SB

293

ALASKA STATE LEGISLATURE

Session
State Capitol Building, Room 125
Juneau, Alaska 99801-1182
Phone (907) 465-2995
Fax (907) 465-6592

Interim
716 West Fourth Avenue, Suite 430
Anchorage, Alaska 99501
Phone (907) 269-0250
Fax (907) 269-0249

Chair
Senate State Affairs
Administrative Regulation Review

Member
Senate Judiciary Committee
Senate Resources Committee

SENATOR LESIL MCGUIRE

MEMORANDUM

To: Senator Hollis French
Chair, Senate Judiciary Committee

From: Senator Lesil McGuire

Date: March 13, 2008

Re: Request for hearing, SB 293 – *Electronic Communication Devices*

I respectfully request that SB 293 – *Electronic Communication Devices* be scheduled for a hearing **pending referral** at your earliest convenience. Attached you will find the most current version of the bill, the sponsor statement, and backup information.

If you have any questions or concerns please feel free to contact me personally, or my staff, Trevor Fulton at x3579. Thank you for your time and consideration.

ALASKA STATE LEGISLATURE

Session
State Capitol Building, Room 125
Juneau, Alaska 99801-1182
Phone (907) 465-2995
Fax (907) 465-6592

Interim
716 West Fourth Avenue, Suite 430
Anchorage, Alaska 99501
Phone (907) 269-0250
Fax (907) 269-0249

Chair
Senate State Affairs
Administrative Regulation Review

Member
Senate Judiciary Committee
Senate Resources Committee

SENATOR LESIL MCGUIRE

SPONSOR STATEMENT

SB 293 – Electronic Communication Devices

Radio Frequency Identification (RFID) is a tagging and tracking technology that uses tiny electronic devices equipped with antennae that can transmit identifying information to a remote reader. This innovative technology has numerous applications, many of which are of benefit to government, businesses, and consumers – some that are not.

As with many new technologies that involve access to private information, there is potential for misuse and abuse with RFID devices. SB 293 minimizes this potential by closely regulating the use of RFID devices in the State of Alaska.

SB 293 regulates the use of RFID devices in Alaska by:

- requiring labeling on all RFID devices
- requiring that business using RFID devices obtain consumer consent
- establishing security standards for storage and access of information gathered via RFID
- prohibiting scanning or remote reading of an RFID without consent
- outlining "form of consent" requirements
- establishing enforcement measures for the misuse of RFID devices

By establishing RFID regulations where none exist, SB 293 aims to safeguard consumer privacy and stay ahead of those who would misuse this emerging technology.

SUMMARY OF CHANGES

SB 293 – Electronic Communication Devices

After hearing Senate Labor & Commerce Committee member comments and public testimony and following discussions with the bill drafter, the Attorney General's office, the Electronic Privacy Information Center, and Dr. Oliver Hedgepeth, Professor of Logistics at University of Alaska Anchorage, the sponsor decided to incorporate the following changes into a draft committee substitute for SB 293:

1. CS Page 1, Line 1
Change
After "information" insert "and making certain violations related to electronic communication devices unfair trade practices."
Explanation
Conforms with the addition of Section 2, which adds violation of this act to the list of Unfair Trade Practices already in statute.

2. CS Page 1, Line 7
Change
Delete "active."
Explanation
"Active" is an industry specific term used to differentiate between two types of devices:

(1) an "active" RFID tag that has a small battery or other source of power and doesn't require power form the reader to send a signal

(2) a "passive" RFID tags those that doesn't have its own power source and are powered by radio signals transmitted from the reader.

We removed "active" even though it was being used in the traditional sense (meaning "turned on" or "functioning") in order to avoid confusion with the industry specific term.

3. CS Page 1, Line 10; Page 2, Lines 13 and 15
Change
Replace "universally acceptable symbol" with "industry recognized symbol."
Explanation
There is no "universally accepted symbol" for RFID. Requiring one would mean that a global industry would have to agree upon a standard label solely for products distributed in the state of Alaska. Allowing for "industry recognized symbols" also accommodates those companies who have already willingly labeled RFID products.

4. CS Page 2, Lines 26-31
Change
Delete (a) and replace with (b)
Insert new (b)
Explanation
Original (a) required consumers to pay costs associated with the deactivation of an RFID. We decided this would place an unnecessary burden on the consumer.
New (b) adds that a provider must delete any personal information on a reactivated RFID. With such a wide variety of RFID devices on the market, it would seem that reuse would be possible if not likely. We did not want RFID devices being reactivated and sent back out into the market unless they were purged of all personal information.

5. CS Page 3, Line 1
Change
Replace "Coerce" and "coercion" with "require" and "requirement"
Explanation
Semantic change. Coercion is a stronger term and more open to interpretation, which could make proving a violation of this section more difficult.

6. CS Page 3, Lines 15-16
Change
Delete "remote"
Explanation
Deletion of superfluous language. All RFID devices scan and read remotely.

7. CS Page 4, Lines 12-14
Change
Delete section.
Create new section entitled Exemption.
Explanation
Enforcement measures are laid out in the Unfair Trade Practices. Making a violation of this act an Unfair Trade Practice removes the need for a separate enforcement clause.
New section creates an exemption for passports and national or international travel documents.

8. CS Page 4, Lines 16-18
Change
Delete definition of "active"
Insert definitions for "activate" and "activated."
Explanation
"Active" no longer appears in the bill for reasons explained in Change 2 above. "Activate" and "activated" are used instead.

9. CS Page 4, Lines 28-29
Change
After "item" insert "that transmits, receives, or stores personal information."
Explanation
Narrows the focus of the bill to only those devices which expose consumers to the threat of identity theft or other misuses of personal information.

10. CS Page 6, Lines 2-3
Change
Insert "Sec. 2."
Explanation
Amends AS 45.50.471 to add violations of this act to the list of Unfair Trade Practices. Opens it up to investigation by the AG's office as well as action by private parties and establishes civil penalties under the Unfair Trade Practices Act.

25-LS1509\C
Bannister
3/12/08

CS FOR SENATE BILL NO. 293( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIFTH LEGISLATURE - SECOND SESSION

BY

Offered:
Referred:

Sponsor(s): SENATOR MCGUIRE

A BILL

FOR AN ACT ENTITLED

"An Act relating to electronic communication devices and to personal information and making certain violations related to electronic communication devices unfair trade practices."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

*** Section 1.** AS 45 is amended by adding a new chapter to read:

Chapter 48. Electronic Communication Devices.

Sec. 45.48.010. Label and information required. (a) A provider of an electronic communication device shall label the electronic communication device, an item it is part of, or the packaging of the device or item clearly and conspicuously with an industry recognized symbol for radio frequency identification technology, and

(1) distribute information to the consumer that explains the meaning of the industry recognized symbol; or

(2) post a sign on the premises where the electronic communication device is sold or issued that

(A) indicates that the provider is selling or issuing an electronic communication device;

(B) explains the industry recognized symbol;

(C) explains how an electronic communication device may send, gather, or transmit information about the consumer that can be read by an unauthorized third party; and

(D) states whether it is technically feasible to deactivate the electronic communication device, and, if technically feasible to deactivate the electronic communication device, provide instructions on

(i) the specific location of the electronic communication device in an item, if it is part of another item; and

(ii) how the consumer may deactivate the electronic communication device.

(b) In this section,

(1) "industry recognized symbol" means a graphical system designed to provide a standard way to show the presence, frequency, and data structure of a radio frequency identification transponder;

(2) "transponder" means a wireless communications, monitoring, or control device that picks up and automatically responds to an incoming signal.

Sec. 45.48.020. Consent required. A provider shall, before the sale or issuance of an electronic communication device, in addition to complying with the requirements of AS 45.48.010, notify the consumer that the electronic communication device transmits personal information about the consumer and obtain the consent of the consumer under AS 45.48.070 for the collection, maintenance, and disclosure of information gathered by the electronic communication device about the consumer.

Sec. 45.48.030. Deactivation. (a) A provider may not activate a deactivated electronic communication device without obtaining the consent under AS 45.48.020 of the consumer who purchased the electronic communication device.

(b) A provider may not activate an electronic communication device that has been deactivated unless the provider deletes any personal information stored in the device before it was deactivated.

Sec. 45.48.040. Requirement prohibited. A provider may not require a consumer to keep an electronic communication device activated in order for the consumer to exchange, return, repair, or service an item that the electronic communication device is a part of.

Sec. 45.48.050. Required security measures. (a) At the point of sale or issuance, a provider shall use industry-accepted best standards to ensure that personal information collected by using the electronic communication device is secure from unauthorized access, loss, and tampering.

(b) A provider who retains personal information gathered through an electronic communication device shall implement adequate security measures to ensure that personal information collected by using the electronic communication device is secure from unauthorized access, loss, and tampering. The security measures must be consistent with the amount and sensitivity of the personal information being stored on the system.

Sec. 45.48.060. Scanning and reading. (a) A person may not scan, read, attempt to scan, or attempt to read an electronic communication device to obtain personal information on a consumer without obtaining the consumer's consent under AS 45.48.070.

(b) This section does not prohibit scanning or reading an electronic communication device or using information gathered through an electronic communication device to

(1) comply with federal or state law;

(2) comply with a properly authorized civil, criminal, administrative, or regulatory investigation, subpoena, or summons by an agency of the federal government, state government, or a municipality; or

(3) respond to a judicial process or, for examination, compliance, or other purposes authorized by law, to a government regulatory authority having jurisdiction over the person.

Sec. 45.48.070. Forms of consent. (a) The consent required by AS 45.48.020, 45.48.030, and 45.48.060 may be made by

(1) an electronic or written record; the record must, at a minimum,

clearly and conspicuously state the provider's privacy policy and the manner in which information relating to the consumer will be collected and disseminated; or

(2) a deliberate act that indicates that the consumer volunteers to be identified with the use of personal information gathered by, or contained within, an electronic communication device; in this paragraph, "deliberate act" includes a consumer voluntarily submitting the consumer's electronic communication device for scanning or reading for the purpose of completing a wholesale or retail transaction.

(b) Consent under (a)(2) of this section that is obtained in one specific situation may not apply to another specific situation unless the provider obtains in a written contract the consumer's permission to apply the consent to more than one specific situation.

Sec. 45.48.080. Exemption. This chapter does not apply to a travel document, including a passport and a passport card, that contains an electronic communication device and is issued by this nation or a foreign nation.

Sec. 45.48.095. Definitions. In this chapter,

(1) "activate" means to make activated;

(2) "activated" means not disabled, not deactivated, or not removed from another item;

(3) "clearly and conspicuously" means reasonably understandable and designed to call attention to the nature and significance of the information being conveyed;

(4) "consumer" means an individual who buys or is issued an electronic communication device for use in this state;

(5) "data" means signs, signals, writing, images, sounds, and other information;

(6) "deactivate" means to disable, deactivate, or remove from an item;

(7) "electronic communication device" means an electronic device, whether sold or issued by itself or as part of another item, that transmits, receives, or stores personal information and that uses radio frequency identification technology in

(A) the 902 - 928 MHz frequency range or the 2.4 GHz frequency authorized by the Federal Communications Commission; or

(B) another frequency range authorized by the Federal Communications Commission for radio frequency identification technology;

(8) "person" has the meaning given in AS 01.10.060, but expressly includes an agency of this state, a municipality of this state, or an agency of a municipality of this state; "person" does not include an agency in the judicial branch of the government of this state;

(9) "personal information" means one of the following data elements about a consumer whether used alone or with other information to identify the consumer:

(A) first or last name;

(B) social security number;

(C) driver's license number or state identification card;

(D) bank account number or other financial institution account number;

(E) credit card number or debit card number;

(F) automated or electronic signature;

(G) unique biometric data;

(H) an unlisted telephone number;

(I) medical information;

(J) address;

(K) date of birth;

(L) ethnicity or nationality;

(M) religion;

(N) political affiliation;

(O) sexual orientation;

(P) a private group affiliation not available in the public domain;

(10) "provider" means a person who sells, offers to sell, or issues an electronic communication device; in this paragraph, "sell" does not mean resale by a consumer;

(11) "radio frequency identification" means a tagging and tracking

technology that uses electronic devices to transmit information to a reader.

* **Sec. 2.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(53) violating AS 45.48 (electronic communication devices).

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

State Capitol
Juneau, Alaska 99801-1182
Deliveries to: 129 6th St., Rm. 329

MEMORANDUM March 3, 2008

SUBJECT: Sectional summary of SB 293 relating to electronic communication devices and to personal information
(Work Order No. 25-LS1509\A)

TO: Senator Lesil McGuire
Attn: Trevor Fulton

FROM: Theresa Bannister
Legislative Counsel

You have requested a sectional summary of the above-described bill. As a preliminary matter, note that a sectional summary of a bill should not be considered an authoritative interpretation of the bill and the bill itself is the best statement of its contents.

Section 1. Adds a new chapter dealing with selling, issuing, or offering to sell electronic communication devices.

Sec. 45.48.010. Requires the seller or issuer of an active electronic communication device to label (1) the device, (2) an item that the device is part of, or (3) the device or item's packaging with a universally accepted symbol for radio frequency identification technology. Requires the seller or issuer to (1) give the consumer information explaining the meaning of the symbol, or (2) post a sign indicating that the devices is being sold or issued, explaining the symbol, providing information about what the device does, and providing information about deactivation.

Sec. 45.48.020. Requires the seller or issuer of a device to also notify the consumer (before the sale or issuance) that the device transmits personal information about the consumer, if the device does that, and to obtain the consumer's consent for the collection, maintenance, and disclosure of the information.

Sec. 45.48.030. Allows for the consumer to be required to pay the costs of deactivation if the consumer wants a device deactivated but previously consented under sec. 45.48.020. When the device is deactivated, prohibits reactivation without getting consent under sec. 45.48.020.

Sec. 45.48.040. Prohibits a seller or issuer of a device from coercing a consumer to keep a device active in order to exchange, return, repair, or service an item that contains the device.

Sec. 45.48.050. When sold or issued, requires the seller or issuer of a device to use industry-accepted best standards to ensure that personal information collected by using the device is secure from unauthorized access, loss, and tampering. Requires a seller or issuer of a device who retains personal information obtained from using a device to implement adequate security measures to ensure that the personal information is secure from unauthorized access, loss, and tampering. Requires the security measures to be consistent with the amount and sensitivity of the information involved.

Sec. 45.48.060. Prohibits a person from remotely scanning or reading, or attempting to scan or read, a device to obtain a consumer's personal information without obtaining the consumer's consent under sec. 45.48.070. Identifies certain exceptions to this prohibition.

Sec. 45.48.070. Describes how the consent may be made. Indicates that consent obtained in one situation may not apply to another situation unless there is a written contract containing the consumer's permission to apply the consent to more than one situation.

Sec. 45.48.080. Allows the attorney general to bring an action against a violator of this chapter to enjoin further violations and to recover damages. Addresses how to handle multiple violations resulting from one single act or instance of conduct. Provides for the award of costs and attorney fees.

Sec. 45.48.095. Defines terms for the chapter.

If I may be of further assistance, please advise.

TLB:lmb
08-052.lmb

Response to questions brought up in the March 4th, 2008 Senate Labor & Commerce Committee hearing on SB 293: Electronic Communication Devices

Last week Senator Bunde asked if SB 293 was in essence a proactive bill or if it addressed any current problems with RFID use in the State of Alaska. My answer was that we were not aware of any current problems but that there have been numerous studies done in other states that show the vulnerabilities of this technology.

I would like to add two things to that response:
(1) Assistant Attorney General Ed Sniffen's statement that his office had not received "any direct complaints, at least not that I'm aware of, concerning this RFID technology, but it wouldn't surprise me if some identity theft victims in Alaska have had their identity stolen as a result of new technology that is able to remotely scan and get this information from consumer devices."

(2) The fact that RFID technology facilitates the tracking and profiling of consumers and of the public.

From the Stanford Technology Law Review:

> "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 name, social security number, or other random number—permits tracking of the movements and activities of an individual."

Also from the Stanford Technology Law Review:

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

While some of this may seem a little Orwellian in nature and perhaps even a bit paranoid, the fact is that a lot of people, and I would venture to say Alaskans in particular, are very sensitive to this sort of intrusion into their personal lives.

So, from a personal privacy perspective, SB 293 does address current problems with RFID use in Alaska, namely tracking and profiling.

Senator Bunde also asked how SB 293 would affect the use of US Passports equipped with RFID technology. We have drafted a CS that would exempt US Passports and other international travel documents.

I would also like to respond to the question of whether there are similar laws regulating RFID technology in other states. RFID technology—while not a new technology—is a relatively new area of concern for the public. It wasn't until 2005 that parents from Sutter, CA objected to middle-school badges equipped with RFID devices and, with the ACLU's help, brought RFID to the nation's attention. Since then, there have been more than 50 bills introduced in 27 states addressing RFID. While none of this legislation has made it into the law books, much of it is still pending. With such a robust response from lawmakers, it would seem that it is just a matter of time before state and federal laws catch up with this rapidly growing technology.

Please contact Trevor Fulton in Sen. McGuire's office with any further questions or clarifications.

