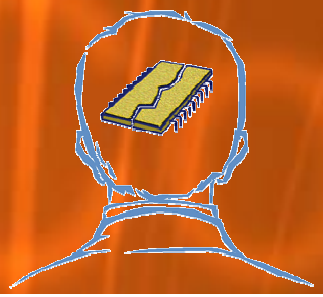



Legislating Against RF Technology



What Happening and What Is Wrong with the Legislation

Richard J. H. Varn

NextCard℠

HID

The Challenges of Explaining RFID and Drafting Sound Legislation

The Challenges of Explaining RFID and Drafting Sound Legislation

- Lots of FUD
- Misinformation
- It’s technical
- Privacy advocates who state unequivocally that what can be imagined or patented can and will be done
- Lagging response by industry (this is changing)
- The systems are either invisible or not yet deployed and their benefits are not visible

What Are Legislatures Doing?

- Apprehension about potential uses of RFID has prompted introduction of legislation
- Although no states have yet enacted legislation related to RFID, at least 10 states in 2004, 12 states in 2005, and 13 in 2006 introduced privacy legislation relating to the use of RFID
- Most bills would require disclosure to consumers if RFID tags are used in products.

What Are Legislatures Doing?

- Some prohibit linking RFID data to personal information
- Some criminalize unauthorized remote reading of RFID data
- Some prohibit the use of RFID tags in government identification documents and would place other restrictions on the uses of RFID in government IDs.

A Rational Approach

- Note: this is not the path taken so far
- Review one's current laws
- Identify the gaps
- Determine the proper level of government at which any gaps should be addressed

A Rational Approach

- Draft legislation and/or rules narrowly and accurately
- Use sunrise and sunset clauses as appropriate

A Rational Approach

- Prohibit the undesired behaviors, not the technology
- Determine the punishment and method for enforcement
- Differentiate between four different kinds of RFID deployments

A Rational Approach

- Four kinds of RFID deployments:
  - Government documents and devices transferred to the public
  - Government documents and devices internal to government
  - Private documents and devices transferred to the public
  - Private documents and devices internal to a private entity

Government Documents/Devices to Public

Policy Question	Government Documents and Devices Transferred to the Public and Use Is Mandatory	Government Documents and Devices Transferred Where Citizens Knowingly Choose to Use It
Should tracking be allowed?	No. Tracking without consent or operation of law should be forbidden	No. Tracking without consent or operation of law should be forbidden
Does remote reading require explicit consent or operation of law?	Always	Yes unless varied by the terms of any agreement of use or participation
Where should this policy issue be addressed?	In statute	In statute
Notice of presence of remote reading capability required?	Yes	Yes

Government Documents/Devices Internal

Policy Question	Government Documents and Devices Transferred to Government Employees for Their Use	Government Documents and Devices In Use in Government to Track Objects (documents, inventory, animals, etc.)
Should tracking be allowed?	Tracking for non-work purposes should be forbidden but tracking for work purposes depends on employment law and contracts (if any)	Tracking is the purpose of the use of the technology so tracking is allowed, but may not be incidentally be used to track a person in contradiction of the limits in the other three categories
Does remote reading require explicit consent or operation of law?	Depends on employment laws and rules governing public employees	Never
Where should this policy issue be addressed?	In statute	In statute
Notice of presence of remote reading capability required?	Yes	Yes

Private Documents/Devices to Public

Policy Question	Documents and Devices Sold With RFID or Remote Reading Capability as an Explicit Part of the Function of the Document or Device	Documents and Devices Sold or Given Away With RFID or Remote Reading Capability In, On, or Attached to the Product
Should tracking be allowed?	No. Tracking without consent or operation of law should be forbidden	No. Tracking without consent or operation of law should be forbidden
Does remote reading require explicit consent or operation of law?	No	Yes (already covered by state law) unless done incidentally as a result of another legitimate use of the technology and no data is retained or used
Where should this policy issue be addressed?	Tracking issues needs to be clarified by statute	In statute
Notice of presence of remote reading capability required?	No as it is inherent in the product	Unnecessary and of little or no benefit

