



April 14, 2008

Senator Robert E. Clegg Jr.  
Statehouse  
107 N. Main St., Room 124  
Concord, N.H. 03301

1718 Connecticut Ave NW  
Suite 200  
Washington DC 20009  
USA  
+1 202 483 1140 [tel]  
+1 202 483 1248 [fax]  
[www.epic.org](http://www.epic.org)

Dear Senator Clegg:

Thank you for your request for us to review New Hampshire HB 686, "An act relative to the regulation of remotely readable devices and the illegal use of payment card scanning devices or reencoders."<sup>1</sup> EPIC strongly supports HB 686 and its protections for consumers.

The legislation would establish important safeguards for New Hampshire residents including: (1) penalties for illegal use of RFID technology; (2) a private right of action for individuals; (3) restrictions on the use of RFID technology by the State of New Hampshire with few exceptions; (4) prohibitions on electronic tracking of individuals without a valid court order or consent; and (5) prohibitions against forced implantation of RFID devices in humans. However, as we will later explain, EPIC urges the Committee to also: (1) address unique identifiers linked to databases containing personally identifiable information, and (2) label RFID readers and interrogators, as well as RFID tags and products containing tags.

EPIC has considerable expertise on technology issues, including those associated with radio frequency identification (RFID) technology.<sup>2</sup> 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.<sup>3</sup>

#### 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

<sup>1</sup> New Hampshire, HB 686, "An act relative to the regulation of remotely readable devices and the illegal use of payment card scanning devices or reencoders" [hereinafter "NH HB 686"], available at <http://www.gencourt.state.nh.us/legislation/2008/HB0686.html>.

<sup>2</sup> See generally EPIC, Radio Frequency Identification (RFID) Systems, <http://www.epic.org/privacy/rfid/>.

<sup>3</sup> For example, EPIC recently testified about RFID before the Alaska State Senate: Melissa Ngo, Senior Counsel and Dir., EPIC Identification & Surveillance Project, *Prepared Testimony and Statement for the Record at a Hearing on "SB 293: Electronic Communications Devices" Before the Judiciary Comm. of the Alaska Senate* (Mar. 17, 2008), available at [http://www.epic.org/privacy/rfid/ngo\\_test\\_031708.pdf](http://www.epic.org/privacy/rfid/ngo_test_031708.pdf).

university ID cards), credit and debit cards, supply chain management and animal tracking.<sup>4</sup>

RFID systems generally include a tag or chip (on which data is stored) and an antenna (to transmit the data to a reader).<sup>5</sup> “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.”<sup>6</sup> 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 interrogator.

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.”<sup>7</sup> Other tests also have shown that RFID tags can be read from 70 feet or more, posing a significant risk of unauthorized access.<sup>8</sup>

---

<sup>4</sup> See EPIC & PRIVACY INT’L, *Privacy & Human Rights 2006: An International Survey of Privacy Laws and Developments* (EPIC 2007).

<sup>5</sup> *Id.*

<sup>6</sup> See EPIC, *Radio Frequency Identification (RFID) Systems*, *supra* note 2; 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](http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf).

<sup>7</sup> 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>.

<sup>8</sup> 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.

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.

### 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 month, the Dutch government announced that the security of access keys that are based on the widely used Mifare Classic RFID chip has been compromised.<sup>9</sup> Guusje ter Horst, Dutch Interior Minister, said in a letter to Parliament that the Mifare Classic RFID chips have been hacked.<sup>10</sup> 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.<sup>11</sup> The Mifare Classic is also used in Boston and London's transportation cards. According to Ms. 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.<sup>12</sup>

In recent months, several researchers have separately issued papers detailing how to hack the Mifare Classic RFID chip.<sup>13</sup> 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

---

<sup>9</sup> 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"].

<sup>10</sup> *Id.*

<sup>11</sup> 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.

<sup>12</sup> Letter from Guusje ter Horst, *supra* note 9.

<sup>13</sup> 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>.

shaky security employed by credit card companies.<sup>14</sup> 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.

