Radio-Frequency Identification Document Advisory Panel Meeting

914 Capitol Mall, Room 500
Sacramento, CA

Summary Minutes

October 31, 2007

Panel Members in Attendance

Susan Hildreth, Chair
Steve Keil
Bill Newell
Nicole Ozer
Randy Vanderhoof
Paul Preston
J. Clark Kelso
Jennifer King
Leilani Yee
Beth Givens
Roxanne Gould

The meeting came to order at 10:00 a.m.

1. Welcoming Remarks by Dean Misczynski, Director, California Research Bureau

It is the intent of the California Research Bureau to make this advisory process as fair as possible. The Advisory Panel and the CRB will strive for neutrality.

2. Remarks by Chris Marxen, Assistant Director, California Research Bureau

a) This is the first of two Advisory Panel meetings. The second meeting of the panel will be held in February 2008.

b) The CRB has produced a website where background materials will be posted: http://www.library.ca.gov/crb/rfidap/index.html

c) The purpose of the second meeting will be to provide a venue for the Advisory Panel to develop recommendations for the report. Prior to the second meeting, the California Research Bureau will send draft recommendations to the panel members and post these recommendations on the RFID webpage 10-15 days before the second meeting. Comments will be incorporated in the paper. Recommendations by the panel will be included in a final report by the California Research Bureau to Senator Joe Simitian next March.

d) During the advisory process, the panel is to conduct themselves in accordance with the Bagley-Keene Open Meeting Act.

3. Public comments

a) **Anne Kelson, Graduate student, University of California, Davis**
We should be concerned that measures that are supposed to make us safer actually make us less secure. There are risks associated with using RFID cards at a place like UC Davis. People who aren't supposed to be there can gain access, and there is a vulnerability to security breaches, theft of documents. The State Constitution guarantees privacy. Forced use of RFID cards should not happen. An alternative or an opt-out should be offered for those who don't want to use RFID card. More public debate needed so concerns can be raised. The use of insecure RFID is like making people identify themselves wherever they go.

b) **Valarie Small-Navarro, Senior Advocate, American Civil Liberties Union**
The State Constitution bans the stockpiling of personal information, to keep from using info gathered from one purpose for another, or to embarrass us. California voters were clear what they intended when they added it to the State Constitution. They were concerned about personal safety. People have the right to take a personal interest in the way RFIDs will be used. This is an issue that cuts across political lines. Editors of Scientific American said tagging Junior High School children (as happened in Sutter, CA) becomes a form of indoctrination into society, where young minds should be learning to question. Tracking should not happen without discussion by society. It behooves us as individuals and a society to work together, come up with solutions that work.

c) **John Kuester, RFID Global Solution**
We are moving in two directions. There are commercial RFID tags in use, such as on merchandise, military hardware. We must separate the business part of the technology from the personal issues that RFID brings up to organizations. I'm concerned that prohibitive Legislation will leave California at a disadvantage with other states in the implementation of this technology.

d) **Michelle Tatro, Private Citizen**
Her child wore an RFID tag that she received from school. Ms. Tatro worked to get her child's information taken out of the school database. Driver's licenses are needed for State ID, so if a driver's license contains an RFID tag, there is no choice but to use it. It is wrong to be able to be tracked like animals.

e) **Carol Henton, Vice-President State & Local, Information Technology Association of America**
The ITAA is a trade association whose members are responsible for producing the majority of government credentialing and identity management programs at the federal, state, and local levels. The use of RFID technology offers significant benefits in many areas like supply chain efficiency, food and drug safety, credentialing and transportation safety. ITAA recognizes privacy and security concerns surrounding RFID technology. Laws currently exist that address privacy matters. The security of documents depends on a layered security approach. Guidelines should be used to ensure privacy measures are put in place and upheld. Legislating limitations stops technology from advancing. CRB is cautioned against recommending legislation that restricts the use of certain technologies in credentials.

f) Lenny Goldberg, Advocate, Consumer Action & Privacy Rights Clearinghouse
Every technology has good aspects and downsides as well. RFID is a great tracking device, but on humans, it can interfere with privacy. When it comes down to making recommendations, privacy and industry people will probably come to most of the same conclusions. Our conclusions may be more flexible than those that the Department of Homeland Security came up with. Understand limits and dangers when applied in the wrong application.

g) Beth McGovern - California Commission on the Status of Women
Women and children are more vulnerable to the security and safety risks presented by RFID systems because thousands of women and children are victims of stalking, sexual assault and domestic violence. RFIDs would make illegal surveillance easier by allowing secret, long-distance access to personal identifying information and could enable the tracking of victims' movements. A holder whose information has been accessed would not be aware of being at increased risk and would not know to take steps to protect him or herself. Without safeguards, victims would be more vulnerable to these crimes. Current confidentiality programs designed to protect potential victims would be weakened and would make victims more vulnerable to attack by making personal information more accessible. Consistent, effective safeguards are needed when putting RFID technology into place.

h) Jeremy Smith, CA Labor Federation
Employees should not be coerced into giving up privacy in order to keep a job that requires an RFID-equipped identification card. He would not want to see employers be able to track employees on the job or even at night, off the clock. The organization stands with ACLU on privacy issues.

4. Radio-Frequency Identification Document Advisory Panel Member introductions

5. Presentations

Vulnerabilities of the Technology

a) ***Privacy and Security in Radio-Frequency Identification***
David Molnar, University of California Berkeley, Department of Computer Science

b) ***RFID Proximity Badge Cloning Demonstration***
Chris Paget, Independent Security Researcher

c) ***Soylent Badges: An Attack Surface Analysis of RFID***
Dan Kaminsky, Independent Security Researcher

Data Security

a) ***California Research Bureau RFID Hearing***
Joerg Borchert, Vice President Chip Card & Security Integrative Circuits, Infineon
Meg Hardon, Senior Policy Director, Infineon

b) ***Framing the Discussion – Testimony of AeA***
Ed Howard, Howard Advocacy, Inc.

Impact of Vulnerabilities

a) ***RFID and Personal Privacy***
Lee Tien, Electronic Frontier Foundation

b) ***Testimony of the National Network to End Domestic Violence***
Cindy Southworth, Director of Technology, National Network to End Domestic Violence

Comparison to Other ID Options and Technologies Raising Same Concerns

a) ***Written Testimony of AIM Global***
Dan Mullen, AIM Global

b) ***Different Types of Data Collection/Identification Technologies***
Comments delivered by Kathleen Carroll, Director of Government Affairs, HID Global on behalf of Dan Mullen for AIM Global

c) ***Privacy Principals for RFID***
Jim Dempsey, Policy Director, Center for Democracy and Technology

6. Closing remarks

Chris Marxen stated that a survey of panel members is being planned.

7. Public Comments

Tom Ziola, PUFCO
His company produced identification technology for military applications. Technology is not the security issue; rather, it is how data is stored, shared, transferred, accessed, and accounted for. How a system is deployed must be balanced against the application. Cost-effectiveness is a key. Policy suggestions: 1) Place minimum data on the chip. 2) Store sensitive data in secured networks, not on chips. (Note: Mr. Ziola was unable to be present during the morning public comment period. The Chair permitted Mr. Ziola to make his comments at the close of the meeting.)

The meeting adjourned at 5:00 p.m.