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Melissa Ngo
Senior Counsel
Director of the Identification & Surveillance Project
Electronic Privacy Information Center

Hearing on

"SB 293: Electronic Communications Devices"

Before the

Senate Judiciary Committee
Alaska State Legislature

March 17, 2008
Beltz 211
State Capitol
Junea, AK
Via Teleconference

Chairman French, Vice-Chairman Huggins and members of the Committee, thank you for the invitation to appear before you today. My name is Melissa Ngo and I am Senior Counsel and Director of the Identification and Surveillance Project at the Electronic Privacy Information Center (EPIC) in Washington, D.C. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are pleased that you have convened this hearing today on "SB 293: Electronic Communications Devices."

EPIC Has Extensive Expertise In Technology Issues

EPIC has considerable expertise on technology issues, including those associated with radio frequency identification (RFID) technology.[1] We have testified about RFID and its security problems before the U.S. Congress and State legislatures, and submitted analyses on RFID programs to federal agencies. Some highlights include:

- In August 2007, EPIC detailed numerous privacy and security weaknesses in the U.S. Department of Homeland Security's Western Hemisphere Travel Initiative passport card proposal, which included long-range RFID technology.[2]

- In February 2007 testimony to the Maryland Senate and March 2007 testimony to DHS's Data Privacy and Integrity Advisory Committee, EPIC explained the myriad security and privacy problems that would be created if RFID technology were used in the REAL ID system.[3] In January 2008, DHS announced that RFID technology would not be used in the system.[4]

- In August and October 2005 comments to DHS, we urged the agency to abandon long-range, unsecured RFID technology in its I-94 forms in its United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program; or, in the alternative, to delay such use until the findings of ongoing RFID testing were released and current privacy and security risks were eliminated.[5] Reports from DHS's Inspector General and the Government

---

[1] *See generally* EPIC, Radio Frequency Identification (RFID) Systems, http://www.epic.org/privacy/rfid/.

[2] EPIC, *Comments on Docket No. USCBP-2007-0061: Proposed Rule: Documents Required for Travelers Departing From or Arriving in the United States From Within the Western Hemisphere* (Aug. 1, 2007), *available at* http://www.epic.org/privacy/rfid/whti_080107.pdf.

[3] Melissa Ngo, Dir., EPIC Identification & Surveillance Project. *Prepared Testimony and Statement for the Record at a Hearing on "Maryland Senate Joint Resolution 5" Before the Judicial Proceedings Comm. of the Maryland Senate* (Feb. 15, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_021507.pdf; Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, *Prepared Testimony and Statement for the Record at a Meeting on "REAL ID Rulemaking" Before the Data Privacy & Integrity Advisory Comm.*, Dep't of Homeland Sec. (Mar. 21, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf.

[4] Dep't of Homeland Sec., *Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 73 Fed. Reg. 5271 (Jan. 29, 2008), *available at* http://edocket.access.gpo.gov/2008/08-140.htm.

[5] EPIC, *Comments on Docket No. DHS-2005-0040: Notice of Privacy Act System of Records: The Automated Identification Management System* (Aug. 4, 2005), *available at* http://www.epic.org/privacy/us-

Accountability Office echoed many of EPIC's warnings.[6] The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony last year that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security.[7]

- In April 2005, we joined other civil liberties and technology groups in submitting comments urging the U.S. State Department to either abandon its proposal, because it would have made personal data contained in hi-tech passports vulnerable to unauthorized access, or to significantly strengthen the security standards.[8] Later that year, the State Department agreed to improve E-passport security and included Basic Access Control in an attempt to prevent unauthorized access to the data.[9]

- In July 2004, in testimony before the U.S. House of Representatives' Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, EPIC urged Congress to adopt a framework of fair information practices to govern collection of personal information through RFID.[10]

Public and Private Sectors Are Increasingly Using RFID Technology

RFID technology is rapidly increasing. Major uses of RFID include electronic roadway toll collection (E-Z pass systems), passports, various ID cards (such as university ID cards), credit and debit cards, supply chain management and animal tracking.[11]

---

visit/comments080405.pdf; EPIC, *Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry* (Oct. 3, 2005), *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf.

[6] Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006), *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_06-53_Jul06.pdf; Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Terrorism, Tech., & Homeland Sec., S. Comm. on the Judiciary*, 110th Cong. (Jan. 31, 2007), *available at* http://www.gao.gov/new.items/d07378t.pdf.

[7] Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal Year 2008 Dep't of Homeland Sec. Budget Before the H. Comm. on Homeland Sec.*, 110th Cong. (Feb. 9, 2007), *available at* http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.

[8] EPIC, EFF et. al, *Comments on RIN 1400-AB93: Electronic Passport* (Apr. 4, 2005), *available at* http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf.

[9] Dep't of State, *Final Rule: Electronic Passport*, 70 Fed. Reg. 61,553 (Oct. 25, 2005), *available at* http://edocket.access.gpo.gov/2005/05-21284.htm.

[10] Cedric Laurant, Policy Counsel, EPIC, *Testimony at a Hearing on "Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer" Before the Subcom. on Commerce, Trade, & Consumer Protection, H. Comm. on Energy & Commerce*, 108th Cong. (July 14, 2004), *available at* http://epic.org/privacy/rfid/rfidtestimony0704.html.

[11] *See* EPIC & PRIVACY INT'L, Privacy & Human Rights 2006: An International Survey of Privacy Laws and Developments (EPIC 2007).

RFID systems generally include a tag or chip (on which data is stored) and an antenna (to transmit the data to a reader).[12] "Active" RFID tags or chips have an internal power source, transmit continuously, and can initiate communication with readers. "Passive" RFID tags or chips do not have an internal power source but rather derive power from the reader's signal; nor can they initiate communication with readers.

RFID tags are small enough to be invisibly embedded in products, product packaging and even printing inks. They can be read from a distance and through a variety of substances such as snow, fog, ice or paint. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, or date of purchase.

Strong Regulations Are Needed To Protect Consumers

As RFID technology is increasingly used, we must be aware of the many problems inherent in the use of this technology. Privacy and security risks associated with RFID-enabled identification cards include "skimming" and "eavesdropping."[13] Skimming occurs when an individual with unauthorized RFID reader gathers information from an RFID chip without the cardholder's knowledge. Eavesdropping occurs when an unauthorized individual intercepts data as it is read by an authorized RFID reader or transponder.

In the absence of effective security techniques, RFID tags are remotely and secretly readable. Although the creation of a small, easily portable RFID reader may be complex and expensive now, it will be easier as time passes. For example, the distance necessary to read RFID tags was initially thought to be a few inches. The Department of Homeland Security said in 2005, "reliable reads can be received from a few inches to as much as 30 feet away from the reader."[14] Other tests also have shown that RFID tags can be read from 70 feet or more, posing a significant risk of unauthorized access.[15]

The danger of RFID technology is its wireless nature. If someone steals your RFID-enabled passport or credit card, then you would know that the data is missing and protect herself from identity theft by putting a fraud alert on your card and reporting your passport as stolen. But, how would you know if your credit card or passport information was stolen through skimming or eavesdropping? Strong regulations are needed to protect consumers from such misuse and abuse of RFID technology.

---

[12] *Id.*

[13] *See* EPIC, Radio Frequency Identification (RFID) Systems, *supra* note 1; EPIC & 24 Experts in Privacy & Technology, *Comments on DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* 24-28 (May 8, 2007), *available at* http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.

[14] Dep't of Homeland Sec., *Notice with request for comments*, 70 Fed. Reg. 44,934, 44,395 (Aug. 4, 2005), *available at* http://edocket.access.gpo.gov/2005/05-15487.htm.

[15] *See* Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems* (Feb. 22, 2005), *available at* http://eprint.iacr.org/2005/052; Scott Bradner, *An RFID warning shot*, NETWORK WORLD, Feb. 7, 2005.

Security Problems Associated with RFID Technology

Companies and groups often say that wireless technology, such as RFID systems, are used because they are convenient. However, with this convenience comes a significant security cost. Two high-profile examples demonstrate the security problems associated with the use of RFID technology.

Last week, the Dutch government announced that the security of access keys that are based on the widely used Mifare Classic RFID chip has been compromised.[16] Guusje ter Horst, Dutch Interior Minister, said in a letter to Parliament that the Mifare Classic RFID chips have been hacked.[17] The Mifare Classic RFID chip, created by Netherlands-based NXP Semiconductors, is part of the new Dutch RFID-enabled transportation card, which has cost $2 billion to develop and implement.[18] The Mifare Classic is also used in Boston and London's transportation cards. According to ter Horst, the Mifare Classic chip is used in 2 million Dutch building access passes and one billion cards with the technology are in use worldwide, she said.[19] In recent months, several researchers have separately issued papers detailing how to hack the Mifare Classic RFID chip.[20] The hacks allow criminals to clone cards that use the Mifare Classic chip, enabling them to create copies of building access keys or fraudulent transportation cards to avoid paying for such transportation.

This is not an anomaly. Security problems have plagued RFID chips for years. For examples, some companies are offering RFID-enabled credit cards, but in October 2006, researchers at the University of Massachusetts and RSA Labs revealed the shaky security employed by credit card companies.[21] In tests on 20 cards from Visa, MasterCard and American Express, they found that the cards transmitted the cardholder's name and other data in plain text and without encryption. The researchers gathered the data with a device made out of commercially available electronic components and were able to use the stolen data to buy products online.

---

[16] Letter from Guusje ter Horst, Dutch Interior Minister, to Netherlands Federal Parliament, *Regarding Chip Technology Access Passes*, Mar. 12, 2008 [hereinafter "Letter from Guusje ter Horst"].
[17] *Id.*
[18] Tom Sanders, *RFID-Hack Hits 1 Billion Digital Access Cards Worldwide*, WEBWERELD-NETHERLANDS, Mar. 12, 2008; *Dutch interior affairs minister says widely used security pass can be hacked*, ASSOCIATED PRESS, Mar. 12, 2008.
[19] Letter from Guusje ter Horst, *supra* note 16.
[20] Karsten Nohl, Univ. of Virginia, *Cryptanalysis of Crypto-1* (Mar. 10, 2008), *available at* http://www.cs.virginia.edu/~kn5f/pdf/Mifare.Cryptanalysis.pdf; Roel Verdult, Radboud Univ. Nijmegen, *Proof of concept, cloning the OV-Chip card* (Jan. 2008), *available at* http://www.cs.ru.nl/~flaviog/OV-Chip.pdf; Pieter Siekerman & Maurits van der Schee, Univ. of Amsterdam, *Security Evaluation of the disposable OV-chipkaart* (July 26, 2007), *available at* http://staff.science.uva.nl/~delaat/snc-2006-2007/p41/report.pdf.
[21] John Schwartz, *Researchers See Privacy Pitfalls in No-Swipe Credit Cards*, N.Y. TIMES, Oct. 22, 2006; Thomas S. Heydt-Benjamin, Daniel V. Bailey, et al, *Vulnerabilities in First-Generation RFID-enabled Credit Cards* (Oct. 22, 2006), *available at* http://prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf.

Many States Are Taking Steps To Establish Appropriate Safeguards for the Use of RFID Technology

Like Alaska, many states are debating legislation to ensure adequate protections for RFID use.

- Last week, Washington state passed a law to prevent "skimming" of data from RFID tags;[22]
- California, North Dakota and Wisconsin have passed legislation forbidding the compelled implantation of RFID chips in humans[23];
- Currently, California is debating a law to prevent "skimming"[24];
- A number of other states are debating legislation to restrict the use of RFID technology.[25]

EPIC Guidelines on Commercial Use of RFID Technology

EPIC does not believe that it is necessary to use RFID technology in most instances. However, if RFID is to be used we have created a set of guidelines that would help ensure the privacy and security of data.[26]

For RFID technology users who do not collect personally identifiable information, their duties under the EPIC Guidelines are: to notify consumers of the presence of RFID, to allow for people to disable and remove the tags, to be accountable for security and privacy breaches that occur. Also, users are prohibited from tracing individuals with RFID tags, recording data or requiring data collection through RFID use.

For RFID technology users who do collect personally identifiable information, their duties under the EPIC Guidelines are: to receive explicit written consent from those affected, to use Fair Information Practices (minimization of data collection, data quality, purpose specification, security safeguards, openness, individual participation, and

---

[22] Washington, HB 1031, "An Act Relating to electronic communication devices; adding a new chapter to Title 19 RCW; creating new sections; and prescribing penalties," passed Mar. 11, 2008, *available at* http://apps.leg.wa.gov/billinfo/summary.aspx?year=2007&bill=1031.

[23] California, SB 362, "An act to add Section 52.7 to the Civil Code, relating to identification devices," enrolled Oct. 12, 2007, *available at* http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0351-0400/sb_362_bill_20071012_chaptered.html; North Dakota, SB 2415, "An Act to create and enact a new section to chapter 12.1-15 of the North Dakota Century Code, relating to implanted microchips in individuals; and to provide a penalty," signed Apr. 4, 2007, *available at* http://www.legis.nd.gov/assembly/60-2007/bill-text/HBPJ0300.pdf; Wisconsin, Act 482, "An Act to create 146.25 of the statutes; relating to: prohibiting the required implanting of a microchip in an individual and providing a penalty," enacted May 30, 2006, *available at* http://www.legis.state.wi.us/2005/data/acts/05Act482.pdf.

[24] California, SB 31, *An act to add Title 1.80 (commencing with Section 1798.79) and Title 1.81.4 (commencing with Section 1798.98) to Part 4 of Division 3 of the Civil Code, relating to privacy*, *available at* http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_31_bill_20080107_amended_sen_v96.html.

[25] *See* EPIC, Radio Frequency Identification (RFID) Systems, *supra* note 1.

[26] EPIC, *Guidelines on Commercial Use of RFID Technology* (July 2004), *available at* http://epic.org/privacy/rfid/rfid_gdlnes-070904.pdf.

accountability). They also have the same prohibitions as RFID users who do not collect personally identifiable information.

Under the EPIC Guidelines, RFID subjects have certain rights. They have the right: to access and correct their data, to remove tags so that data cannot be collected, and to hold data-gatherers accountable for privacy and security violations. In this way, people can protect their rights, including their right to informational self-determination – so an individual can decide who has what information about that individual.

SB 293 Includes Many Protections for Consumers, But Safeguards Can Be Strengthened

EPIC strongly supports SB 293, "An act relating to electronic communication devices and to personal information and making certain violations related to electronic communication devices unfair trade practices." SB 293 includes follows many of the EPIC Guidelines, but there are some areas that could be improved in the bill.

We support the bill's requirements for RFID technology users to: (1) clearly label tagged articles, (2) obtain consumer consent for continued activation after the RFID-tagged article is bought, (3) obtain consumer consent to reactivate RFID tags and (4) secure the data gathered through the RFID systems. We also support SB 293's prohibitions against: (1) allowing RFID technology users' to require continued activation of RFID tags in order for consumers "to exchange, return, repair, or service an item that" contain RFID tags, and (2) unauthorized scanning and reading of RFID tags.

Regulation of Unique Identifiers Needed

Though SB 293 includes many protections for consumers, there are four ways in which the bill can be strengthened. First, and most importantly, we urge the Committee to also address in SB 293 unique identifiers linked to databases containing personally identifiable information. Though companies have urged against the regulation of these unique identifiers, they should be covered under SB 293 because the misuse or abuse of such unique identifiers could be as risky as misuse or abuse of Social Security Numbers.[27]

The Government Accountability Office (GAO), the investigative arm of Congress, has cautioned against the use of RFID technology to track individuals. "Once a particular individual is identified through an RFID tag, personally identifiable information can be retrieved from any number of sources and then aggregated to develop a profile of the individual. Both tracking and profiling can compromise an individual's

[27] For more information on unique identifiers associated with RFID tags, *see* Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), *The METRO "Future Store" Special Report* (2004) *available at* http://www.spychips.com/metro/overview.html; KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move (Penguin 2006).

privacy," the GAO said.[28] EPIC urges the Committee to regulate the use of these unique identifiers and the detailed profiles that can be constructed with them.

Private Right of Action Needed

Second, SB 293 needs to contain an enforcement provision that includes a private right of action for consumers. An earlier version of the bill included an enforcement provision that said:

> "**Sec. 45.48.080. Enforcement.** (a) The attorney general may bring an action against a person who violates this chapter to enjoin further violations and to recover the greater of
>
> (1) the actual damages suffered by a consumer; or
> (2) $10,000 for each separate violation.
>
> (b) In (a) of this section, if multiple violations of this chapter result from a single act or instance of conduct, the multiple violations are considered one violation.
>
> (c) In an action under (a) of this section, a court may
>
> (1) increase the damages up to three times the damages allowed by (a) of this section if the person who violated this chapter has engaged in a pattern and practice of violating this chapter; and
> (2) award costs and attorney fees as provided by the rules of court."