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

Like New Hampshire, many states are debating legislation to ensure adequate protections for RFID use:

- Last month, Washington state passed a law to prevent “skimming” of data from RFID tags;<sup>15</sup>
- California, North Dakota and Wisconsin have passed legislation forbidding the compelled implantation of RFID chips in humans;<sup>16</sup>
- Currently, California is debating a law to prevent “skimming”;<sup>17</sup>
- Also, Alaska is debating legislation that includes prohibitions against unauthorized scanning and reading of RFID tags and against 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;<sup>18</sup> and,
- A number of other states are debating legislation to restrict the use of RFID technology.<sup>19</sup>

---

<sup>14</sup> 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>.

<sup>15</sup> 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>.

<sup>16</sup> 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](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>.

<sup>17</sup> 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](http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_31_bill_20080107_amended_sen_v96.html).

<sup>18</sup> Alaska, SB 293, “An Act relating to electronic communication devices and to personal information,” available at [http://www.legis.state.ak.us/basis/get\\_bill.asp?session=25&bill=SB293](http://www.legis.state.ak.us/basis/get_bill.asp?session=25&bill=SB293).

<sup>19</sup> See EPIC, Radio Frequency Identification (RFID) Systems, *supra* note 2.

## 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.<sup>20</sup>

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 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 data about that individual.

## HB 686 Includes Many Protections for Consumers and EPIC Supports the Legislation

EPIC strongly supports New Hampshire's HB 686, "An act relative to the regulation of remotely readable devices and the illegal use of payment card scanning devices or reencoders." There are a number of provisions of HB 686 that are necessary to ensure strong protection of consumer rights and follow the EPIC Guidelines on Commercial Use of RFID Technology. However, we urge the Committee to also: (1) address unique identifiers linked to databases containing personally identifiable information, and (2) label RFID readers and interrogators, as well as RFID tags and products containing tags.

In HB 686, Section 358-T:4 Restrictions on State Use of Remotely Readable Devices, provision II reads: "No identification document permitted under this section shall contain, transmit, or enable the remote reading of any personal information other than a unique personal identifier number which is not a social security number."<sup>21</sup> These unique identifiers can be used to create detailed personal profiles on individuals. Though companies have urged against the regulation of these unique

---

<sup>20</sup> EPIC, *Guidelines on Commercial Use of RFID Technology* (July 2004), available at [http://epic.org/privacy/rfid/rfid\\_gdlnes-070904.pdf](http://epic.org/privacy/rfid/rfid_gdlnes-070904.pdf).

<sup>21</sup> NH HB 686 at § 358-T:4 Restrictions on State Use of Remotely Readable Devices, *supra* note 1.

identifiers, they should be covered under HB 686 because the misuse or abuse of such unique identifiers could be as risky as misuse or abuse of Social Security Numbers.<sup>22</sup>

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 privacy," the GAO said.<sup>23</sup> EPIC urges the Committee to regulate the use of these unique identifiers and the detailed profiles that can be constructed with them.

EPIC also recommends that consumers should be given notice of RFID readers or interrogators, as well. Though HB 686 includes provisions requiring the labeling of products containing RFID tags, we recommend that there should be a requirement that RFID readers or interrogators 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.<sup>24</sup>

There are several provisions of HB 686 that EPIC endorses. First, we believe that 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. Therefore, we support Section 358-T:6, which sets out penalties for illegal use of RFID technology and includes a private right of action:

- I. Any person convicted of violating RSA 358-T:2 or RSA 358-T:5 shall be guilty of a misdemeanor if a natural person and a felony if any other person. Each such act shall constitute a separate offense.
- II. Any person convicted of violating RSA 358-T:3 shall be guilty of a class B felony.
- III. An aggrieved individual or the state may bring suit for civil penalties for up to \$1,000 or actual damages, whichever is greater, plus court costs and reasonable attorney's fees, for each violation of this chapter.<sup>25</sup>

Second, we agree with Section 358-T:4, which restricts the use of RFID technology by the State of New Hampshire with few exceptions:

---

<sup>22</sup> 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).

