ALASKA LEGISLATURE COMMITTEE FILES 2007-2008 SJUD 12564

City of Kodiak
KODIAK POLICE DEPARTMENT
Animal Control

To Whom It May Concern:

RE: Senate Bill 273

I am for stronger punishment for Animal Cruelty offenders. Far too often animals are treated inhumanely in heinous acts of cruelty and they are let off with little more than a slap on the wrist. If we can get Senate Bill 273 passed I believe it would be a step forward in keeping animals safe. There is a link where people who abuse their animals also have other abuse problems in their lives. By making cruelty have a stronger penalty it may discourage future crimes of a different kind as well as discourage them from ever inflicting cruelty on another animal.

Thank You,
Animal Control Officer Amy Wagner

217 Lower Mill Bay Rd
Kodiak, AK 99615
907-486-8000

Katherine Pustay

From: Fetko, Dee Ann [FetkoDA@ci.anchorage.ak.us]
Sent: Monday, March 03, 2008 8:17 AM
To: Katherine Pustay
Subject: FW: Senate Bill 273 - Letter from Animal Control Advisory Board

Katherine,

Here is the letter from the Animal Control Advisory Board. Thank you.

DeeAnn Fetko
Grants and Contracts Supervisor
Municipality of Anchorage
Department of Health & Human Services
(907) 343-4634 phone
(907) 249-7659 fax
fetkoda@muni.org

-----Original Message-----
From: Stephanie & Neil Koeniger [mailto:slknrk@gci.net]
Sent: Tuesday, February 26, 2008 8:42 PM
To: katherine.pustay@legis.state.ak.us
Cc: George Doty; Mary Troll; Sandy Traini; Laura Bain; Lori Hackenberger; Patty Ginsburg; Kayla Epstein; Fetko, Dee Ann
Subject: Senate Bill 273

Hi Katherine-

I am writing in support of Senate Bill 273. I understand that this bill may be coming up for hearing on February 27th. I am not available to testify on this bill on that date but did want you to have these written comments for the hearing.

Having read the bill, my understanding is that it would make dog fighting a Class C felony. It would also make repeat offenses on other abuse activities a Class C felony instead of the current Class B misdemeanor status. I have reviewed these proposed changes with the other members of the Municipal Animal Control Advisory Board and we support both proposed changes.

It has been acknowledged for many years now by both most law enforcement agencies throughout this country, as well as many social service agencies, that there is a direct correlation between individuals who abuse animals and their abuse of other people. This type of behavior cannot and should not be condoned. Elevation of these offenses to felony status reinforces that position and, while it may not stop the offenses, should be a significant deterrent to them.

We encourage Legislative passage of this Bill. In our efforts to discourage criminal behavior in Alaska this is a positive step. Support should be a "no brainer".

Please feel free to share these comments with the sponsor of the bill as well as any other legislators who may be interested in them and also make them available for tomorrow's hearing on this bill. While I have schedule conflicts which preclude my testifying, I would be happy to do so if it comes up later. I also am available electronically to answer questions any of them may have concerning my support and/or to provide additional input should they so desire.

Thank you for your attention to this input. Also please extend our thanks to Senator Wielechowski for advancing this proposed legislation.
We will follow its progress with interest.

Neil Koeniger, Chair
Animal Control Advisory Board
Municipality of Anchorage

As an Alaska resident and a supporter of the American Humane Association, I urge you to vote for Senate Bill 273 as it comes before your committee on Monday, March 3.

Alaska remains one of seven states without a felony law regarding animal cruelty. Because of this, even the most horrific acts of torture to companion animals are virtually ignored. Last November, a Fairbanks man, following an argument with his wife, was accused of slamming her cat against a tree until it was unconscious. He was only charged with a misdemeanor. In 2006, an Anchorage man was convicted of beating his brother's dog. He only received a $100 fine.

Alaska's weak animal cruelty law has a tremendously detrimental impact on children and animals. The Link® between animal abuse and other forms of societal violence is nationally recognized. Threats or actions against companion animals are strong indicators that violence against human family members will follow.

Introduced by Sen. Bill Wielechowski, SB 273 will make it a felony punishable by up to five years' incarceration and/or a $50,000 fine to knowingly inflict severe pain or suffering on an animal, to kill or injure an animal by use of a decompression chamber, to intentionally kill or injure a pet or livestock via poison and to promote animal fighting exhibitions. Intentionally participating as a spectator at an animal fight for the second time would also become a felony offense. SB 273 will help ensure such actions will be properly reported, investigated and prosecuted as crimes with serious consequences.

As an Animal Control Commissioner at our local Division of Animal Control since 1996, I have been exposed directly to first hand knowledge concerning incidents - educating me as to how limited we are legally to our efforts to gain justice for the voiceless. Even when the carcass of the animal-victim is brought forth, with background information and photographs that leave it absolutely evident of the abuse inflicted, and yet, because of the weakness of the laws or lack there-of, we are not able to gain a conviction of any sort against these abusers - short of a menial fine. The fine is paid, animal returned to owner, only to have further animals suffer at the hands of [many times] the same known abuser, again, fined and released.

What message does this send to our society?! As those who care remain horrified first at the act and/or level of abuse and secondly, the lack of seriousness by current Animal Abuse Laws given to the horrible crime.

We are the only hope for justice that these unconditional loving and defenseless creatures have. Please help give us the support necessary to help make the difference needed so desparately.

Please help ensure a more humane Alaska for future generations by voting for SB 273.

Sincerely,

Ms. Mary Ann Fortune
PO Box 72596
Fairbanks, AK 99707-2596

My name is Kiki Stirling. My husband and I have been rescuing and rehabilitating dogs in the interior for the last ten years. We've only recently become an official entity, and are in the process of building an animal refuge here in Fairbanks. Domestic animals in this state have little regard or protection, and along with our nationally high rape rate, domestic abuse rate, and murder rate, we are one of the worst animal welfare states in the union. These aren't things to be proud of.

It takes on average, a year for a dog to become rehabilitated when it's been either horribly abused physically, or mentally, or severely neglected. I realize that this bill doesn't include definitions of, or punishments for neglect, but neglect is as big a problem in Alaska as abuse is, and in many cases, the line between them is barely visible.

A guy in Fairbanks went on a rage one night in an apartment, and started beating his black lab with a pipe. Neighbors who tried to intervene were threatened. The cops were called, and he was charged with disorderly conduct or something, but wasn't charged for the abuse of the dog.

The dog, who lived, was brought to a rescue group, who spent hundreds of dollars to save this dog's life. He's currently living his life in a good home, minus a good chunk of his skull and one eye. Why does the man who's capable of doing this walk away without consequence? Can you imagine doing something so horrific? You look at your dogs, cats, horses etc., can you imagine them going through something so traumatizing? Look at your neighbors' animals. How many are well taken care of, well loved, and how many are not?

Animal shelters and law enforcement need to be able to prosecute animal abusers. There'll never be an end to abuse, torture, and neglect if there aren't laws that are strong enough, or can't be enforced.

Kiki Stirling
Thistledown Animal Rescue
Box 80724 Fairbanks, Alaska 99708

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.