Private Documents/Devices Internal

Policy Question	Documents and Devices Transferred to Private Employees for Their Use	Documents and Devices In Use by Private Persons to Track Objects (inventory, animals, etc.)
Should tracking be allowed?	Tracking for non-work purposes should be forbidden but tracking for work purposes depends on employment law and contracts (if any)	Tracking is the purpose of the use of the technology so tracking is allowed, but may not be incidentally be used to track a person in contradiction of the limits in the other three categories
Does remote reading require explicit consent or operation of law?	Depends on employment laws and rules governing employees	No
Where should this policy issue be addressed?	In statute as needed, rules, and contracts	No legislative action required
Notice of presence of remote reading capability required?	Depends on employment laws and rules governing employees	No

Current Legislative Approach

- Broad based bans, limitations, and requirements
- Overbroad definitions that cover commonly used technologies including non-RFID technologies
- Interlocking and overlapping definitions that have broad and unintended effect

Legislative Approach

- Language focusing on technology rather than behavior
- Current applicable statutes are ignored
- Language seeks to codify private codes of conduct
- Language based on false or unsupported assumptions

Definitional Problem Example

- **New Hampshire HB 203**
- “Identification document” means any document or object containing personal information that an individual uses alone or in conjunction with any other information to establish his or her identity, to engage in government-regulated activities, or to engage in financial transactions.
- Note that contains is not defined so even if it is just printed on the card, it contains personal information

Definitional Problem Example

- **New Hampshire HB 203**
- **“Personal information”** means information that can be used to identify an individual. Such information includes an individual’s name, address, telephone and cellular telephone number, social security number, credit card and financial account numbers, driver’s license number, e-mail address, date of birth, race, religion, ethnicity, nationality, political affiliation, photograph and digital image, fingerprint or other biometric identification, and **any other unique personal identifier or number.**

Definitional Problem Example

- **New Hampshire HB 203**
- **“Tracking Device”** is any *item or application that is actively or passively capable of transmitting unique identification or location information.”*
- Tracking devices are banned in any government identification document or device

Definitional Problem Example

- Washington State Proposed Bill HB 2521
- "Identification document" means any document or device containing personal information that an individual uses alone or in conjunction with other information to establish his or her identity

Definitional Problem Example

- **Rhode Island 42-140-1. Restriction of radio frequency identification devices. –** Except where required by federal law, no state or municipal agency, or any subdivision thereof, shall use, or request the use of Radio Frequency Identification Devices (RFID) for the purpose of tracking the movement or identity of any employee, student or client, or of any other individual as a condition of obtaining a benefit or services from such agency.

Definitional Problem Effect

- Mobile Phones – Cellular phones, by definition, transmit unique identification information and would be banned.
- E-911 for fixed and mobile phones is an application/device that transmits location and identification information by design and government mandate would be banned

Definitional Problem Effect

- Mobile Computers – Notebook computers, personal digital assistants (PDAs), and hand-held computers that access networks wirelessly must transmit unique identifiers and data used to locate and identify the device to the network node and host system to give them access and to send them back the data they request (so it gets to the right machine). So mobile government is banned.

Definitional Problem Effect

- Contact-less cards and tokens for financial transactions would be banned for government use
- Access Cards – have been in use for years and contain a unique number used to identify the holder as authorized to enter or use a facility or service would be banned for most uses

Definitional Problem Effect

- Secure document systems and document check out processes that can cut down on information threats but would be banned
- Police and fire digital radios that transmit unique numbers would be banned

Definitional Problem Effect

- Cars with the OnStar System, keyless-entry fobs, and other security and safety systems transmit a unique identifier so most modern cars would be banned or need serious modifications
- GPS devices and GPS enabled anything would be banned
- An on, and on, and on

Notice Issue

- Legislators have a hard time stopping themselves from codifying what ethical actors promise they will do anyway
- So they want to permanently mandate RFID notice on everything with remote read capability
- Notice: Bar Codes in Use…

Notice Issue

- Just like kindergarten, the rest of us are punished for that one kid who eats the chalk and sniffs the magic markers until he passes out
- Notice will only be useful after substantial deployment and before ubiquity and then it will be silly or at best unneeded

Alternative Language

- Follow the grid above
- Other examples:
- "Personal information" includes any of the following: an individual's name, address, telephone number, e-mail address, date of birth, religion, ethnicity, nationality, photograph, fingerprint or other biometric identification, social security number, or any other unique personal identification number assigned to a person.