There must be a private right of action so that individuals may be able to police their rights in case of misuse or abuse of the RFID systems or data. Attorneys general are very busy and would not be able to pursue violations as determinedly as individuals who are affected. We urge the Committee to put this provision back into SB 293 with this change:

> "**Sec. 45.48.080. Enforcement.** (a) The attorney general *or any individual* may bring an action against a person or business who violates this chapter to enjoin further violations and to recover the greater of" (emphasis ours)

Stronger Provisions on Deactivation Are Needed

Third, SB 293 would also be improved by including stronger provisions on deactivation. In Sec. 45.48.010 (a)(2)(D)(ii), the language "how the consumer may deactivate the device" puts the burden on the consumer to deactivate the device, and this language should be changed. We recommend the language be changed to "how the consumer may have the device deactivated, at no cost to the consumer, by the provider of

---

[28] Linda D. Koontz, Dir., Info. Mgmt. Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Homeland Sec., H. Comm. on Appropriations*, 110th Cong. (Apr. 14, 2007), *available at* http://www.gao.gov/new.items/d07630t.pdf.

an active communication device." We believe that the consumer should never have to pay to have such tracking technology deactivated.

We also recommend that there be an option to permanently deactivate RFID tags so that it would not be possible for the tags to be reactivated at a later time. In Sec. 45.48.030, we recommend adding a new (a) section and moving the current (a) and (b) sections to (b) and (c), respectively. The new (a) section would allow consumers to choose the permanent deactivation of RFID tags. We recommend this language: "(a) A consumer must clearly and conspicuously be given the choice to permanently deactivate an electronic device, wherein permanent deactivation allows no possibility for reactivation of the device."

RFID Readers and Transponders Should Also be Labeled

Finally, we recommend that consumers should be given notice of RFID readers or transponders, as well as RFID tags. In Sec. 45.48.010, we recommend that there should be a requirement that RFID readers also clearly and prominently display a universally recognized symbol for RFID technology, so that consumers will know where there is a danger of their data being read without their knowledge. We recommend this language: "**Sec. 45.48.010. Label and information required.** (a) A provider of an active electronic communication device shall label the electronic communication device and electronic communication device readers, an item either the device or reader is part of, the packaging of either the device, reader, or item clearly and conspicuously with a universally accepted symbol for radio frequency identification technology."

Conclusion

As the use of RFID technology increases, there will be more questions about privacy and security. Consumers need strong protections against misuse and abuse of theses systems and the data collected. SB 293, "An act relating to electronic communication devices and to personal information and making certain violations related to electronic communication devices unfair trade practices," has taken a number of steps to safeguard consumers. We support the bill, but urge the four changes that have outlined: (1) including regulations on the use of unique identifiers and the profiles that can be created; (2) including an enforcement provision with a private right of action; (3) stronger provisions on deactivation of tags, including the possibility of permanent deactivation; and (4) clearly and prominently labeling RFID readers or transponders.

I appreciate the opportunity to be here today. I will be pleased to answer your questions.

Attachment:

EPIC, *Guidelines on Commercial Use of RFID Technology* (July 2004).

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Guidelines on Commercial Use of RFID Technology

(FINAL VERSION - July 9, 2004)

Introduction

The guidelines are proposed to guide the use of RFID technology in order to protect both private enterprise interests and consumer privacy interests. This means that these guidelines do not address protection of consumer privacy from any governmental action. Rather, they seek to protect consumer privacy from private enterprises. Further, these guidelines focus on use in the retail and manufacturing industry where retailers and manufacturers are beginning to implement item-level RFID tagging to facilitate supply chain efficiency, inventory control, and similar applications.

These guidelines primarily address commercial, private applications which may use RFID tags to draw conclusions about consumers without their knowledge or consent, or that might generate data which could be used for entirely different purposes at a later date.

These guidelines are divided into three parts. Part A addresses the duties of private enterprises that use RFID technology. It imposes minimum requirements on RFID users, recognizing the advantages that RFID technology can provide while at the same time addressing privacy concerns. Part B addresses practices in which the RFID Users should never engage, including tracking, snooping, and coercing consumers to accept live RFID tags or associate their personal data with an RFID application. Finally, Part C states the rights of consumers who are exposed to RFID technology and incorporates some of the Users' duties stated in Part A.

Definitions

"RFID" means Radio Frequency Identification, *i.e.*, technologies that use radio waves to automatically identify individual items.

"Tag" means a microchip that is attached to an antenna and is able to transmit identification information, *i.e.*, capable of receiving data from, or transmitting data to, a Reader.

"Reader" means a device, capable of reading data from a tag or transmitting data to a RFID tag.

"RFID Subject" or "Individual" means a consumer, customer, or any other such individual that comes in contact with a product that has attached to it, or contains, an RFID tag.

"RFID User" means an RFID operator, such as a store, warehouse, hospital, and the like, who employs RFID technology, including RFID readers and tags.

"Premises" means a store, a warehouse, a hospital, or any other such equivalent space that encompass the tags and the readers that communicate with RFID tags.

"Consent" means the freely given, specific and informed indication of a RFID subject's wish to have his/her personal information processed by the means of RFID technologies.

RFID Guidelines

A. What RFID Users Must Do:

*1. **NOTICE***. Give notice to a RFID Subject of:

a. ***Tag presence***, whether through labels, logos, or equivalent means, or through display, either at the place where a tagged item is stored, such as a shelf or counter, or at point of sale, such as a cash register. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

b. ***Reader presence***, whether through labels, logos, or equivalent means, or through display, whenever tag readers are present. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

c. ***Reading activity***. RFID Users must use a tone, light, or other readily observable and recognized signal whenever a tag reader is in the act of drawing information from an RFID tag anywhere on the sales floor.

2. ***REMOVAL***. Attach tags to items in such a way as to allow for the easiest possible removal of tags.

3. ***ANONYMITY PRIORITY***. Any RFID user -- before linking RFID tags to personal information -- should first consider alternatives which achieve the same goal without collecting personal information or profiling customers. If personal information must be collected and associated with tag data, the RFID user must satisfy the following five requirements:

a. ***Consent***. Obtain written consent from an individual before any personally identifiable information of the individual, including name, address, telephone number, credit card number, and the like, is attached to, stored with, or otherwise associated with data collected via the RFID System.

b. ***Purpose***. Before obtaining written consent, the RFID User must inform the RFID subject about the purpose of associating gathered data with personal information, and specify that purpose before such attaching, storing, or association.

c. ***Use limitation***. Before obtaining written consent, the RFID User must inform individuals about the scope of use of gathered data, whether the use is limited to the person's own interests or whether the data will be disclosed to third parties. Keep data only as long as it is necessary for the purpose for which the data was associated with personal information.

d. ***No third party disclosure***. Not disclose, directly or through an affiliate, to a nonaffiliated third party an individual's personally identifying information in association with RFID tag identification information.

e. ***Data quality***. Keep gathered data accurate, complete and up-to-date, as is necessary for the purposes for which it is to be used.

4. ***SECURITY***. Take reasonable measures to ensure that any data processed via an RFID system is transmitted and stored in a secure manner, and that access to the data is limited to those individuals needed to operate and maintain the RFID system.

5. ***OPENNESS***. RFID Users must make readily available to individuals, through the Internet or other equivalent means, specific information about their policies and practices relating to its handling of personal information. Any personally identifiable information itself shall be provided upon written request of the individual in a secure manner.

6. ***ACCOUNTABILITY***. Designate someone who is accountable for the RFID User's compliance with these guidelines.

B. What RFID Users Must NOT Do:

1. ***TRACK***. Track the movement of RFID subjects at any time without their written consent to all tag reading events. RFID users shall not track individuals via tagged items on the premises or outside the premises where an RFID system is employed to obtain individual shopping habits or any other such information obtainable through tracking, even upon suspicion of such activities as fraud or shoplifting.

2. ***SNOOP***. Record or store tag data from tags that do not belong to the RFID User for any reason except for the processing of returns or warranty service and upon the consumer's request. RFID users shall not collect RFID data from objects on, or carried by, an individual person for the purpose of generating a consumer profile, even if the profile is assigned anonymously.

3. ***COERCE***. Coerce or force individuals to keep tags turned on after purchase for such benefits as warranty tracking, loss recovery, or compliance with smart appliances; and not require individuals to provide unnecessary personal information as a precondition of a transaction. RFID Users must allow individuals who so desire to enroll anonymously in any RFID data-gathering scheme.

C. RFID Subjects' rights:

1. ***ACCESS***. RFID Subjects must have the right to access data containing personally identifiable information collected through an RFID system, and have the opportunity to make corrections to that information.

2. ***REMOVAL***. RFID Subjects have the right to get tags removed from tagged items.

3. ***ACCOUNTABILITY***. RFID Subjects have the right to challenge the compliance of persons employing RFID systems when practice contradicts the guidelines set forth above.

March 25, 2008

The Honorable Gary Stevens
Chairman, Rules Committee
Alaska State Senate
State Capitol, Room 103
Juneau, AK 99801-1182

Dear Chairman Stevens:
On behalf of our more than 300 member companies and the information technology industry at large, the Information Technology Association of America (ITAA) would like to register our opposition to Senate Bill 293.

The use of RFID technology offers significant benefits in many areas, including supply-chain efficiency, ensuring accurate pharmaceutical drug tracking, safe handling of hazardous materials, food safety/recall, transport, security, logistics and stock control. As RFID technology matures and applications proliferate, it has the potential to enable global commerce and spur American innovation and competitiveness, while providing significant improvements in safety and security. RFID is often mentioned as one of a set of emerging and connective technologies that may potentially have an impact on business and daily life that is as profound as the rise of the Internet.

ITAA is concerned that SB 293 will stifle innovation and delay RFID benefits to the citizens of Alaska. As written this legislation provides onerous consent requirements, and seeks to regulate a technology rather than punishing unlawful behavior.

This legislation assumes that all RFID applications transmit personally identifiable information and are vulnerable to illegal attacks. This could not be farther from the truth. Many radio frequency applications simply transmit a unique identifier that links to information in a secure database. If a program requires the transmission of personally identifiable information security measures can be put in place to prevent the unwanted theft of information. Dozens of laws exist to protect consumer information.

ITAA believes that data collected using RFID should be protected with the most rigorous privacy and security standards to protect all individual data regardless of the source. Caution should be used, however, when creating new legislation that seeks to regulate a

Information Technology Association of America
1401 Wilson Blvd., Suite 1100, Arlington, VA 22209-2318 • Phone: (703) 522-5055 Fax: (703) 525-2279

particular technology or mandate particular standards for its application. In today's environment, technology evolves and is updated every 18 months. A technology that is cutting edge today will be surpassed by new innovations within a two-year period. Legislation calling for particular solutions or standards is not flexible enough to accommodate this pace of change.

We urge Alaska legislators not to prematurely regulate RFID technology and prohibit innovation. If you or your staff have any questions, please feel free to contact me at (703) 284-5337 or jkerber@itaa.org.

Sincerely,

Jennifer Kerber
Senior Director, Identity Management Policy

cc: Alaska State Senate

About ITAA

The Information Technology Association of America (ITAA) is the premier IT industry association working to maintain America's role as the world's innovation headquarters. Our members are responsible for producing the majority of credentialing and identity management programs. Our members include companies producing drivers licenses and other identity cards; managing federal, state and local smart card and identity credentialing programs; providing biometric devices, radio frequency identification technologies and middleware solutions; as well as performing background checks and other identity proofing and authentication services for government and commercial customers worldwide. Its members range from the smallest start-ups to industry leaders offering Internet, software, services and hardware solutions to the public and commercial sector markets. The Association maintains a formal alliance with more than 40 regional groups in the U.S. and Canada, representing 16,000 technology-related companies through the Council of Regional Information Technology Associations. It also serves as secretariat for the World Information Technology and Services Alliance, a network of 69 industry associations from around the world. For more information, visit www.itaa.org.

Information Technology Association of America
1401 Wilson Blvd., Suite 1100, Arlington, VA 22209-2318 • Phone: (703) 522-5055 Fax: (703) 525-2279

ITAA

TRANSMITTAL SHEET

Date 3/27/08 **No. of Pages (including cover)** 3

Deliver to Senator Hollis French **Company**

Dept. **Fax No.** 907-465-6595

Sender: Jennifer Korber **Phone:** 703-284-5337

Attached is a letter sent to Senator Stevens that outlines our concerns with Senate B. 1193

Information Technology Association of America
1401 Wilson Blvd., Suite 1100, Arlington, VA 22209-2318 ■ Phone (703) 522-5055 FAX (703) 525-2279

The Seattle Times

Monday, February 19, 2007 - Page updated at 12:00 AM

Does RFID technology pose risk?

By Elliott Wilson
Seattle Times staff reporter

OLYMPIA — Tiny radio transmitters in credit cards, on clothing tags and even inside animals expedite sales, guide products through the supply chain and help lost pets get home.

But privacy advocates worry the same technology could be used to spy on consumers.

To pre-empt such high-tech surveillance, state Rep. Jeff Morris, D-Mount Vernon, wants to make sure no one can use such technology to track people through the merchandise they buy, or to tap into their personal information.

His proposal, House Bill 1031, includes some of the nation's tightest restrictions on the technology known as radio frequency identification, or RFID.

Morris has the support of privacy groups, but technology companies say his bill addresses a problem that doesn't need fixing. The companies say they already work hard to protect customers' privacy and that additional regulation would only hurt their industries.

RFID tags store data that can be transmitted wirelessly when they come close to a reader device.

The uses range from tiny stickers that help track crates in Wal-Mart storerooms to sophisticated chips that transmit an address or account information from a cellp one or other electronic gadget.

The distance the information is transmitted varies: Some tags need almost direct contact with an RFID reader, while others can send signals several feet or even farther.

Under Morris' bill, anyone distributing items equipped with RFID technology would have to label the products, notify consumers if the item can transmit personal data, and show how to deactivate the transmitter if possible.

Retailers and other distributors also would have to ensure that RFID transmissions are securely encrypted.

The bill had its second hearing Friday in the House Technology, Energy and Communications Committee, which Morris chairs.

Representatives from RFID producers, retailers and the cellphone industry said the regulations would hamper their businesses and stifle new technology.

If the legislation passes, companies working on new uses for RFID may abandon their efforts, said Allison Fleming, a manager with the RFID company EPCglobal.

T-Mobile lobbyist Russell Sarazen said, "It would have devastating effects to T-Mobile and the rest of the wireless industry." He and other phone-industry representatives argue for an exemption for cellphones.

Wireless companies are developing RFID-equipped phones that allow users to order products simply by holding a handset close to a poster or advertising billboard, according to RFID Journal, a trade publication.

Sarazen also said the regulations are pointless for his industry because the whole purpose of the products is to send electronic messages.

Liz McIntyre, co-author of the book "Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move," said the RFID chips are everywhere and are small enough to slip between layers of paint, hide in tennis shoes, or secretly stick on computers.

"I could walk by things tagged with RFID and never even know," she said.

McIntyre foresees consumers unwittingly wearing RFID-tagged garments that could be tracked by strategically placed RFID readers.

That would give companies a complete history of each product, from store room to landfill, and give them a detailed look into consumer habits.

"It's likely when you buy a pair of shoes, it's going to be a proxy for you," McIntyre said.

Elliott Wilson: 360-236-8169

or ewilson@seattletimes.com

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Guidelines on Commercial Use of RFID Technology

(FINAL VERSION - July 9, 2004)

Introduction

The guidelines are proposed to guide the use of RFID technology in order to protect both private enterprise interests and consumer privacy interests. This means that these guidelines do not address protection of consumer privacy from any governmental action. Rather, they seek to protect consumer privacy from private enterprises. Further, these guidelines focus on use in the retail and manufacturing industry where retailers and manufacturers are beginning to implement item-level RFID tagging to facilitate supply chain efficiency, inventory control, and similar applications.

These guidelines primarily address commercial, private applications which may use RFID tags to draw conclusions about consumers without their knowledge or consent, or that might generate data which could be used for entirely different purposes at a later date.

These guidelines are divided into three parts. Part A addresses the duties of private enterprises that use RFID technology. It imposes minimum requirements on RFID users, recognizing the advantages that RFID technology can provide while at the same time addressing privacy concerns. Part B addresses practices in which the RFID Users should never engage, including tracking, snooping, and coercing consumers to accept live RFID tags or associate their personal data with an RFID application. Finally, Part C states the rights of consumers who are exposed to RFID technology and incorporates some of the Users' duties stated in Part A.

Definitions

"RFID" means Radio Frequency Identification, *i.e.*, technologies that use radio waves to automatically identify individual items.

"Tag" means a microchip that is attached to an antenna and is able to transmit identification information, *i.e.*, capable of receiving data from, or transmitting data to, a Reader.

"Reader" means a device, capable of reading data from a tag or transmitting data to a RFID tag.

"RFID Subject" or "Individual" means a consumer, customer, or any other such individual that comes in contact with a product that has attached to it, or contains, an RFID tag.

"RFID User" means an RFID operator, such as a store, warehouse, hospital, and the like, who employs RFID technology, including RFID readers and tags.

"Premises" means a store, a warehouse, a hospital, or any other such equivalent space that encompass the tags and the readers that communicate with RFID tags.

"Consent": means the freely given, specific and informed indication of a RFID subject's wish to have his/her personal information processed by the means of RFID technologies.

RFID Guidelines

A. What RFID Users Must Do:

1. NOTICE. Give notice to a RFID Subject of:

a. ***Tag presence***, whether through labels, logos, or equivalent means, or through display, either at the place where a tagged item is stored, such as a shelf or counter, or at point of sale, such as a cash register. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

b. ***Reader presence***, whether through labels, logos, or equivalent means, or through display, whenever tag readers are present. The notice shall be reasonably conspicuous to the individual and contain information that enables the individual to be reasonably aware of the nature of the RFID system and the data processing in place.

c. ***Reading activity***. RFID Users must use a tone, light, or other readily observable and recognized signal whenever a tag reader is in the act of drawing information from an RFID tag anywhere on the sales floor.

