading, many of the privacy and tracking issues are greatly diminished. By not transmitting the information via radio waves that can be picked up for spoofing and cloning, these other options are also more secure. Optical scan cards, in particular, which the U.S. government uses successfully at the Mexican border, offer unparalleled data security, card durability, and memory storage, without the same privacy and security risks associated with RFID technology. Such technologies, which provide many of the benefits of RFID technology without the same privacy and security risks, are better options for government identification documents.

Given the readily available alternatives to RFID technology and the serious threat that it poses to the privacy, personal safety, and financial security of Americans, the bottom line is that RFID technology simply should not be used in government identification documents. If there is any use of RFID in identification documents, the protections delineated in the Identity Information Protection Act must be followed at a bare minimum, with frequent tests to ensure that they are actually keeping private information safe and secure.