

The High-Tech Trust Coalition

601 Pennsylvania Ave., NW Suite 600 Washington D.C. 20004 202.682.4428

July 13, 2005

The Honorable Judy Chu
Chair, Assembly Appropriations Committee
State Capitol Room 2114
Sacramento, CA 95814

RE: OPPOSITION to SB 682 (Simitian) – RFID in Government Issued Identification Documents

Dear Assemblymember Chu:

The High-Tech Trust Coalition is writing to express its strong opposition to Senate Bill 682, which would prohibit the use of contactless integrated circuits (also known as “radio frequency identification, or RFID) in four types of government-issued identification documents, and would requiring over-reaching, expensive security requirements for the applications that are allowed. The High-Tech Trust Coalition is strongly committed to ensuring that the privacy and security of all California citizens is protected. The high-tech industry is steadfast in its efforts to earn the public’s trust in the technologies we produce, for these products are specifically designed to protect their safety and welfare; it is important that these technologies remain available to the State of California for the benefits that these promising technologies can provide. It is this commitment to the safety of California citizens and the security of their information that has prompted our opposition to SB 682, even as of the latest amended version dated July 7, 2005.

The **High-Tech Trust Coalition** is an ad hoc consortium of American businesses and trade associations whose primary purpose is to promote good consumer privacy practices within high-tech applications. As a general principle, we seek to work with federal and state legislators who are committed to protecting consumer privacy and data security by the creation of strong penalties for bad behavior and the promotion of industry and consumer best practices. We oppose any legislation that acts as a ban on technology.

Radio Frequency Identification (RFID) and smart-cards are being implemented world-wide, thanks to their ability to offer increasing privacy protections that older, outdated technologies simply cannot match. Additionally, the technology helps drastically reduce costs, increases efficiency and improves the accuracy in which information is delivered. Many governmental organizations – at the state, federal and international levels – are beginning to use these technologies in their government-issued identification documents in order to protect citizens’ physical security and privacy and to realize the considerable savings in taxpayer dollars. Further, because these technologies will factor greatly into nation-wide programs and initiatives aimed at strengthening homeland security, legislatively prohibiting their use in critical applications can only serve to make California the weakest link in our nation’s defense. For these reasons, we must respectfully oppose SB 682.

SB 682 Is Poorly Drafted, Legislating Preferences for Specific Technologies

The High-Tech Trust Coalition’s paramount criticism about SB 682 is that it embraces false fears and misrepresentations of fact to impose a ban against a technology proven both secure and reliable. To truly protect the citizens of California, SB 682 should attack the behaviors of those who would violate the public’s trust – namely, **it should create strong criminal and civil penalties against those who seek to remotely scan a person’s identification document without their knowledge or without the authority of a court-**

issued warrant. Instead, SB 682 relies on an overbroad assault on the technology, done without aid of scientific study.

Shortly after it was introduced, SB 682's over-breadth was found to have inadvertently prohibited so many common and truly beneficial uses of RFID and smartcard technologies that carve-outs needed to be granted, and ultimately the bill had to be restructured. The bill was flipped to ban four specific applications, in fact the applications which would benefit most from incorporating this secure, tested technology, while allowing other applications to go forward so long as certain specifications are met. The specifications outlined in the bill are not only highly technical and confusing; they are extremely costly, raising the price of a single card from under one dollar to around \$10. The bill also attempts to grandfather in "current applications", clearly with the intent of phasing out the technology altogether by not allowing the group that uses it to grow or change.

The approach SB 682 takes to public policy is deeply flawed, as it will produce law that will prohibit current and future beneficial uses and innovations not yet known to the legislature – innovations that will save time, save money, and most importantly, save lives. The High-Tech Trust Coalition applauds the author's concern over privacy rights, but respectfully recommends that resolution be sought not by prohibiting the use of a technology – which is inherently benign – but instead creating privacy and data safeguards that are necessary when using the technology.

SB 682 Ignores Federal and International Technology Standards that Protect Privacy

Smart card technology, both in contactless or contact forms, is widely recognized as having the strongest security features of any identity token technology and is the best choice for improving the security of identity documents. Many nations, international organizations, and security-concerned industries have turned to RFID and contactless ICs to confidently provide for the integrity and safety of stored and transmitted data. At the center of these decisions are internationally accepted general security standards, such those found under FIPS 201, FIPS 140-2 and ISO 14443, standards that do not rely on proprietary intellectual property.