2. *REMOVAL*. Attach tags to items in such a way as to allow for the easiest possible removal of tags.

3. *ANONYMITY PRIORITY*. Any RFID user -- before linking RFID tags to personal information -- should first consider alternatives which achieve the same goal without collecting personal information or profiling customers. If personal information must be collected and associated with tag data, the RFID user must satisfy the following five requirements:

a. ***Consent***. Obtain written consent from an individual before any personally identifiable information of the individual, including name, address, telephone number, credit card number, and the like, is attached to, stored with, or otherwise associated with data collected via the RFID System.

b. ***Purpose***. Before obtaining written consent, the RFID User must inform the RFID subject about the purpose of associating gathered data with personal information, and specify that purpose before such attaching, storing, or association.

c. ***Use limitation***. Before obtaining written consent, the RFID User must inform individuals about the scope of use of gathered data, whether the use is limited to the person's own interests or whether the data will be disclosed to third parties. Keep data only as long as it is necessary for the purpose for which the data was associated with personal information.

d. ***No third party disclosure***. Not disclose, directly or through an affiliate, to a nonaffiliated third party an individual's personally identifying information in association with RFID tag identification information.

e. ***Data quality***. Keep gathered data accurate, complete and up-to-date, as is necessary for the purposes for which it is to be used.

4. *SECURITY*. Take reasonable measures to ensure that any data processed via an RFID system is transmitted and stored in a secure manner, and that access to the data is limited to those individuals needed to operate and maintain the RFID system.

5. *OPENNESS*. RFID Users must make readily available to individuals, through the Internet or other equivalent means, specific information about their policies and practices relating to its handling of personal information. Any personally identifiable information itself shall be provided upon written request of the individual in a secure manner.

6. *ACCOUNTABILITY*. Designate someone who is accountable for the RFID User's compliance with these guidelines.

B. What RFID Users Must NOT Do:

1. *TRACK*. Track the movement of RFID subjects at any time without their written consent to all tag reading events. RFID users shall not track individuals via tagged items on the premises or outside the premises where an RFID system is employed to obtain individual shopping habits or any other such information obtainable through tracking, even upon suspicion of such activities as fraud or shoplifting.

***2. SNOOP*.** Record or store tag data from tags that do not belong to the RFID User for any reason except for the processing of returns or warranty service and upon the consumer's request. RFID users shall not collect RFID data from objects on, or carried by, an individual person for the purpose of generating a consumer profile, even if the profile is assigned anonymously.

***3. COERCE*.** Coerce or force individuals to keep tags turned on after purchase for such benefits as warranty tracking, loss recovery, or compliance with smart appliances; and not require individuals to provide unnecessary personal information as a precondition of a transaction. RFID Users must allow individuals who so desire to enroll anonymously in any RFID data-gathering scheme.

C. RFID Subjects' rights:

1. *ACCESS*. RFID Subjects must have the right to access data containing personally identifiable information collected through an RFID system, and have the opportunity to make corrections to that information.

2. *REMOVAL*. RFID Subjects have the right to get tags removed from tagged items.

3. *ACCOUNTABILITY*. RFID Subjects have the right to challenge the compliance of persons employing RFID systems when practice contradicts the guidelines set forth above.

our mission

about NCL

NCL's Mission Statement

Our mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad. The National Consumers League is a private, nonprofit advocacy group representing consumers on marketplace and workplace issues. We are the nation's oldest consumer organization.

NCL provides government, businesses, and other organizations with the consumer's perspective on concerns including child labor, privacy, food safety, and medication information.

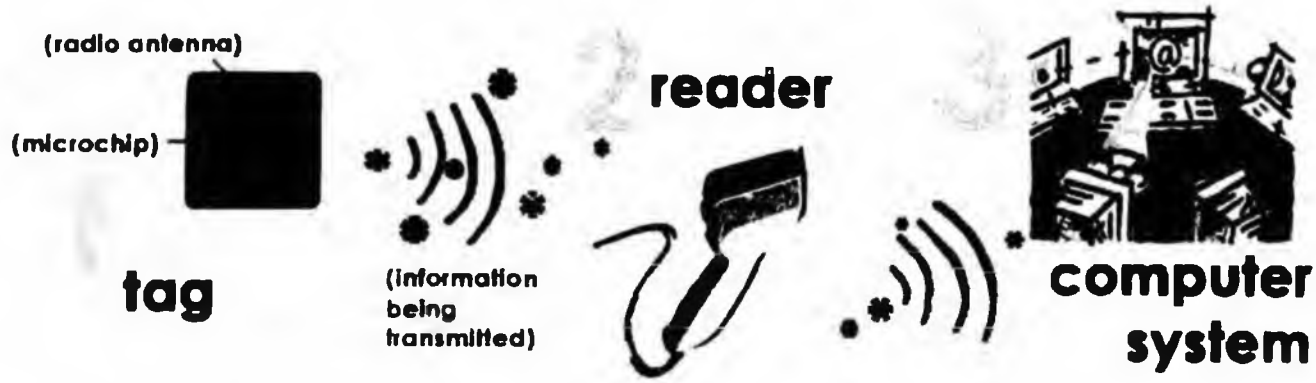
other info from NCL:
health
fraud
finances
labor
food
technology
utilities
privacy
general interests

Fraud.org • LifeSmarts • StopChildLabor.org • SOSRx • Fields Of Hope • Phishinginfo.org

Frequently asked questions about RFID

Understanding RFID

RFID - radio frequency identification - has been around for over 60 years. Today, consumers come into contact with this technology in many forms, from the passes that employees use to gain access to the buildings where they work to payment cards that don't have to be swiped through a machine. As RFID is increasingly used in people's daily lives, it's important to what it is and how it works.



What is RFID and how does it work?

RFID is a wireless technology that is used to identify things. It typically involves three components: a **tag**, a **reader**, and a **computer system**.

Sometimes referred to as a **transponder**, the tag consists of a microchip and a radio antenna. The chip in the tag contains information about the item that it is either attached to or that it is embedded in. The tag transmits that information to the reader using radio signals.

The reader, also called an **interrogator**, is a device that is designed to pick up those radio signals and deliver the information they contain to the computer system.

The computer system can use the information in a variety of ways, depending on what it is set up to do - for example, it might be to track inventory or give a person access to an office building. It may be connected to databases that contain more information linked to the item and, in some cases, to the person using it.

How big are the tags?

The tags vary in size depending on the size of the chip they contain. Some tags are smaller than a grain of rice and can be embedded in products or labels, even planted

under the skin. Others are as big as a deck of playing cards and are attached to pallets and cases. Tags also vary in how much information their chips can store or process, with inexpensive "dumb" tags having little memory or processing capacity and more costly "smart" tags having far greater computing power.

How is RFID used in the real world?

Many consumers are already familiar with one form of RFID - the toll-pass that drivers can keep inside their cars to go through toll booths without having to stop to pay. The chip in the toll-pass sends information to a reader located in the toll booth. This information, the reader's location, and the time and date of the reading are then transmitted to a computer system, which may be linked to databases containing other information such as the toll fee and the bank account that will be billed for the toll.

Another use of RFID that some consumers are familiar with are payment systems that allow them to wave a tag in front of a reader on a gas pump to fill up a gas tank. RFID technology is also being used to control entry into certain buildings. Some pet owners are having their dogs or cats implanted to help track them in case they get lost, and the U.S. Food and Drug Administration has approved a tag to be implanted in humans containing their patient records for use in hospitals. RFID is being used in supply chains to track the movement of products from a manufacturer to a distributor to a retailer and any points in between. Depending on their intended use, RFID systems vary in capability, the complexity and cost of the tag, the amount and sensitivity of the information that the chips contain, and the distance from which readers can pick up the signals from the tags.

How close to the tag does the reader need to be?

That depends on the type of RFID tag. Some tags are called passive because they don't have their own power source. The reader powers up the tag by sending it a radio signal, and the tag responds by sending radio signals back with the information the chip contains. An active tag has its own small battery or other source of power and doesn't require power from the reader to send a signal to it. Passive tags can be read only from a relatively short distance, from a few inches to a few yards. Active tags can generally be read from a longer distance.

The radio signals used to communicate between tags and readers can pass through objects - they don't require a direct line of sight between them as barcodes do with bar code readers. This means that if individual items in a grocery store were tagged, it is theoretically possible to go through the checkout simply by wheeling the shopping cart by a reader, without having to unload it. As the technology advances, the ability to get consistently accurate reads is improving.

What information can be stored on the chips in the tags?

The chips in the tags may have all sorts of information on them, depending on the purpose for which the tags are used. For example, those that control access to buildings may contain the employee's name, job title, and information about which parts of the building the person can go. Some tags have only a unique ID code for the item they are identifying (see Understanding the EPC). The information on the chips may be linked to databases that contain more information, including about individuals. As technology advances, the chips in the tags will be able to store and process an increasing amount of information.

What about security?

As with any technology, criminals might try to exploit RFID, so security is important. For consumers, the main security concern is about RFID uses in which their personal information, such as health records or bank account numbers, is stored on the chips in the tags or in databases that are linked to them. There are various types of security measures that can be used to protect information as it is transmitted and stored, such as encrypting it - turning it into a code that only authorized users can translate. Devices such as key fobs and wireless phones that are equipped with RFID in order to use them to pay for purchases present another security concern - what happens if they are lost or stolen? One way to prevent unauthorized use would be to have the ability to "lock" these devices so their functions can be turned off if they fall into the wrong hands.

How can RFID benefit consumers?

Convenience is one of the biggest benefits of RFID. In addition to the tags that allow drivers to pass through toll booths quickly, consumers can also use cell phones, key fobs, and credit cards that are equipped with RFID to pay for purchases simply by waving them in front of readers. RFID tags on items can make it easier for consumers to make product returns without receipts. Similar to the way that pets can be implanted with tags to make it easier to identify them if they are lost, Alzheimer's patients may wear tagged wrist bands in case they wander away from their caregivers. Patients in some hospitals wear them to ensure that they get the right medications, and expensive hospital equipment is being tagged so it can be located quickly and be more efficiently used.

Understanding EPC

What does "EPC" mean?

EPC stands for Electronic Product Code. It is also sometimes called "the next generation barcode." It's a unique identification code that is stored in the chip on a tag as a product goes through the supply chain. Unlike the bar codes that are commonly used on items to distinguish a can of soup from a box of crackers, the EPC can identify a specific can of soup or box of crackers by its unique ID number.

Do all RFID systems use the EPC?

No, the EPC is a unique numbering system enabled by RFID and is mainly used on shipping cartons and pallets to track products from the manufacturer to the warehouse to delivery at the retail location. If individual items have tags with the EPC, the tags are usually on the packaging - on the box that contains the television a consumer buys, for instance, not on the television itself.

How can the EPC benefit consumers?

Convenience is also one of the biggest benefits of the EPC. It can also help merchants keep popular products from running out by tracking inventory and ordering re-supplies more quickly. Some shopping carts are being equipped with readers that will communicate with tags embedded on store shelves. When the consumer walks by, a small screen on the cart will display promotions, recipes, and other information connected with those products.

Safety is another benefit. For example, tagging prescription drug bottles with the EPC at the manufacturer can help pharmacies assure that the drugs they are providing to consumers are real, not counterfeit and that the prescription drugs being dispensed are those that the doctor prescribed. Stores can use RFID to locate and remove perishable items that are past their prime or recalled items from their shelves. RFID can also help protect the public health by enabling companies to track the source of an item - like a bag of spinach or beef from a cow, in case of disease.

What about my privacy?

Though few individual items are presently being tagged, the use of tags is growing. As RFID use becomes more widespread, it is important to know what information, if any, will be collected, how it will be used, if it will be stored and for how long, and whether it will be shared and with whom, especially if it is or can be linked to personal information about individuals.

Tags with chips programmed with the EPC to track items through the supply chain don't contain information about individuals. But as with barcodes today, it's possible that information about individuals could be linked to purchasing those items. For example when consumers use store loyalty cards to get sale prices, the retailer can keep track of the types of products they buy by linking the information from the barcodes on those items to the personal information those individuals may have provided when they signed up for the cards. With that information, retailers can track the spending habits of customers in a certain zip code, or send them advertisements for certain kinds of products.

In other uses of RFID technology, information about individuals may be stored on the chips in the tags. Again, the information on the chips may also be linked with information about individuals stored in databases connected to the system. Take the

toll-pass system - it's designed to collect information about where the tag was, and when, and links that data with information in a database about whose account to bill. This information could potentially be used in ways that may raise privacy concerns. For instance, an employer who installs a toll pass in a company car and monitors the charges made against the account could track where and when an employee has driven the car on toll roads.

How do I know if RFID is being used?

Because the tags can be so small, their use may not be readily visible. Sometimes they are embedded in items - for instance, tags are being built into new tires to monitor the tire pressure for safety purposes.

Items with tags that have chips containing the EPC are marked with a symbol that contains those letters, which indicates that the manufacturer participates in a voluntary program that requires it to disclose the use of RFID technology and follow certain practices to protect consumer privacy. The symbol will usually appear on the back of the package.

In other uses of RFID, there may be disclosures on signs in the store, on product labels, or in contracts and user agreements, or there may be no notice at all. There is no U.S. federal requirement to label RFID tagged items or to disclose that RFID is being used. Some states are considering laws concerning RFID, which may include requirements to disclose its use.

If RFID is being used, can I remove it or deactivate the tag if I choose?

That depends on how the tag is attached and how it is intended to be used. If it's embedded in an item, like a tire, it may not be possible to remove or deactivate it, or to do so without destroying the product. In other cases, removing it may be pointless. For example, if someone were to remove the RFID technology from the keyless remote for their car, it would become useless. If a tag can be easily removed or turned off, consumers may have that option.

In the case of tags with chips that contain the EPC, they are usually on the packaging and will be discarded with when the packages are thrown out. In some cases, a store clerk may remove a tag at the point of purchase, as is done now with the security tags on certain items, such as a DVD or clothing item.

If there is a choice about removing or disabling a tag, consider any benefits it provides and weigh them against any trade-offs you'd have to make. For example, if the tag is designed to make returning items easier, what is the return process without the tag? Are there other options? Is it possible to get the same or a similar item without the tag?

Also consider what privacy implications, if any, there may be in relation to the tag. Will any personal information be on the tag or linked to it? What type of information

is it and how will it be used? Is it possible to get the benefits without any personal information being linked to the tag? If the tag is used as part of a payment system or for another sensitive purpose, such as providing health records, is there adequate security to prevent it from being read or used without authorization? Look for explanations about privacy and security and ask questions to make informed decisions about using products with RFID.

Where can I get more information about RFID?

Information is available from these sources and consumers can search online for more resources about RFID.

Trans Atlantic Consumer Dialogue
Consumer and privacy issues related to using RFID
http://www.tacd.org/cgi-bin/db.cgi?
page=list&config=admin/docs.cfg&col_docsecid=4

Center for Democracy and Technology
Best practices for companies using RFID
http://www.cdt.org/privacy/20060501rfid-best-practices.php

EPCglobal
Guidelines for companies using the EPC
http://www.epcglobalinc.org/

EPCglobal US
Guidelines for U.S. companies using the EPC
http://www.epcglobalus.org/

FAQ menu

RFID Home

RFID
Radio Frequency Identification

Glossary of useful RFID terms

RFID Home

Active RFID tag: has its own small battery or other source of power and doesn't require power from the reader to send a signal to it.

Computer system: receives information about the item that is stored in the RFID tag.

Encrypting: turns information into a code that only authorized users can translate.

EPC: the Electronic Product Code. It's a unique identification code that is stored in the chip on an RFID tag as a product goes through the supply chain.

Interrogator: another word for a reader.

Passive RFID tags: don't have their own power source. The reader powers up the tag by sending it a radio signal, and the tag responds by sending radio signals back with the information about the item that the chip contains.

Reader: a device that is designed to pick up the radio signals from the RFID tag and deliver the information it contains to the computer system.

RFID: a wireless technology that is used to identify things.

RFID tag: consists of a microchip and a radio antenna. The chip in the tag contains information about the item that it is either attached to or embedded in. The tag transmits that information to the reader using radio signals.

Supply chains: the movement of products from a manufacturer to a distributor to a retailer and any points in between.

Transponder: another name for the RFID tag.

testimony, comments & speeches

NCL advocacy

CDT Working Group on RFID
Privacy Best Practices for Deployment of RFID Technology
Interim Draft
May 1, 2006

Introduction

Creative applications of radio frequency identification ("RFID") technologies hold promise for consumers, businesses and government. They suggest possibilities for reducing costs through better inventory management, for improving the safety of the drug supply, for aiding in the care of the elderly and impaired, for reducing error rates in hospitals and for improved tracking of luggage and cargo at airports to improve security and passenger service, among other applications.

There are many possible applications of RFID that do not pose major privacy concerns. But to the extent that RFID devices can be linked to personally identifiable information ("PII"), including where such devices facilitate the tracking of an individual's location, RFID raises important privacy questions. While this document is primarily intended to address these privacy implications, particularly with respect to control of PII, its goal is also to increase transparency about the use of RFID technology involving consumers.