Alternative Language

- Personal information does not include any unique identifier including but not limited to unique personal identification number assigned to a person, unique identifier assigned to a document, or a unique identifier that acts as an ID number for a computer chip, computer chip bearing device, or computer system if…

Alternative Language

- (1) That number cannot be used to identify a person or be related to personal information except by use of separate data system and;
- (2) If such a separate data system is protected from unauthorized access as determined by applicable law.

Alternative Language

- "Contact-less means use of radio waves or other non-visible means to read or transmit data, but does not include bar code scanning systems and other similar light wave based systems which cannot read or transmit data without the holder's knowledge.

Alternative Language

- Except as provided herein, all **identification documents** created, mandated, or issued by a state, county, or municipal government, or subdivision or agency thereof **that allow remote contact-less reading or transmission of personal information** and that have been transferred from government possession into the possession of a lawful holder of the document **shall meet these requirements**:

Alternative Language

- (1) The identification document shall not transmit or enable the remote reading of any personal information except by an explicit consent process or operation of law.
- 2) The identification document, and the systems supporting creation, authentication or use of the identification document, shall comply with the requirements of subdivisions (X)-(X).

Alternative Language

- (X) The Chief Information Officer will adopt technology standards to ensure that no personal information is disclosed from an identity document without an explicit consent process by the lawful holder of the document or by operation of law, in accordance with section (a). Such standards may require protecting personal information in identification documents by such methods as mutual authentication, on and off switches for remote contact-less reading, encryption, and shield devices. Such protections shall be proportional to the risks presented by each system, including the identity document and context of use relevant to each system. Such standards and may require different protections for different systems, depending upon the applicable risks. The Chief Information Officer shall certify whether systems are compliant prior to purchase or other method of adoption by an agency and again prior to implementation.

Alternative Language

- (X) The Chief Information Officer shall also establish a process by which security flaws may be reported to the office of the Chief Information Officer. Such reported security flaws shall not be disclosed and shall be kept confidential unless such disclosure is deemed to advance the ability to protect persons and systems from the flaw. The existence of a reported flaw and any details as to its nature which do not aid in the exploitation of the flaw shall be made public and reported to the TBD Committee of the House and the Senate within 3 working days of receipt of such a report. Any countermeasure known to be effective against the flaw shall be made publicly available. For any system for which a security flaw results in unauthorized disclosure of personal information, the Chief Information Officer shall review such system and may revoke its authority to operate or may mandate specific changes be made as a condition of continued operation.

Alternative Language

- (X) The TBD Agency will establish a process for individuals and entities to report disclosures of personal information from any identification document. In the event of such disclosure, the agency responsible for the implementation of the identity document shall follow applicable law as to security breaches resulting in the unauthorized release of personal information (INSERT CODE CHAPTER REFERENCE).

Alternative Language

- Use sunsets on a date certain
- Be creative about sunsets
  - E.G. When 50% of all products sold at retail use RFID then notice is no longer required

Alternative Language

- Exempt products that contain computer chips or other technology capable of remote reading that is part of their commonly understood purpose, specifically designed for that purpose, and sold for that purpose
  - E.G. GPS, cell phones, wireless network products, car security systems

Alternative Language

- California 502.6. (a) Any person who knowingly, willfully, and with the intent to defraud, possesses a scanning device, or who knowingly, willfully, and with intent to defraud, uses a scanning device to access, read, obtain, memorize or store, temporarily or permanently, information ***encoded or printed on or within the payment card or other payment token that serves as an indicia of permission to engage in a financial transaction*** without the permission of the authorized user of the payment card is guilty of a misdemeanor, punishable by a term in a county jail not to exceed one year, or a fine of one thousand dollars ($1,000), or both the imprisonment and fine.

Give Them Something Useful to Do

- Study and learn
- Update the anti-skimming laws
- Review current statutes and consider updates
- Watch the developments in the market and in the criminal world
- Boost cyber crime enforcement funds for laws already on the books and make enforcement a priority

Questions and Comments

Contact Information:

rjmvarn@msn.com

Home/Office:(515) 255-3650