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 example, 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/sne-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 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 we 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.