What is RFID?

RFID refers to a technology that uses radio waves to identify an object. An RFID system typically includes three elements: a tag, a reader, and a database.

An RFID tag or transponder comprises a chip that contains a unique number that identifies an object (and perhaps other information) and is connected to an antenna. Each antenna enables the chip to communicate via radio waves to a reader, which captures the unique number or other data on the tag. That data can then be transmitted to computers that store information about the object to which the tags are attached. In most instances, the protocol for communication between the reader and tag enables a fixed set of commands; tags typically do not have the capacity to upload and execute additional software programs.

RFID Tags

The simplest RFID tags are "passive" and as such do not carry their own power supply to enable data transmission. Passive tags receive their power from the electromagnetic waves emitted by readers that induce a current in the tags, thereby enabling the transmission of the information stored on the tags. Other tags are "active" and do contain some form of power supply allowing the broadcast of information from the reader. Active tags are often able to transmit over a much longer range than passive tags - typically 100 feet or more. In comparison, passive tags have ranges that are minimal, in the range of several yards or less. There are even RFID tags designed to have a communication range of a few inches or less.

Both active and passive tags may be "dumb," without any capability of processing data on

board or "smart," having significant storage capacity that can support possible data security measures such as encryption, or including sensors for measuring conditions such as pressure or heat.

Readers and Read Range

RFID readers interrogate RFID chips to receive the identification number and other data. Readers interact with chips using varying radio frequencies. Low frequency readers and tags are less expensive than ultra high frequency readers and tags, use less power and penetrate non-metallic substances better. On the other hand, ultra high frequency tags can be read at a greater range from readers and can transfer data faster than their lower frequency counterparts. Both high and low frequency RFID systems have certain advantages over the more traditional bar code systems in that they can read objects within their range witnout line of sight access and can also read multiple objects at the same time, unlike the individual object scanning required by the bar codes systems.

Read range refers to the maximum distance an RFID chip can be accessed by a reader. Read ranges can vary widely: while some systems may have a read range of 100 feet, others may have a read range of only one or two inches. The read range designed into a particular RFID system is selected to serve the requirements of a specific application. In some cases, the desired read range is long, as in the case of inventory control or inventory tracking. In other situations, only an extremely short read range is necessary, and may in fact be preferable for security reasons.

Data and RFID Systems Networks

Finally, data may be transmitted over a network from the readers to business process applications, and to databases where information about the identified objects is stored.

The security of these networks is critical to the security of the overall RFID system. Depending on the sensitivity of the data within an RFID system, the data may be encrypted and include other security measures.[1]

The family of RFID technologies contains many sub-groupings with unique attributes and abilities that depend upon the various capabilities of the components of the technology, including the sophistication of the circuitry in the tags, the levels and sources of power involved, the communication protocols linking the tags and the readers, and the distance required between tags and readers for effective communication. Because different standards have developed for the varying uses of the tags, not every reader can read every tag.

Broadly speaking, RFID technology can be used for four general purposes: 1) to keep track of objects, 2) to keep track of people, 3) to provide services, or 4) as an internal component of a product or device.[2] Technical differences in the technology are reflected in its different applications.[3]

RFID and Privacy

RFID technology raises privacy concerns when its use enables parties to obtain personally identifiable information, including location information, about particular individuals that those parties otherwise would be unable or unauthorized to obtain. This information may be a person's location; it may be that the person has a certain product in his or her possession; it may be that the person has used a particular service. Security concerns arise if unauthorized parties are able to obtain such information either from interception of the radio

communications between tags and readers, through unauthorized reading of the tags, or via unauthorized access to the network or the database.

Detailed analysis of privacy and security issues in the context of these new technologies is clearly called for. Three general principles emerge from this analysis that can be applied to help address concerns about privacy in existing and new applications of RFID: the principle of technology neutrality; the principle of privacy and security as fundamental design requirements; and the principle of transparency.

Technology Neutrality: RFID technology in and of itself does not impose threats to privacy. Rather privacy breaches occur when RFID, like any technology, is deployed in a way that is not consistent with responsible information management practices that foster sound privacy protection.

Privacy and Security as Primary Design Requirements: Users of RFID technology should address the privacy and security issues as part of its initial design. Rather than retrofitting RFID systems to respond to privacy and security issues, it is much preferable that privacy and security should be designed in from the beginning.

Consumer Transparency: There should be no secret RFID tags or readers. Use of RFID technology should be as transparent as possible, and consumers should know about the implementation and use of any RFID technology (including tags, readers and storage of PII) as they engage in any transaction that utilizes an RFID system. At the same time, it is important to recognize that notice alone does not mitigate all concerns about privacy. Notice alone does not, for example, justify any inappropriate data collection or sharing, and/or the failure to deploy appropriate security measures. Notice must be supplemented by thoughtful, robust implementation of responsible information practices.

The Purpose of these Guidelines

Representatives from various consumer groups and commercial enterprises developed these guidelines under the leadership of the Center for Democracy and Technology ("CDT") in an effort to address current privacy concerns, as well as to limit future concerns regarding the deployment of RFID technology. This document is the result of an extensive analysis of current and near-term applications of RFID, the ways in which those applications do or do not implicate privacy, and the manner in which companies can address them. These guidelines have been designed at the principles level in consideration of the wide variety and versatility of current RFID systems, the breadth of applications, and the speed at which the technology is developing. This document is intended to provide guidance for policymakers, developers and users about privacy in the context of RFID technology.

To focus their discussions, the participants in this effort used the framework of fair information practices as articulated in the Organization for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data ("OECD Guidelines"). While this framework proved helpful to relate RFID technology to specific issues regarding electronic data flows, it became evident to the participants that many of the privacy issues related to RFID are common to any system of information collection and storage, while in other cases RFID does raise its own novel challenges. Thus, this document does not reflect a point-by-point application of the OECD Guidelines, but rather focuses on specific challenges posed by RFID technology when applying certain aspects of fair information practices in the areas of notice, choice and consent, onward transfers, access and security.

These guidelines are designed to be sufficiently flexible so as to apply across a range of

industry sectors. Their success will depend upon companies making sound decisions about how they are best implemented and maintained. We expect that some companies may, for example, provide notice in a way that differs markedly from the way in which others do, based upon the nature of a given RFID application, the company's business model, and the environment in which both are deployed. Thus, a retailer may provide notice in a manner different from the way in which a home health care system provider provides notice. It should also be noted that this document assumes that companies deploying RFID will comply with existing laws and regulations related to information collection and sharing.

This document is targeted at commercial and private sector consumer applications. It is not intended to address government applications of RFID or applications of RFID deployed internally by companies in the employer-employee context, business-to-business applications, or uses of RFID for personal identification systems.

The participants in this initiative are keenly aware that this guidance may need to be revisited as RFID technology continues to develop and as more is learned about its impact on privacy. For example, one issue that garners significant attention is whether and to what extent RFID practically could be used to track an individual's location. Issues such as location tracking, as well as others, will warrant reconsideration as the technology evolves and new applications emerge. As RFID technology and applications are developing rapidly, the drafters intend to review and refine the guidelines as the private sector gains experience in their implementation.

Finally, the purpose of this activity has been to attempt to define best practices. The process has involved extensive discussion about both principles and practicalities that entailed healthy give and take among parties representing widely different perspectives. Thus, while not every participant necessarily supports every recommendation, the final product represents a collective judgment that these guidelines should provide a workable set of practices that allow for realization of the potential benefits of RFID without undermining the privacy of consumers.

These guidelines are not designed as a blueprint for legislation. The participants in the drafting process believe that widespread and voluntary adoption of these guidelines, combined with a major effort at consumer education, would dramatically improve the environment for the use of RFID.

Best Practices
Notice

Consumers should be provided with clear, conspicuous and concise notice when information, including location information, is collected through an RFID system and linked, or is intended by a commercial entity to become linked, to an individual's personal information either on the RFID tag itself or through a database. (For purposes of this document, this information shall be referred to as "linked information.")

- In either of these situations, the notice should specify:
    - the presence of RFID involving linked information;
    - the purposes for which the linked information is being collected;
    - how linked information will be used;
    - whether the linked information is used solely to enable the functioning of the device the consumer has purchased or delivery of the service for which the consumer has contracted, or to facilitate completion of the commercial business's transaction with the consumer;
    - whether the linked information may be used for additional or subsequent uses, such as marketing;
    - that if the linked information is to be used for such additional or subsequent

uses, it will be used only consistent with the consumer's choice; and
    - o whether the RFID tag can be removed or deactivated.
- Whenever practicable, notice of the use of the RFID system to collect linked information should be provided prior to the completion of the transaction through which the good or service is obtained. In cases where there is no good or service obtained, then notice should be provided prior to the association of PII with information collected through the RFID system.

Responsibility for providing notice lies with the company having the direct relationship with the consumer.[4]

When the information on the RFID tag, such as the tag number, is not directly associated with an identified individual, in order to create a link between the information on the RFID tag and an identified individual it is usually necessary to access a series of databases or other information repositories.[5] It is the responsibility of the commercial entities involved in the deployment of RFID systems to exercise judicious discretion in determining whether the degree of linkage is sufficiently close so as to consider the information collected to be linked information.

- In general, commercial entities should consider the likelihood of the linkage between PII and/or location information and the RFID identification number in determining whether notice is necessary. In making this determination, a company should give good faith consideration to the following:
    - o The likelihood of a single individual or entity having access to all elements of information and databases necessary to effect the linkage;
    - o The number of elements of information required to effect the linkage;
    - o The security measures surrounding the information;
    - o Legal protections or safeguards applicable to accessing or using the information; and
    - o The sensitivity of the information linked to the RFID data.
- As the attenuation between the PII and RFID identification number becomes greater, the risk to privacy arguably decreases, and the requirement for notice becomes increasingly subject to discretion.

Consumers should be notified when entering a commercial or public environment where RFID technology is in use. Wherever practicable, individual RFID readers should be identified as such.

Companies should engage in annual internal assessments to confirm that the posted notices accurately reflect their information practices related to RFID systems.

Companies deploying RFID technology are strongly encouraged to participate in consumer education efforts that provide background and context to consumers regarding PII collection enabled by RFID, and to raise public awareness of the technology and its benefits.

Choice and Consent

Choice pertains to the use of the RFID technology, and to the uses of linked information collected on the RFID tag or associated with the RFID number.

Consistent with the guidelines for notice, consumers should be clearly notified when there is an opportunity to exercise choice with respect to the use of the RFID technology or with respect to the use of linked information collected on the RFID tag or associated with the RFID

number.

Consumers should be offered such choice before the conclusion of the transaction to obtain a good or service, wherever practicable, so that, when coupled with robust notice, consumers are given the tools to effectively exercise their choice with respect to the use of RFID technology.

- Consumer choice about the use of the RFID technology
  - The consumer should be informed in a clear, conspicuous and concise manner when there is an option to remove, de-activate, or destroy a tag and, when there is, how that option may be exercised.
  - In such instances, the option to remove, de-activate or destroy an RFID tag must be readily available to the consumer and readily exercised.
  - By exercising choice to remove, de-activate or destroy a tag, the consumer's ability to return an item, benefit from a warranty, or benefit from the protections of local law should not be compromised. Exercising this choice should not result in any damage or defect to a product.
- Choice and consent about the uses of PII collected on the tag or associated with the RFID number.
  - In some cases, linked information is used solely to enable the functioning of the device[6] the consumer has purchased or delivery of the service for which the consumer has contracted, or to facilitate completion of the commercial business's transaction with the consumer. In such instances, the consumer should be informed of the existence of the RFID tag (consistent with the provision on notice), but the consumer's consent or choice about the use of PII need not be solicited.

  When linked information collected and associated with an RFID number is used for purposes other than to enable the functioning of the device the consumer has purchased or delivery of the service for which the consumer has contracted, or to facilitate completion of the commercial business's transaction with the consumer (such as marketing or sharing linked information with a third party for some other purpose), the consumer should be so notified and given the opportunity to consent to such uses.

Responsibility for providing choice lies with the company having the direct relationship with the consumer. [7]

Onward Transfer

Wherever practicable, a company collecting PII via the deployment of an RFID system should include in its contracts provisions requiring that the companies with which it shares PII, including its affiliates, subsidiaries and any third party companies, will afford that shared data a level of protection consistent with or greater than that afforded by the company collecting the information.

Access

When PII is maintained on the tag itself, individuals should have reasonable access to that information.

If an individual receives an adverse decision based on linked information[8] about him or herself, that individual should have reasonable access to that information. As a general principle, it is desirable to provide consumers with, if cost effective and efficient, reasonable access to personally identifiable information, including location information, collected using RFID technology.

In the above situations, appropriate access should be provided by the entity interfacing with the individual.

When access is offered it should be easily and readily available to the consumer.

Government access to linked information should be allowed only upon service of process under applicable law.

Security

Companies should exercise reasonable and appropriate efforts to secure RFID tags, readers and, whenever applicable, any corollary linked information from unauthorized reading, logging and tracking, including any network or database transmitting or containing that information and radio transmissions between readers and tags. In addition, companies should exercise reasonable and appropriate efforts to secure the linked information from unauthorized access, loss or tampering.

In so doing, companies should establish and maintain an information security program in keeping with industry standards, appropriate to the amount and sensitivity of the information stored on their system. Such a security program should include processes to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of linked information, and address those risks.

To enhance the security of information that may be transmitted between tags and reader, companies should, to the extent practicable, minimize the information stored on RFID tags themselves.

American Library Association
aQuantive, Inc.
Center for Democracy & Technology
Cisco Systems Inc.
Eli Lilly and Company
IBM
Intel Corporation
Elliot E. Maxwell, RFID consultant and Fellow, Communications Program, Johns Hopkins University
Microsoft Corporation
National Consumers League
The Procter & Gamble Company
Verisign
Visa U.S.A.

---

[1] For example, many contact-less payment cards employ128-bit and triple DES encryption. In a payment transaction, a contact-less chip generates a unique numeric code. If the code is not detected, the transaction is declined.

[2] Examples of these purposes are plentiful. RFID systems are used to keep track of things in manufacturing inventory warehouses, for example, where deliveries can be recorded automatically by simply moving incoming pallets (with tags embedded) past a reader. The information is then logged into the inventory system. RFID systems keep track of people in hospitals and prisons and, in the future may be used for home health care applications that enable caregivers to monitor the daily habits of the very elderly or infirm in their homes. A familiar and early service application of RFID technology has been in toll-collection tags on highways, which allow motorists with RFID-enabled cards to pay tolls simply by passing through collection plazas. Contact-less payment cards are another service application. Additionally, RFID tags with a unique identifier are now an internal component of automobile keys; when the key is inserted in the lock, it communicates with a reader built into the car's electrical system.

[3] For example, the chip used to provide electronic bar codes has the capability to manage security via passwords and other safeguards and can be read at a distance of several feet. RFID tags used for contact-less smart cards, on the other hand, typically are designed to support substantial cryptography and to be read at distances of an inch or so; cryptography can be used to protect tags or to secure transmission protocols.

[4] Commercial entities that do not have a direct relationship with consumers but are involved with the deployment and/or use of RFID systems should make good faith efforts to encourage the notification of consumers. A commercial entity incorporating RFID systems within its products should give notice to its direct purchasers of that fact, and to the extent practicable encourage its direct purchaser to give similar notice to their purchasers, and so on, with the objective of enabling the company having the direct relationship with consumers to give proper notice of the use of RFID technology.

The rationale for this provision is that companies not participating in or benefiting from the use of RFID but who receive products containing tags may not know that products they receive contain RFID tags, and will need to have adequate information to participate in providing notice. Use of a well-recognized logo in accordance with corresponding guidelines, such as those followed by EPCglobal association members, would be one way to support this notification.

Where RFID tags in the retail environment function solely as a replacement for barcodes as currently deployed and do not provide enhanced or additional functions, notice may be provided consistent with current practice.

[5] For example, it would arguably require several linkages to correlate the RFID tag in an automobile tire to PII about the car's owner.

[6] For example, RFID may enable the function of an electronic device.

[7] Commercial entities that do not have a direct relationship with the consumer but are involved with deployment and/or use of the RFID system should make good faith efforts to encourage consumer choice.

A commercial entity which incorporates RFID systems in its products should inform its direct purchasers as to when a system includes RFID to help the purchaser assess whether the consumer should be offered choice and the opportunity to consent, and to the extent practicable encourage its direct purchaser to provide choice to its purchasers, and so on, with the objective of enabling the company having the direct relationship with the consumer to offer appropriate choice to consumers. Use of a well-recognized logo in accordance with corresponding guidelines, such as those followed by EPCglobal association members, is one means to support this notification.

[8] For example, an adverse decision related to the availability of a good or service, or the ability to obtain credit.

Stanford Law Review

Rights "Chipped" Away: RFID and Identification Documents

NICOLE A. OZER*

CITE AS: 2008 STAN. TECH. L. REV. 1
http://stlr.stanford.edu/pdf/ozer-rights-chipped-away.pdf

I. INTRODUCTION

¶1 In January 2005, parents from a small town named Sutter, California, an hour north of Sacramento, sent a letter to the offices of the American Civil Liberties Union (ACLU) of Northern California. Their daughters had come home from their public middle school with new identification badges 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.[1] 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.[2] But, in the past six years, RFID technology has been increasingly considered

---

* © 2007, Nicole A. Ozer, Technology and Civil Liberties Director at the ACLU of Northern California. The opinions expressed in this article are not necessarily those 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 much of the 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.

