



**Testimony of AIM Global –
Radio Frequency Identification (RFID)
Document Advisory Panel
Public Meeting –
California Research Bureau
October 31, 2007**

1. RFID – Putting it into Perspective

AIM Global is dedicated to ensuring full compliance with all relevant personal privacy and security regulations and laws. AIM Global has taken proactive steps to address privacy questions and concerns around RFID. Our members are continually working to address valid privacy concerns where RFID technology-based solutions can be applied. This written testimony is provided to support the continued development of best practices and to provide thoughtful background on the issues that face emerging technologies like RFID.

Today's meeting may be focused on RFID technology, particularly in government identification documents, but it is important to remember that the earliest versions of RFID have been around since World War II. The technology continues to evolve as an enabling technology that can improve consumer safety and security while delivering convenience in their everyday lives. RFID is not a singular technology but a family of technologies that is already used in a variety of applications from managing herds of cattle to enabling payment at the gas pump.

Where RFID has been considered for identification applications, organizations have been astute in requiring appropriate levels of security depending on the given application. Not surprisingly, ensuring security in different applications requires an implementer to not only consider technology choice, but to carefully define business processes that will govern, for example, what information is collected, where and how it is stored, and who is permitted to access it.

Given the situational nature of choosing an appropriate level of security, a legislative definition of required security would be an attempt to force fit one solution that isn't appropriate for most RFID applications.

2. Learning from the Past and Moving Forward

Suppose, 15 years ago, you had been told about a technology that could potentially erase (or copy) all the files from your computer, aid criminals in stealing your credit card and bank information, and even make you a party to unethical and illegal activities. And suppose a state legislature proposed banning that technology. Would you have supported the legislation?

Or suppose that you had been told that there was a new technology on the horizon that would claim one life every 13 minutes in the United States alone, damage the environment, and leave the country hostage to foreign interests. Would you have supported banning that technology?

Couched in those terms, many people would.

Yet if such legislation had been enacted, neither the Internet nor the automobile would be in use today.

3. Putting the Question in Context

AIM Global believes that it is counter-productive to discuss the privacy challenges of any particular technology without an accompanying and honest assessment of the vulnerabilities of the alternatives that are currently in use. Privacy and security concerns cannot be adequately assessed if the potential vulnerability of personal information on an RFID document is examined without also weighing the vulnerabilities of this information in databases, represented in plain text, bar codes, magnetic strips, biometrics, passwords, or the potential of human error with guards looking at a photo ID. When RFID -- or any technology -- is viewed in isolation, it is easy to create scenarios that suggest that it is insecure -- without considering whether it is riskier than existing alternatives.

No means of identification is hacker-proof or foolproof. The fact that a particular technology can, with determination and in a laboratory-like setting, be compromised only proves that it is a man-made technology. What matters is the relative ease with which various technologies can be compromised, and the economic feasibility of doing it.

Thus, policymakers, business executives, and procurement officials must – if their efforts are to be credited as ones based on facts – carefully consider RFID contextually, always asking whether if used wisely it is

more or less secure than other technology choices, used with comparable wisdom.

4. What is a Practical Approach?

Today, some people are trying to portray Radio Frequency Identification (RFID) technology in much the same way as the examples mentioned in section 2. To garner attention and raise fear of RFID, some media coverage focuses only on negative or hypothetical scenarios without providing an accurate perspective on how the technology works, what it offers in comparison to alternative solutions, and its current applications that can improve and protect our quality of life.

It is doubly ironic that critics of this technology raise fears about its potential for invading privacy when in fact this technology can help protect our security, ensure the safety of the food we eat and authenticate the medications we take.

It's important to realize that RFID is not a monolithic technology. It is, instead, a family of similar but not identical systems, each with its own capabilities and limitations. Different systems have different capabilities and require different levels of security to ensure privacy. Attempting to develop a one-size-fits-all approach to privacy and security would, instead, result in a one-size-fits-none "solution" that could deprive citizens of existing and future benefits of the technology.

The question is, do you ban the technology or do you establish realistic and effective safety and security procedures (best practices) to protect users of the technology?

5. Establish a Clear Focus

What separates the parties in the RFID debate is not whether there are privacy challenges posed by RFID. What separates the parties is the level of risk. It is important to assess whether those challenges are based solely on hypothetical scenarios, whether they are unique to the technology, and whether alternatives offer greater or lesser risk. Further, it must be determined whether any potential risks are unwarranted or unprecedented, thereby warranting unusually restrictive legislative micro-management of an evolving, potentially beneficial technology.

Laws currently exist to prohibit the illicit or unethical gathering, dissemination or use of personal information. AIM Global would not oppose efforts to strengthen legislation in these areas. What we will oppose is the introduction of punitive legislation that focuses on a

particular technology rather than the illegal behavior that would result in a breach of personal privacy or security.

6. AIM Global Recommendations

AIM Global supports every consumer's right to privacy in every state. We believe that the establishment of accepted best practices -- from the selection of the appropriate type of RFID technology to recommended security measures -- is the most efficient way to outline issues, define parameters, and ensure that proper measures are available to guard against personal identity theft. The RFID industry has a vested interest in protecting the rights of consumers, and has a history of self-regulation. We encourage the California Research Bureau to consider carefully that RFID is a family of technologies that has never been breached for identity theft in more than 50 years of use; that can be more secure than other technology choices; and to legislate prematurely against its use will severely limit the development of technology that contributes to the competitiveness of all states, the safety of its citizens and the quality of the foods, medications and products available to them.

Respectfully submitted: AIM Global
31 October 2007
Sacramento, California