<sup>23</sup> 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>.

<sup>24</sup> NH HB 686 at § 358-T:2 Notice Required; Consumer Products, *supra* note 1.

<sup>25</sup> *Id.* at § 358-T:6 Penalties.

I. The state or a political subdivision, department, or agency shall not issue, or permit others to issue on its behalf, any identification document that contains a remotely readable device or uses remotely readable devices to locate an individual, either directly or indirectly through other persons, except in the following circumstances:

(a) To locate a person who is incarcerated in the state prison or county jail, is housed in a mental health facility pursuant to a court order after having been charged with a crime, is subject to court-ordered electronic monitoring, or is a resident of a state or county hospital, nursing facility or assisted living facility.

(b) When the remotely readable device is implanted in an identification document that is to be used on a toll road or bridge owned or operated by the state or a political subdivision, department, or agency thereof, but only for the specific purpose of collecting funds for the use of that road or bridge.

(c) An identification document that is issued to a person for the limited purpose of facilitating secure access by the identification document holder to a secured public building or parking area.

(d) The identification document is part of a contactless identification document system used by the state or a political subdivision, department, or agency of the state that is operational and in use prior to January 1, 2007.

(e) Credit, debit, or financial account cards issued to a person for use on behalf of the state or a political subdivision, department, or agency of the state, provided that such card complies with RSA 358-T:2.<sup>26</sup>

Third, we agree with Section 358-T:5, which prohibits electronic tracking of individuals without a valid court order or consent:

Except as otherwise provided in this chapter, no person may track an individual without a valid court order or the consent of the person being tracked.

Notwithstanding the foregoing, a person may track property owned or otherwise legally possessed where the person has reason to believe the property is being used in violation of the person's property interests.<sup>27</sup>

Finally, we support Section 358-T:3, the prohibition against forced implantation of RFID devices in humans.<sup>28</sup> Three other states have already passed legislation against compelled implantation in humans, and New Hampshire should join their ranks.<sup>29</sup>

I. No person shall implant or attempt to implant or physically incorporate a remotely readable device into or on the body, skin, teeth, hair or nails of another individual

---

<sup>26</sup> *Id.* at § 358-T:4 Restrictions on State Use of Remotely Readable Devices.

<sup>27</sup> *Id.* at § 358-T:5 Electronic Tracking Prohibited.

<sup>28</sup> *Id.* at § 358-T:3 Human Implantation of Remotely Readable Device Prohibited.

<sup>29</sup> See section entitled "Many States Are Taking Steps To Establish Appropriate Safeguards for the Use of RFID Technology," *supra*.

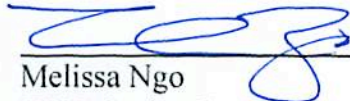
without the prior, informed written consent of the individual. Consent of a guardian, guardian ad litem, attorney-in-fact, or parent of a minor child shall be considered adequate consent, unless a written instrument executed by the individual precludes implantation or physical incorporation. Use of a bracelet or other readily removable device is not considered implantation or physical incorporation under this section.

II. No individual shall be offered an incentive, denied an opportunity, or in any way treated by a person differently from any other individual as a consequence of providing or withholding such consent.

III. No person shall use the presence or absence of an implanted remotely readable device as a basis for discriminating against an individual for any purpose whatsoever, including, but not limited to, employment, housing, insurance, medical care, voting, education, travel, and commerce.

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 these systems and the data collected. HB 686, "An act relative to the regulation of remotely readable devices and the illegal use of payment card scanning devices or reencoders," has taken a number of steps to safeguard consumer rights. Though we strongly support HB 686 and recommend its passage, we urge the Committee to also: (1) address unique identifiers linked to databases containing personally identifiable information, and (2) label RFID readers and interrogators, as well as RFID tags and products containing tags.

Sincerely,



Melissa Ngo  
EPIC Senior Counsel