[1] See Press Release, Privacy Rights are at Risk—Parents and Civil Liberties Groups Urge School District to Terminate Use of Tracking Devices (Feb. 7, 2005), *available 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 for more information about Sutter. *See also* Press Release, Victory for Students, Parents and Civil Liberties Groups—Company Announces it will End Tracking Pilot Program (Feb. 16, 2005), *available 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; Greg Lucas, *Sutter County: Students Kept Under Surveillance at School*, S.F. CHRON., Feb. 10, 2005, at B1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/02/10/BAGG0B8I4D1.DTL; Kim Zetter, *School RFID Plan Gets an F*, WIRED, Feb. 10, 2005, http://www.wired.com/politics/security/news/2005/02/66554;

[2] Developing National Policies on the Deployment of Radio Frequency Identification (RFID) Technology, Feb. 17, 2006,

for use in government-issued identification documents like passports, driver's 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 have come into greater focus as government oversight organizations such as the Government Accountability Office ("GAO"), the Privacy Integrity Committee of the Department of Homeland Security, politicians, researchers, and industry organizations have looked more carefully at the risks of RFID and fostered critical debate about whether it is an appropriate technology for use in government-issued identification documents.

¶2 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.

II. RFID – WHAT IS IT?

¶3 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 being relatively well-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 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 the 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, 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

---

http://www.ieeeusa.org/policy/positions/rfid.html; *see also* Ass'n for Automatic Identification and Data Capture Tech., Shrouds of Time: The History of RFID, Oct. 1, 2001, http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf.

[3] *See* ACLU of Northern California, Don't Chip Our Rights Away!, http://www.aclunc.org/issues/technology/dont_chip_our_rights_away!.shtml (last visited Dec. 5, 2007).

[4] *See* Mary Catherine O'Connor, *Surveys Reveal Dubious Consumers*, RFID JOURNAL, Feb. 17, 2005, http://www.rfidjournal.com/article/articleview/1409/1/1/ (discussing 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) ("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.")

[5] Doug Farry, *Act Now! RFID Providers and Users Can Influence Public Policies That Impact the RFID Industry*, RFID JOURNAL, http://www.rfidjournal.com/article/articleview/2768/1/128/ (last visited Jan. 8, 2007) ("The [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.")

[6] Gene J. Koprowski, *Wireless Industry Defends RFID for Passports*, TECH NEWS WORLD, April 25, 2005, http://www.technewsworld.com/story/42349.html (noting that 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 . . ."); *see also* SMART CARD ALLIANCE, RFID TAGS AND CONTACTLESS SMART CARD TECHNOLOGY: COMPARING AND CONTRASTING APPLICATIONS AND CAPABILITIES 3, http://www.hidcorp.com/documents/tagsVsSmartcards_wp_en.pdf ("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.") (last visited Dec. 5, 2007).

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 chip does not alert anyone that it is transmitting this information or to what reader this information has been sent. On top of this foundational technology lie several permutations of RFID tags—"passive" tags, "active" tags, and "smart" tags.

¶4 "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 twenty feet, with others scientists demonstrating that they can be read at greater than sixty-nine 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.

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

¶6 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]

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

¶7 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.

---

[7] The Hitachi "Mu chip" is .4 mm square—small enough to be embedded in paper. Hitachi Corp., 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, http://www.hitachi.co.jp/Prod/mu-chip/ (last visited Oct. 5, 2007).

[8] U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT 6 (2005), *available at* http://www.gao.gov/new.items/d05551.pdf (noting that testing conducted by the U.S. State Department showed that smart cards with passive chips that had an intended read range of only four inches could actually be read from a distance six times as far—twenty-four inches—and could theoretically be read from more than three feet away). Scientists from Los Angeles-based Flexilis showed at DefCon in 2005 that passive RFID chips can be read at up to sixty-nine feet. Brian Krebs, *Leaving Las Vegas. So Long DefCon and Blackhat*, SECURITY FIX, Aug. 1, 2005, http://blog.washingtonpost.com/securityfix/2005/08/leaving_las_vegas_so_long_defc.html. It has also been reported that readers can "eavesdrop" on legitimate reader-to-card communications from a distance of 30 feet. *See* Heydt-Benjamin et al., RFID Payment Card Vulnerabilities Technical Report, Oct. 11, 2006, http://www.nytimes.com/packages/pdf/business/20061023_CARD/techreport.pdf.

[9] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 8, at 7-8.

[10] Very generally, cryptography is the procedure to translate data written in plain text into cipher text, coded text that requires access to a key or password 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 Part III for a discussion of some of the vulnerabilities of "smart" tags.

[12] Hahn Kim Quach, *ID Tech on Fast Track—For Better or Worse*, ORANGE COUNTY REG., Aug. 7, 2005, *available at* http://www.ocregister.com/ocr/sections/news/news/article_625690.php.

A. Mass-Distributed Building Entry Card System Cracked

¶8 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 twenty dollars 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 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]

B. British E-passports Cracked

¶9 In November 2006, the technology protections on three million British e-passports were cracked by software written in less than forty-eight hours and an RFID reader bought for about five hundred dollars.[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, the passport holder's date of birth, and the expiration date.[17] Once this not-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 their technological protection measures. The British government apparently chose not to do so.[18] According to Adam Laurie, the computer expert who helped crack the e-passport, the protections put in place to protect this

---

[13] Flash video: RSA: Door Cards—The Enterprise's Weakest Link, http://www.infoworld.com/video/archives/2007/02/rsa_ioactive.html (interviewing Chris Paget demonstrating the RFID cloner at the RSA Security Conference).

[14] *See* Paul F. Roberts, *Black Hat Dispute Stirs RFID Security Awareness*, INFOWORLD, Feb. 28, 2007, http://www.infoworld.com/article/07/02/28/HNblackhatrfid_1.html, *see also* Brian Krebs, *RFID Flap Silences Security Researchers*, SECURITY FIX, Feb. 27, 2007, http://blog.washingtonpost.com/securityfix/2007/02/legal_threat_silences_rfid_sec.html; Robert Lemos, *Legal Threats Scuttle RFID Flaw Demo*, SECURITY FOCUS Feb. 27, 2007, 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 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 its 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." Larry Greenemeier, *Security Researchers and Vendors Clash at Black Hat, Users Lose*, INFORMATION WEEK, Feb. 28, 2007, http://www.informationweek.com/story/showArticle.jhtml?articleID=197700101. 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 (February 28, 2007) *available at* http://www.aclunc.org/news/press_releases/hid_threatens_patent_lawsuit,_silences_important_rfid_presentation_at_national_conference.shtml.

[15] Flash Video: RSA: Door Cards—The Enterprise's Weakest Link, *supra* note 13.

[16] Steven Boggan, *Cracked It!*, GUARDIAN UNLIMITED, Nov. 17, 2006, http://www.guardian.co.uk/idcards/story/0,,1950226,00.html.

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

[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. Ari Juels et al., Security and Privacy Issues in E-passports at 1 (2005), http://eprint.iacr.org/2005/095.pdf. Active Authentication is detailed in the ICAO PKI Technical Report. Int'l Civil Aviation Org., PKI for Machine Readable Travel Documents Offering ICC Read-Only Access at 15-16, 2004, http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf. For more information about the history of the e-passport, see Am. Civil Liberties Union, Naked Data: How the U.S. Ignored International Concerns and Pushed for Radio Chips in Passports Without Security (2004), http://www.aclu.org/privacy/spying/15780res20050426.html.

sensitive information were the equivalent of "installing a solid steel front door to your house and then putting the key under the mat."[19]

C. RFID-embedded Credit Cards Cracked

¶10 In October 2006, researchers at the University of Massachusetts Amherst demonstrated a technique for intercepting the information being transmitted by an RFID-embedded credit card; tens of millions of similar cards have been issued.[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 for 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.

D. California Capitol Entry Cards Cracked

¶11 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 investment in concrete barricades, posts, and other security measures to secure the California State Capitol, 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 Assembly member Fran Pavley, he gained access to the California State Capitol.[23]

E. Dutch E-passport Prototype Cracked

¶12 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]

F. VeriChip Human-implantable RFID Cracked

¶13 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]

---

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

[20] John Schwartz, Researches See Privacy Pitfalls in No-Swipe Credit Cards, N.Y. TIMES, Oct. 23, 2006, at C1.

[21] *See id.* ("American Express has 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.'").

[22] ABC 7 News: Cloning RFID Tags in Sacramento (ABC television broadcast Aug. 2006), available at http://www.youtube.com/watch?v=4jpRFgDP[illegible]

[23] *Capitol building to be ringed with barricades*, SILICON VALLEY/SAN JOSE BUSINESS JOURNAL, *available at* http://www.bizjournals.com/sanjose/stories/2002/03/18/daily35.html. 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, Feb. 3, 2006, http://www.engadget.com/2006/02/03/dutch-rfid-e-passport-cracked-us-next/.

[25] The Dutch e-passport, also based on the ICAO standard, also failed to incorporate additional optional technological protections such as active authentication. For more information, see discussion infra Part III.B.

[26] Annalee Newitz, *The RFID Hacking Underground*, WIRED, May 16, 2006, http://www.wired.com/wired/archive/14.05/rfid_pr.html; Susan Kuchinskas, *The New Chip-erati*, INTERNETNEWS.COM, Feb. 6, 2006, http://www.internetnews.com/security/article.php/3582971

While the VeriChip corporate website still claims that its tags are "safe," "secure," and "cannot be counterf[illegible]," Westhues was able to read and clone the chip in the arm of a *Wired News* reporter in mere ho[illegible]th 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 twenty dollars 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 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.

G. RFID Gas Cards and Car Keys Cracked

¶14 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 successfully cracked the encryption code on the Texas Instruments chips in thirty 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 to 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 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]

IV. 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]

¶15 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, by independent researchers who specialize in RFID technology, and even by segments of the technology industry itself.[35]

---

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

[28] *See* VeriChip RFID 101, http://www.verichipcorp.com/content/company/rfid101 (last visited Oct. 8, 2007).

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

[30] *See* VeriChip's Company Page, http://www.verichipcorp.com/company.html (last visited Oct. 8, 2007).

[31] Peter Weiss, *Outsmarting the Electronic Gatekeeper: Code Breakers Beat Security Scheme of Car Locks, Gas Pumps*, SCIENCE NEWS ONLINE, Feb. 5, 2005, http://www.sciencenews.org/articles/20050205/fob8.asp.

[32] Robert Vamosi, *Gone in 60 Seconds—The High Tech Version*, CNET NEWS, May 8, 2006, http://news.com.com/2100-7349_3-6069287.html.

[33] Jack M. Germain, *RFID Technology Faced with Privacy Considerations*, E-COMMERCE TIMES, July 11, 2005, http://www.ecommercetimes.com/story/44406.html

[34] Matthew Kazmierczak & Josh James, RFID: Security, Privacy, and Good Public Policy, http://www.aeanet.org/publications/idjj_rfid_grad_overview.asp (last visited Oct. 8, 2007).

[35] Neville Pattinson, director of Technology & Government at Axalto Inc. of Austin, Texas, commented at the June 7, 2006

A. Tracking and Profiling: Concerns Expressed by Diverse Groups

¶16 **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]

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

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

1. Government Accountability Office (GAO)

¶19 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 on 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]

DHS Data Privacy and Integrity Advisory Committee that "[i]t's inappropriate to use RFID technology for tracking and authenticating identities of people." He further noted, "[y]ou 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, May 19, 2006, http://www.identityblog.com/?p=451.

[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. *See* Westhues' Home Page, http://cq.cx/prox.pl (last visited Oct. 8, 2007) (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.

[37] Kelly Shermach, *Legoland RFID Tracks Lost Kids, Collects Data*, CRMBUYER, Oct. 28, 2004, http://www.crmbuyer.com/story/Legoland-RFID-Tracks-Lost-Kids-Collects-Data-37694.html, *see also* Justin Matlick, *Technology (A Special Report): Consumer Technology*, WALL ST. J., Apr. 25, 2006, at R11.

[38] *See* Shermach, *supra* note 37.

[39] RFID in Japan, Sept. 11, 2006, http://ubiks.net/local/blog/jmt/archives3/005739.html.

[40] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 8.

[41] *See id.*

¶20 The GAO continued by stating that "[a]mong the key privacy issues are notifying individuals of the use or existence of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing for secondary uses of information."[42] The GAO expanded on its concerns with tracking and profiling. It cautioned that:

> [t]he 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]

2. Department of Homeland Security Data Privacy and Integrity Advisory Committee

¶21 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, the Committee 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 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, the Committee 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 fewer privacy and security risks.[47]

3. Institute of Electrical and Electronics Engineers (IEEE)

¶22 The Institute of Electrical and Electronics Engineers, a nonprofit group representing more than 220,000 U.S. electrical, electronics, computer, and software engineers, has also expressed serious worries about the privacy and tracking issues associated with the use of RFID in identification documents. In its position paper adopted by the Board of 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."[48] It advised that "[t]he 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."[49] The IEEE was also very concerned about information being used for secondary purposes unrelated

---

[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, data interoperability and other privacy related issues. For more information, see HOMELAND SECURITY, PRIVACY OFFICE—DHS DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE (Aug. 13, 2007), *available at* http //www.dhs.gov/xinfoshare/committees/editorial_0512.shtm.

[45] DEPARTMENT OF HOMELAND SECURITY, THE USE OF RFID FOR HUMAN IDENTITY VERIFICATION, Report No 2006-02 (2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID pdf.

[46] THE USE OF RFID FOR HUMAN IDENTIFICATION, DHS (DRAFT) 7, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf

[47] DEPARTMENT OF HOMELAND SECURITY, *supra* note 45.

[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." Developing National Policies, *supra* note 2.

[49] *Id.*

to the original reason for carrying or using the RFID-embedded card, without the knowledge of the cardholder: "[b]ecause 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."[50]

4. Industry Representatives

¶23 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,[51] explained that EPC 2 Global tags, a basic form of RFID technology that lacks additional multilayered protections, "was designed to track packages and products" and "is not the appropriate technology to use for securing human identification systems."[52] The Smart Card Alliance confirmed that 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."[53] 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."[54] 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."[55]

¶24 The AeA and leading technology companies have also echoed the concerns that core RFID technology does not adequately protect privacy. In a 2006 letter to the Department of State and Department of Homeland Security regarding what type of machine-readable technology should be deployed in the new Western Hemisphere Travel Initiative ("WHTI") card, the trade organization and companies explained that basic RFID designed for identifying pallets of goods and allowing rapid inventory tracking is "inappropriate for personal identification applications."[56] 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."[57] The information on the tag could also be "surreptitiously skim[med]."[58] 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."[59]

5. Elected Officials

¶25 Elected officials are also becoming increasingly alarmed about the implications of RFID technology used in identification documents. Senator Hillary Clinton (D-NY) submitted a letter to

---

[50] *Id.*

[51] The Smart Card Alliance is a membership organization that "includes over 150 U.S.-based and international organizations covering the full spectrum [of] industry suppliers, integrators, and end user groups." Smart Card Alliance Activities: Overview, http://www.smartcardalliance.org/pages/activities (last visited Nov. 11, 2007).

[52] Smart Card Alliance, Comments on the Smart Card Alliance to the Department of State Federal Register Notice, Nov. 3, 2006, at 3, http://www.smartcardalliance.org/resources/pdf/Smart_Card_Alliance_Response_Passport_Card_Final.pdf.

[53] Smart Card Alliance Identity Council, Contactless Smart Cards vs. EPC Gen 2 RFID Tags: Frequently Asked Questions, July 2006, at 5, http://www.smartcardalliance.org/resources/pdf/EPC_Gen_2_FAQ_FINAL.pdf.

[54] Press Release, Proposed Passport Card with RFID Technology Bad News for Privacy and Security, Says Smart Card Alliance, (Oct. 19, 2006), http://www.marketwire.com/mw/release.do?id=708412.

[55] Smart Card Alliance Identity Council, *supra* note 53, at 5.

[56] This January 30, 2006 letter was 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. Letter from AeA to Department of State and Department of Homeland Security, RE: Privacy and Security Concerns with the use of EPCglobal UHF Generation 2 technology in the Western Hemisphere Travel Initiative Card Program, Jan. 30, 2006, http://www.aeanet.org/governmentaffairs/AeA_Letter_Jan_30_2006.asp.

[57] *Id.*

[58] *Id.*

[59] *Id.*

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.[60] Senator John Sununu (R-NH) and Senator Daniel Akaka (D-HI) have also proposed legislation to address the possible technological implications of potential widespread use of RFID technology in ID documents like driver's licenses, and the security risks associated with databases that might be built as a result.[61] State representatives around the country have introduced more than fifty bills in twenty-seven states addressing privacy and security implications of RFID technology use by the government and commercial sectors.[62]

B. Insecure RFID Technology Interferes with Constitutional Rights

¶26 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 widespread impact on privacy and free speech rights. Such rights are not aspirational, but are guaranteed by both the United States Constitution and further augmented by many state constitutions.

1. Insecure RFID Impacts Privacy Rights

¶27 Privacy rights are guaranteed by the Fourth Amendment to the United States Constitution and many state constitutional provisions.[63] 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—it also protects places or things that a person "seeks to preserve as private, even in an area accessible to the public."[64] The use of insecure RFID technology in government identification documents interferes with Fourth Amendment rights by facilitating unreasonable searches.

2. Insecure RFID in Government IDs Facilitates Unreasonable Search

¶28 The use of insecure RFID in government identification documents facilitates unreasonable searches. A search violates the Fourth Amendment if the government violates a subjective expectation of privacy that society recognizes as reasonable.[65] The inquiry involves two discrete questions: (1) has the individual, by his or her 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.[66]

¶29 Individuals take actions to preserve the privacy of the personal information on government identification documents, and their expectation of privacy for 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

---

[60] Alice Lipowicz, *Clinton: PASS Card Initiative Needs 'Rigorous' Review*, GOVERNMENT COMPUTER NEWS, Dec. 19, 2006, http://www.gcn.com/online/vol1_no1/42815-1.html

[61] Renee Boucher Ferguson, *Senators Question Use of RFID in E-Passports, National ID Cards*, EWEEK, Dec. 15, 2006, http://www.eweek.com/article2/0,1759,2073670,00.asp.

[62] Am. Legislative Exch. Council, RFID State Legislative Activity, Oct. 2006, http://downloads.heartland.org/20144.pdf.

[63] "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." U.S. CONST. amend. IV. The states of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington have explicit constitutional privacy provisions. National Conference of State Legislatures, Privacy Protections in State Constitutions, http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm (last visited Nov. 11, 2007). The District of Columbia also includes an explicit privacy provision in its code. D.C. CODE, § 1-4 (2001). The California privacy provision will be discussed later in more depth.

[64] Katz v. United States, 389 U.S. 347, 351 (1967) (reversing Olmstead v. United States, 277 U.S. 438 (1928)) (holding that a wiretap of a public telephone violated the Fourth Amendment).

[65] Kyllo v. United States, 533 U.S. 27, 33 (2001).

[66] *Katz*, 389 U.S. at 361.

safely away from view in wallets and purses.[67] This information, hidden away, cannot be read and recorded by law enforcement with mere observation. Individuals must either be stopped and forced to produce their identification documents, or technology must be utilized to penetrate an individual's pocket or purse to 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.

¶30 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 explicit authority to law enforcement to require individuals to display their driver's licenses for identification purposes.[68] However, initial stops of individuals, which then lead to requests by law enforcement to display identification, must still be based on reasonable suspicion.[69] Thus, the default position is that individuals, absent reasonable suspicion by law enforcement, have control over their personal information and the disclosure of their identities. 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.[70] 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.

¶31 The Supreme Court has long found Fourth Amendment protection against searches that cannot 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."[71] 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 would otherwise require physical intrusion into the home in order to discern—was also a search prohibited by the Fourth Amendment. 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."[72] 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 considered equally because the technology 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, facilitates law enforcement actions that are tantamount to unreasonable stops, and enables unreasonable search.

---

[67] 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 a 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) (holding that 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, RFID should be distinguished and found to implicate the Fourth Amendment.

[68] *See* VA. CODE ANN. § 46.2-104 (2007); WASH. REV. CODE ANN. § 46.20.037 (LexisNexis 2007); IDAHO CODE ANN. § 49-316 (2007).

[69] Hubel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 184-185 (2004) (interpreting stop and identify statute and finding that Fourth Amendment was not violated by requiring individuals to reveal identity to police officer in the course of reasonable stop under Terry v. Ohio, 392 U.S. 1 (1968) (holding that police 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).

[70] CAL. CIV. CODE § 1798.90.1 (Deering 2007).

[71] Bond v. United States, 529 U.S. 334, 337 (2000).

[72] *Kyllo*, 533 U.S. at 40.

3. Insecure RFID Implicates State Constitutional Protections

¶32 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 information 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.[73] Overwhelmingly approved by 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."[74] In *White v. Davis*, the first California Supreme Court to interpret the privacy amendment noted:

> [T]he 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 most modern threat to personal privacy.[75]

¶33 State constitutional protections, like those 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.

4. Insecure RFID Technology Impacts Rights to Free Speech

¶34 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 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."[76] 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 monitored surreptitiously and records were maintained about their activities. From political speech to daily activities, once individuals think they could be "observed and recorded, their habits change; they change."[77]

¶35 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; the same is true for laws requiring identification of a person's association with others or with organizations. Individuals have a right to protest, distribute leaflets, and circulate petitions anonymously,[78] and it is improper to force disclosure of membership

---

[73] The election brochure provides insight into the legislative history of the amendment. *See* White v. Davis, 13 Cal. 3d 757, 773-775 (1975).

[74] *Id.* at 774.

[75] *Id.*

[76] Richard Wasserstrom, Privacy: Some Arguments and Assumptions, 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).

[77] 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 76, at 244.

[78] Buckley v. Am. Constitution Law Found., 525 U.S. 182 (1999) (striking down Colorado's requirement that petition

lists.[79] 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 free speech and the right of association.[80] 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."[81] The use of insecure RFID in identification documents is inappropriate because of its chilling effect on the exercise of free speech.

¶36 **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.[82]

¶37 As the editors of *Scientific American* wrote in response to learning about the use of RFID tags in student badges in Sutter, California, "tagging 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."[83]

¶38 **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 to access 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 over the disclosure of their personal information, and the use of RFID technology in identification documents threatens this ability.

¶39 **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

---

solicitors 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")

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

[80] *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).

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

[82] Article 13 of the UN Declaration of Human Rights: "Everyone has the right to freedom of movement." Universal Declaration of Human Rights (1948), available at http://www.un.org/Overview/rights.html.

[83] Editorial, *Human Inventory Control*, SCIENTIFIC AMERICAN (May 2005), *available at* http://www.sciam.com/article.cfm?articleID=00093B44-71DB-1264-B1DB83414B7F0000&sc=I100322.

laptop, as was done by Jonathan Westhues at the Sacramento Capitol, or cloning the card by taking the information and encoding it on another chip in a new card.

¶40 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.[84] Basic RFID technology simply "does not support the necessary security safeguards to allow border officials to verify that the passport card is authentic."[85] 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.[86]

> 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.[87]

¶41 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."[88] Succinctly stated by Marc-Anthony Signorino, Director and Counsel for Technology Policy, AeA, "[i]f it doesn't keep the bad guys out, if it's easily spoofed, then what good is it?"[89]

¶42 **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 number, 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.

¶43 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 $6000 dollars, total losses of more than $56 billion dollars, and a cost of 40 hours of time per person to make claims and resolve losses, identity theft already impacts a significant segment of the American population.[90] So, what advice did the largest study on identity theft provide to consumers to try to stem the rise of

---

[84] "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, http://www.smartcardalliance.org/alliance_activities/whti.cfm (last visited Jan. 8, 2007).

[85] Proposed PASSport card with RFID technology bad news for privacy and security, says Smart Card Alliance, *supra* note 54.

[86] Letter from AeA to Frank E. Moss, Deputy Ass't Sec'y, Passport Services, and Elaine Dezenski, Acting Ass't Sec'y, Border and Transp. Sec. Policy (Jan. 30, 2006), *available at* http://www.aeanet.org/governmentaffairs/AeA_Letter_Jan_30_2006.asp.

[87] *Id.* (emphasis added)

[88] *Id.*

[89] Michael Arnone, *Beaming across the Border*, FEDERAL COMPUTER WEEK, Apr. 24, 2006, http://www.fcw.com/article94156-04-24-06-Print.

[90] 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 6383, total of $56.6 billion.

Press Release, New Research Shows Identity Fraud Growth Is Contained and More Control Than They Think (Jan. 31, 2006), *available at* http://www.bbbonline.org/IDtheft/safetyQuiz.asp (last visited January 8, 2007).

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."[91] 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. . . . These security problems are simply inherent in the technology."[92] 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.[93] This is because a majority of identity theft occurs through lost or stolen wallets, credit cards, and check books and many people can determine when and how their information was accessed by another individual.[94] Since RFID technology does not alert an individual to 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.[95]

V. IMPACT OF SURVEILLANCE INFRASTRUCTURE

¶44 The privacy and security concerns associated with RFID technology itself are magnified by 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 fifty-state interlinked database) the new e-passports, the Western Hemisphere Travel Initiative, and travel databases such as the Automated Tracking System ("ATS").[96] By accumulating and aggregating countless individual points of data, these technologies, identification systems, and databases threaten to allow the government—and potentially others—to invade the privacy of individuals at an unprecedented scale.

¶45 **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 driver's licenses pursuant to the Real ID Act. The Department of Homeland Security's draft regulations for Real ID recommended selection of a 2-D barcode that is scanned optically as the common machine-readable technology to replace the

---

[91] *Id.*

[92] Paul Faber, *RFID Strategy—RFID Privacy And Security Issues: A look at the evolving state of tag security*, INDUSTRY WEEK, Jan. 9, 2007, *available at* http //www industryweek com/ReadArticle aspx?ArticleID=13371&SectionID=4

[93] Forty-seven percent of victims could identify the source of the data compromise. Thirty-six percent of victims could identify the person who misused their information. New Research Shows Identity Fraud Growth Is Contained and More Control Than They Think, *supra* note 90

[94] In sixty-three percent 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 checkbooks, breached home computers or stolen mail or trash. Trash as a source of data compromise is now less than one percent. *See id.*

[95] *Id.*

[96] For more information about the Real ID Act, see Real Nightmare, http://www.realnightmare.org (last visited January 8, 2007). For more information about WHTI, see Press Release, ACLU and Allies Oppose Western Hemisphere Travel Initiative, Say Plan Undermines Privacy, Provides Little Security (Sept. 7, 2006), *available at* http://www.aclu.org/safefree/general/26681prs20060907 html For more information about ATS, see Press Release, Government Secretly Tracks Millions of Americans, ACLU (Dec. 1, 2006), *available at* http //www.aclunc org/news/press_releases/government_secretly_tracks_millions_of_americans shtml

magnetic strip that is used on many licenses today.[97] 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 driver's licenses and identification cards to be routinely read at a distance."[98] However, RFID passports continue to roll out and other RFID travel documents are in the pipeline.[99]

A. RFID Passports

¶46 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.[100] 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.[101] The United States government 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.[102] 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.[103] As predicted, e-passports issued by other countries under the same international e-passport standards have already been compromised, 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.

B. Western Hemisphere Travel Initiative

¶47 The federal government is also in the process of creating a new RFID-embedded travel document, the People Access Security Service ("PASS") card.[104] This new document is being

---

[97] 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) 76, *available at* http://www.aclu.org/images/general/asset_upload_file993_28735.pdf

[98] *Id.*

[99] 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 sixteen. 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 2-D 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 twenty-eight states to modify the Real ID Act.

More information is available at http://www.realnightmare.org.

[100] RFID-embedded passports started issuing on August 16, 2006.

Press Release, Department of State Begins ... ing Electronic Passports to the Public (Aug. 14, 2006), *available at* http://www.state.gov/r/pa/prs/ps/2006/70432.htm

Information about the e-passports is available here: http://travel.state.gov/passport/eppt/epptnew_2807.html.

[101] *See* ACLU, Naked Data: How the U.S. Ignored International Concerns and Pushed for Radio Chips in Passports Without Security (Nov. 24, 2004), *available at* http://www.aclu.org/pdfs/privacy/nakeddata20041124.pdf.;

ACLU, Global Identity Cards, Apr. 26, 2005, http://www.aclu.org/privacy/spying/15780res20050426.html.

[102] *Are E-Passports More Secure?*, WALL ST. J., Sept. 29, 2006, *available at* http://online.wsj.com/public/article/SB115938787873075826-6AbUpMIaJVCS1i_UBVoGrWP867k_20070929.html.

[103] The metal shielding that has been woven into the cover to stop the information from being read—since radio waves do 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, and have 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 is only what has been uncovered in the short time these chips have been available, who knows what will happen in the ten-year lifespan of the chips now being used? *See id.*

[104] Laurie Sullivan, *New Border-Crossing Card Could Boost RFID Demand*, INTELLIGENT ENTERPRISE, Sept. 7, 2006,

developed pursuant to the Western Hemisphere Travel Initiative ("WHTI"), which requires that all people traveling between the United States and Mexico, Canada, Bermuda, and the Caribbean show a passport or other DHS-approved document.[105] Starting 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.[106]

C. RFID and Video Surveillance

¶48 The further use of RFID technology in government identification documents, combined with ever-growing public surveillance systems, presents particularly grave concerns. Public surveillance cameras are proliferating throughout the United States, funded in part by $800 million in grants from the Department of Homeland Security.[107] 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 over two years, the San Francisco "pilot program" with two video surveillance cameras has grown to over sixty cameras, with plans to seek DHS funding in the coming years.[108] Chicago Mayor Richard M. Daley expects cameras to be on "almost every block" of his city by 2016.[109]

¶49 The video surveillance market is expected to be a $9 billion industry by 2011.[110] 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."[111] The coupling of RFID technology with the proliferation of national identification documents means that that the government is more likely to be able to confirm the identity of an individual coming into the range of a camera and to access a wealth of information about that person—likely anything stored in a computerized database—including such personal information as motor vehicle records, police records, employment history, travel and buying habits, and DNA and drug testing records.[112]

VI. THE SYMBOL OF SUTTER

¶50 The RFID security vulnerabilities that have come to light, the research and policy papers completed by both government agencies and academic institutions, and the admissions by segments of the technology industry itself that basic RFID technology allows for tracking individuals and

---

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

[105] For a thorough discussion of WHTI and the privacy and security impact of the PASS card, see Katherine Walkenhorst, *Border Security: PASS Card Fails on Cost, Privacy* 4 (Sept. 7, 2006), *available at* http://www.cagw.org/site/DocServer/WHTI_Report__2_.pdf?docID=1721

[106] Alice Lipowicz, *Alliance: NIST Smart Card Evaluations Insufficient*, GOVERNMENT COMPUTER NEWS, May 24, 2007, *available at* http://www.gcn.com/online/vol1_no1/44338-1.html.

[107] Martha T. Moore, *Cities Opening More Video Surveillance Eyes*, USA TODAY, July 18, 2005, at 3A (also mentioning an additional $1 billion in money available through state grants).

[108] For more information about public video surveillance, see Nicole Ozer & Mark Schlosberg, Under The Watchful Eye: The Proliferation of Video Surveillance in California, Aug. 2007, http://www.aclunc.org/docs/criminal_justice/police_practices/Under_the_Watchful_Eye_The_Proliferation_of_Video_Surveillance_Systems_in_California.pdf

[109] Fran Spielman, *Daley: By 2016, Cameras on 'Almost Every Block'*, CHI. SUN TIMES, Oct.12, 2006, at 22.

[110] *Networking/IP to drive video surveillance market growth, says iSuppli*, TEKRATI, Mar. 20, 2007, http://semiconductors.tekrati.com/research/news.asp?id=8608

[111] Moore, *supra* note 107.

[112] 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 . . . " For more information, see Choicepoint, Mar. 14, 2006, http://www.epic.org/privacy/choicepoint/.

cloning tags all point to the fact that it is a risky technology to use in identification documents. The public's distrust of RFID technology, particularly when utilized by the government, is also prevalent and growing.[113] However, RFID technology is still being considered for more and more uses by the government and private sector. Why?

A. Privacy and Security Issues Not Properly Considered

¶51 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 Government Accountability Office found that only one of the sixteen federal agencies that responded to its 2005-2006 survey seemed aware that the use of RFID technology may give rise to legal issues such as its impact on privacy and tracking.[114]

B. Concerns Dismissed as Exaggerated and Paranoid

¶52 Industry and the government have also often tried to dismiss the concerns of individuals like the parents in Sutter and of national organizations such as the ACLU, saying that the worries and concerns are "often exaggerated."[115] 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 United States government has quietly tried to dismiss the concerns of other nations and the ACLU about the privacy and security of the new RFID-embedded passports.

C. RFID is Big Money; Relationships between Industry and Decision-Makers

¶53 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 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. The RFID market is expected to rocket 120% just between 2007 and 2009.[116] Access cards for the financial, security, and safety markets are the key volume applications for RFID technology.[117] Americans are paying for this RFID technology and fueling growth in the market not just with tax dollars, but also with the loss of their privacy, personal safety, and financial security.

---

[113] According to the RFID Consumer Buzz report, a quantitative survey conducted during December 2004 and January 2005 of more than 7000 consumers and also focus groups, "concerns over the use of RFID technology are still 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." O'Connor, *supra* note 4.

[114] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 8, at 17.

[115] AeA says the concerns are "often exaggerated." Kazmierczak, *supra* note 34, at 1. The parents in Sutter were thought by some of their neighbors to be engaged in "unfounded paranoia." William Dean Hinton, *Spy Hunter: A South Bay Legislator Is Trying to Jam the Emerging Use of RFID Technology for Personal Tracking*, METRO, Sept. 7, 2005, http://www.metroactive.com/papers/metro/09.07.05/rfid-0536.html.

[116] Robert Jaques, *RFID Set for Growth Explosion*, VUNET.COM, Feb. 28, 2005, http://www.vnunet.com/vnunet/news/2126853/rfid-set-growth-explosion.

[117] *RFID Market to Reach $7.26Bn in 2008*, IDTECHEX, Apr. 10, 2005, http://www.idtechex.com/products/en/articles/00000169.asp. 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.

¶54 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 was appointed to the board of directors of RFID maker and DHS contractor Savi Technology.[118] He stated at a conference that "RFID will make us safer" and that government tests of using RFID to identify passengers and cargo at airports were a "success" and that the "Feds will safeguard the data gathered."[119] Tommy Thompson, the former Secretary of Health and Human Services under President George W. Bush, was appointed to the board of Applied Digital, the manufacturer of the human-implantable RFID tag (the "VeriChip").[120] 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 elementary school were actually teachers at the high school. They provided the RFID systems for free to the school and gave the school a donation of "a couple thousand dollars."[121] The company also promised to give royalties to the school district for future sales of the product to other schools.[122] 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 answered the questions of concerned parents at school board meetings, was (or would soon be) a lobbyist for the RFID company.[123]

¶55 Because privacy and security issues are overlooked, concerns are often dismissed, and money and relationships often make good decisions about privacy and security more difficult, the privacy and security issues concerning RFID in identification documents should not be "worked out" on a case-by-case basis. They are often "worked out" to the detriment of the privacy, personal safety, and financial security of individuals.

VII. PROBLEMS IN NEED OF SOLUTIONS

¶56 Legislators are starting to heed the necessity of taking action to protect the privacy, personal safety, and financial security of their constituents by introducing RFID bills. In the last several years, over fifty RFID bills have been introduced in over thirty states.[124] 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 recently reintroduced, 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.[125]

A. Identity Information Protection Act

¶57 The Identity Information Protection Act protects all state-issued documents, such as driver's licenses and government health and other benefit cards, with adequate levels of security to ensure that people are able to decide who can access their information and when. It also requires that all people are given notice about the technology and the location of the RFID readers. The bill is a straightforward example of the type of solution discussed by security professionals like those from

---

[118] Koprowski, *supra* note [illegible]

[119] *Id.*

[120] Press Release, Applied Digital, VeriChip Corporation Appoints Former Secretary of Health & Human Services and Former Governor of Wisconsin Tommy G. Thompson to Its Board of Directors (July 7, 2005), *available at* http://www.adsx.com/pressreleases/2005-07-07.html

[121] Zetter, *supra* note 1.

[122] Catherine Komp, *Parents Fight 'Demean...' School Tracking Technology*, THE NEW STANDARD, Feb. 14, 2005, http://newstandardnews.net/content/index.cfm/items/1473.

[123] It is not clear whether 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 while he was in Sacramento lobbying for InCom and against the Identity Information Protection Act, he was still the attorney for the school district.

[124] Am. Legislation Exch. Council, *supra* note 62, at 7.

[125] S.B. 30, 2007 Leg. Sess. (Cal. 2006), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_30_bill_20061204_introduced.pdf.

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 have stated 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."[126] The legislation also incorporates the "Best Practices" recommended by the DHS Data Privacy & Integrity Advisory Committee to provide notice, secure readers and data, and avoid secondary usages.[127]

¶58 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 licenses. As discussed *supra*, both California constitutional and statutory law guarantees privacy and control over such information. Article I, Section 1 of the California Constitution provides for an inalienable right to privacy,[128] 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.[129] California law also prohibits displaying a Social Security number on a license or other identity document[130, 131] or embedding it on a machine-readable magnetic strip.[132]

1. Provisions of the Legislation

¶59 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.[133] 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.

a. All Government Documents

¶60 The first layer provides that every state-issued identification document must meet three basic standards: (1) tamper resistant features in order to prevent duplication, forgery, or cloning of the ID; (2) an 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;[134] and (3) notice to all individuals issued an RFID-embedded government identification document about RFID technology, the privacy and security implications, and how they can protect their information.[135]

---

[126] Jack M. Germain, *RFID Technology Faced with Privacy Considerations*, E-COMMERCE TIMES, July 11, 2005, http://www.ecommercetimes.com/story/44406.html.

[127] DATA PRIVACY & INTEGRITY ADVISORY COMM., THE USE OF RFID FOR HUMAN IDENTITY VERIFICATION, Report No. 2006-02 10-11 (2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf; DATA PRIVACY & INTEGRITY ADVISORY COMM., *supra* note 44, at 10-11.

[128] For example, California's State Constitution grants its residents an inherent right to privacy: "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." CAL. CONST. art. I, § 1.

[129] Cal. Civ. Code § 1798.90.1 (Deering 2007).

[130] Cal. Veh. Code § 12801(b) (Deering 2007).

[131] Cal. Civ. Code § 1798.85(a)(2) (Deering 2007).

[132] Cal. Veh. Code § 12801 (Deering 2007); Cal. Civ. Code § 1798.85(f) (Deering 2007).

[133] For more information about the Identity Information Protection Act, including the full text of the legislation, see Don't Chip Our Rights Away, *supra* note 3; *see also* Off'l. Cal. Leg. Info., Bill Documents – SB 30, http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_30&sess=CUR&house=B&author=simitian (last visited Dec. 5, 2007).

[134] *See* Cal. S.B. 30, 2007 Reg. Sess. §1798.10(1-3) (Cal. 2007); Cal. S.B. 30, 2007 Reg. Sess. §1798.135(b) (Cal. 2007) ("'Authentication' means the process of applying a machine-readable process to data or identification documents, or 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.")

[135] Cal. S.B. 30, 2007 Reg. Sess. §1798.10(9) (Cal. 2007).

b. Multiple Uses, Public Schools, Transport, Public Benefit

¶61 Additional layers of protections are built into the legislation when the RFID tag is embedded in identification documents that are used for multiple purposes, that are used for public schools and public transportation, or that confer a public benefit.136 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;137 and (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 waves.138 The additional protections are necessary because such cards are either used by young people or are likely to be carried and used on a regular basis.

c. Encoded with Personal Information

¶62 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.[139] These RFID-embedded documents must implement the *basic standards plus the following four security protections*: (1) the ID implements robust encryption to protect against the unauthorized reading of transmitted information; (2) the 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;[140] (3) the ID implements an additional security feature to ensure that the ID cannot be read unless the ID holder specifically authorizes that reading; and (4) the ID 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.

¶63 Individually, each of the layered protections is 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."[141] However, in concert, these protections may be able to help maintain privacy, personal safety, and financial security.

---

[136] Cal. S.B. 30, 2007 Reg. Sess. §1798.10(7-8) (Cal. 2007).

[137] *See* Cal. S.B. 30, 2007 Reg. Sess. §1798.135(i) (Cal. 2007) ("'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 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.")

[138] *See* Cal. S.B. 30, 2007 Reg. Sess. §1798(10)(6) (Cal. 2007); Cal. S.B. 30, 2007 Reg. Sess. §1798.10(5) (Cal. 2007) ("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.")

[139] Cal. S.B. 30, 2007 Reg. Sess. §1798(10)(3-5) (Cal. 2007).

[140] *See* Cal. S.B. 30, 2007 Reg. Sess. §1798(10)(m) (Cal. 2007) ("'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.")

[141] GOVERNMENT ACCOUNTABILITY OFFICE, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT, *supra* note 8, at 3, *see also* Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID, *supra* note 84 ("The requirement for a protective sleeve is

2. The Real Costs and Benefits

¶64 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. The HID Corporation 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."[142]

3. Support Across the Aisles and Up and Down the State

¶65 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.[143] The legislation also received editorial support from conservative and liberal newspapers up and down the state of California. The *Orange County Register* 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."[144] The *Los Angeles Times* noted that "Simitian is on the right track. Neither government nor private industry has given the public much reason to trust their ability to safeguard sensitive personal information."[145] 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."[146] The *San Francisco Chronicle* wrote that "[the Identity Information Protection Act] represents a restrained, reasoned approach to regulating a technology with potential for abuse."[147]

¶66 While the AeA started the 2005 legislative session standing in opposition to the bill, saying that security breaches were not a worry, lengthy discussions resulted in both AeA and the Information Technology Association of America (ITAA)[148] reaching a neutral position on the legislation.[149] In light of both the facts about vulnerabilities and the widespread support from both sides of the aisle and up and down the state, the California Assembly and Senate overwhelmingly passed the Identity Information Protection Act.[150]

---

also an issue. As drivers are speeding away from the border, they may not always remember to replace the PASS card 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.")

[142] Smart Cards for Access Control Advantages and Technology Choices, 2005, at 2, http://www.hidcorp.com/pdfs/HID_wp_smartcardAC.pdf.

[143] These groups also include the California National Organization for Women, California Alliance Against Domestic Violence, California State Parent Teacher Association (PTA), Consumer Federation of California, Privacy Rights Clearinghouse, Asian Americans for Civil Rights and Equality, the Republican Liberty Caucus, and many more, a complete list of the supporters, *see* CAL. OFFICE OF THE SENATE FLOOR ANALYSES, BILL ANALYSIS: THIRD READING. BILL NO. SB 30, May 21, 2007, *available at* http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_30_cfa_20070521_105105_sen_floor.html.

[144] Editorial, *A Moratorium on Electronic ID Tags*, ORANGE COUNTY REG., Aug. 21, 2005.

[145] Editorial, *Too Much Information*, L.A. TIMES, Aug. 23, 2005, at B12.

[146] Editorial, *Important Little Chips; RFID Transmits Valued Data, But it Needs Some Government Safeguards*, L.B. PRESS-TEL., Aug. 11, 2005, at A16.

[147] Editorial, *The Right to be Left Alone*, S.F. CHRON., Aug. 25, 2005, at B8.

[148] ITAA is the nation's largest information technology trade association, representing over 1100 member companies and affiliates. *See* ITAA homepage, http://www.itaa.org/ (last visited Nov. 10, 2007).

[149] 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. For a full list of the sponsors, *see*, CAL. SENATE JUDICIARY COMMITTEE, BILL ANALYSIS: AS INTRODUCED: SB 30:, Mar. 13, 2007, *available at* http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_30_cfa_20070313_155055_sen_comm.html.

[150] The 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, see Off'l. Cal. Leg. Info., Bill Documents – SB 768,

4. Legislators Thinking Ahead, Governor Short-sighted

¶67 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 opportunity to take a proactive stance in protecting the privacy and security of Californians. In his veto statement, Governor Schwarzenegger 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.[151] Following the Governor's very short-sighted veto, the Identity Information Protection Act was reintroduced in December 2006, passed the California Senate with a vote of 33-3 on May 24, 2007, and is continuing to move through the California legislature, sending 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.[152]

VIII. THREE YEARS AFTER SUTTER

¶68 Three 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, and the protections are available and cost very little to incorporate. Yet insecure RFID technology is still being considered for identification 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, instead of waiting until there is a privacy and security crisis.

¶69 Passing legislation to ensure that there are adequate privacy and security protections in place on the use of RFID in identification documents does not "ban the technology," "stifle the technology," or "hinder development," just like passing regulations to put seatbelts in automobiles has not banned, stifled, or hindered that technology.[153] 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."[154] But individuals 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.[155] Just like we mandate basic safety standards

---

http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_768&sess=PREV&house=B&author=simitian (last visited Oct. 7, 2007).

[151] The 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, see Off'l Cal. Leg. Info., Bill Documents – SB 768, http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_768&sess=PREV&house=B&author=simitian (last visited Oct. 7, 2007).

[152] Off'l Cal. Leg. Info., Bill Documents, http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_30&sess=CUR&house=B&author=simitian (last visited Oct. 7, 2007).

[153] AIM Global, *RFID Legislation—Protection or Pause Button?*, Aug. 29, 2005, *available at* http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=433&zoneid=24; Gregory Lippe, *Legislation based on fear hurts progress*, San Fernando Bus. J., July 4, 2005, *available at* http://www.allbusiness.com/government/advocacy-consumer-protection/484638-1.html. *See also* Kaczmerczak *supra* note 34

[154] Doug Farry, *supra* note 5.

[155] 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.

instead of leaving auto safety up to the car manufacturers, 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 like the Identity Information Protection Act is an important step in the right direction.

IX. BASIC STANDARDS MAY NOT BE ENOUGH

¶70 As important as it is to pass basic standards, 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.

¶71 **Security Failures:** The ultimate success of using countermeasures to mitigate the threats associated with the use of RFID depends on maintaining the security of the 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 associated 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 would therefore 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 not had a good history of database security. Countless cases from the last few years of security breaches at such places as the Department of Motor Vehicles, Veteran's Affairs, and universities cast serious doubt on whether the government can properly safeguard personal information.[156]

¶72 **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. The federal government has engaged in warrantless wiretapping, accessed the private call records of millions of innocent Americans, utilized secret airline travel tracking systems, and attempted 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.

¶73 **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 the 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.

¶74 **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

---

[156] Privacy Rights Clearinghouse, A Chronology of Data Breaches, Oct. 5, 2007, *available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm.

information has been read, it will be difficult to ascertain whether the countermeasures have been breached or whether the technology is being misused.

X. NEXT STEPS

¶75 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 alternative 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.

¶76 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 these documents are actually keeping private information safe and secure.

INTERNATIONAL CONFERENCE OF DATA PROTECTION &

PRIVACY COMMISSIONERS

RESOLUTION ON RADIO-FREQUENCY IDENTIFICATION

Final Version

20 November 2003

Following a proposal by the Data Protection and Access to Information Commissioner Brandenburg, the Independent Center for Privacy Protection Schleswig-Holstein, Germany, the Spanish Data Protection Agency and the Data Protection Commissioner of the Canton Zug, Switzerland, the International Conference resolves that:

Radio-frequency identification (RFID) technology is increasingly being deployed for a variety of purposes. While there are situations in which this technology can have positive and benign effects, there are also potential privacy implications. RFID tags are so far primarily used to identify and manage objects (products) to control the supply chain or to protect the authenticity of the product brand; however, they could be linked with personal information such as credit card details and even used to collect such information, or to locate or profile persons possessing tagged objects. This technology could allow for the tracing of individuals and for linking collected information with existing databases.

The Conference highlights the need to consider data protection principles if RFID tags linked to personal information are to be introduced. All the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology. In particular

a) any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;

b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way ;

c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and

d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.

These principles should be taken into account when designing and using products with RFID.

The remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process, would raise additional privacy concerns.

The Conference and the International Working Group on Data Protection in Telecommunications will monitor closely the technological developments in this field in greater detail in order to ensure the respect for data protection and privacy in the context of "ubiquitous computing".

Explanatory Note:

Radio-frequency identification tags (RFID tags) are currently being tested and increasingly being used as a more advanced form and possible replacement of bar codes ("smart labels"). The size of these microchips is about 1/3 of a millimetre (and smaller – "smart dust"). Most of them operate as passive transponders (without batteries) by listening to radio signals sent by transceivers (RFID readers) and using the energy of the received radio signal to reflect and answer it. Active RFIDs have a greater range (depending on the readers used). Since prices for RFID microchips and readers are dropping their widespread deployment becomes increasingly economically viable. RFID tags are likely to become essential drivers of ubiquitous (or pervasive) computing. Due to their storage and capacity for interactive communication they are far more powerful than bar codes. In addition they provide for unique identification of each tagged unit whereas bar codes are identical for every unit of the same product.

RFID tags can be used to install "smart shelves" in stores in order to better manage the supply chain and facilitate the replenishments of goods or supplies (e.g. the case of Gillette razors). They may also be used for easy (contact-less) payment at the point of sale especially if linked with credit cards. Furthermore an employer may use the technology to tag his property in order to reduce theft by employees. They could be linked with video surveillance cameras to check employee as well as customer behaviour. Specific documents may be tagged to be traced more easily in an office. Identity cards as well as travel documents (passports, visas) may be equipped with RFID tags. More recently the European Central Bank has announced that Euro notes will be issued with RFID tags in order to fight counterfeiting and money laundering as well as to control circulating notes. Washable RFID tags can be embedded in clothes ("wearable computing") in order to prevent or detect counterfeiting of specific brands and to prove the authentic manufacture of the product. Other possible applications range from car keys (immobilizers) to container management.

The RFID technology has numerous privacy implications. This is obvious in the case of implanted microchips But also in the more widespread case of tagged objects and goods undoubtedly the

information transmitted also refers to the person carrying or wearing (or otherwise associated with) a tagged item or a "constellation" of brands thereby revealing the individual's taste. Therefore personal data can be processed and transmitted or read with the help of RFIDs or at least such object-related information can easily be linked with personal information (e.g. when a credit card is used for buying the tagged item). RFID tags have the potential of tracking the movements of a person who possesses or handles tagged objects.

Plans to afford technical devices legal protection against circumvention may prevent data subjects from disabling or deactivating RFID tags which function in a privacy-unfriendly way (e.g. after having paid and left the shop).

Since this issue has led to a growing public debate in a number of countries it is recommended that the International Conference addresses the related privacy problems at this stage in order to encourage privacy-friendly solutions which have been proposed. The International Working Group on Data Protection in Telecommunications at its 34th meeting in Berlin on September 2 and 3, 2003, has expressed its support for this proposal.