As an example, the International Civil Aviation Organization (ICAO) has set the standard for security specifications surrounding contactless travel documents. The ICAO's standards include requirements for Basic Access Controls (BAC) to further protect passport data, as well as best practices for all those who maintain and secure that data. More than 100 of the 188 ICAO member countries have successfully implemented contactless ICs into travel documents using their security standards. Further, officials from the U.S. State Department have indicated that they, too, will be strongly considering the use of BAC and ICAO standards in the U.S. electronic passports. In the news just last month, J.P. Morgan Chase & Co., the nation's largest credit-card issuer, recently announced their roll-out of RFID enabled credit cards, as did American Express. The state of Virginia, having been the target of driver license fraud for the September 11 terrorist attacks, is considering embracing RFID technology in their state issued identification in order to prevent such occurrences in the future. A proven technology with more than 10 years of usage globally in a variety of demanding financial and identity applications, public and private organizations alike are employing technology to ensure consumers' data security.

SB 682 Does Not Promote Privacy Protection

The high tech community vigorously believes that protecting consumer privacy is a top priority – one that technology can play a strong role in. While any type of communication can be protected, the nature of RFID lends itself to a much higher level of protection than the technologies that it will ultimately replace. As such, it can be safely used in a number of different privacy-sensitive areas such as financial transactions and healthcare environments – and in secure identity documents. The level of security incorporated into the technology should mirror the degree of sensitivity of the information stored on the chip.

It is important to note that technology alone is not the answer. It must be backed up by a strong commitment to best practices by all involved – from those who collect the data, those who store the data, and those who design the systems on which the data is used. By using a combination of powerful encryption, unique access keys and strong authentication protocols, coupled with a strong commitment to best practices, securing important information from prying eyes will be increased in very real and substantial ways. The high-tech

community is committed to the best practices surrounding the use of RFID and contactless ICs in identity documents:

- Privacy & Security Policies: Organizations that collect information must have strong policies on hand that describes what information is collected, how it is stored, who has access to it, and how it will be protected.
- Accuracy & Integrity: When someone is given an identity document that contains a contactless IC, strict care must be taken to ensure that all information is accurate, as well as held strictly confidential.
- Security, Security, Security: All information must be protected at all times, from the moment of collection, while being stored, and even when in use. No exceptions.
- The ID Must Be Secure As Well: The identity document needs to protect its contents from being copied, altered or hacked, to prevent unauthorized use, misuse, or disclosure of any personal information it carries.
- Protected Exchange of Information: Transferring of information between the ID and the reader must safeguard against unauthorized capture of information and use of the data to impersonate anyone.
- Authorized Access to Information: Access must only be granted to those who the issuer deems necessary – and even then the information released should be only to authorized persons or systems.
- Internal Commitment to Security: Anyone using the system must be trained and monitored to ensure that all the security policies and practices put in place are adhered to.

The high tech industry supports and commends the author's efforts to protect the privacy of California residents; however, we believe SB 682 will do far more harm to California residents than it will help. We are excited over the possibility that innovative technologies such as RFID can help save California residents billions of dollars in healthcare costs alone – not to mention the billions of taxpayer dollars saved in the protecting the physical security of California residents' personal data and property. **The undersigned companies believe that given the proper commitment to best practices and strong criminal and civil penalties, the Golden State can ensure the security, the safety, and the savings that every California tax payer deserves. Until SB 682 reflects this commitment, we must oppose SB 682.** If you have any questions, please do not hesitate to contact Roxanne Gould at 916/443-9059 x101 or via email at roxanne_gould@aeonet.org.

Respectfully Submitted,

AeA (American Electronics Association)
ActivCard
AIM Global
Aubrey Group, Inc.
Axalto
California Chamber of Commerce
CMTA (California Manufacturer & Technology Association)
EDS
Elpac Electronics, Inc.
EPC Global, Inc.

Gemplus
InCom Corp.
Infineon Technologies
ITAA (Information Technology Association of America)
Kimberly-Clark Corporation
Matheson Tri-Gas
MAXIMUS
National Semiconductor
Natoma Technologies, Inc.
Oberthur Card Systems
Oracle Corporation

Philips Electronics
Precision Dynamics
SAS
SIA (Semiconductor Industry Association)
Sonnet Technologies, Inc.
Symbol Technologies
Texas Instruments
VICA (Valley Industry Commerce Association)
VEDC, Inc.

CC: Members, Assembly Appropriation Committee
Senator Simitian
Cynthia Bryant, Office of the Governor
Geoff Long, Chief Consultant to Assembly Appropriations Committee
Richard Mersereau, Chief Consultant to Assembly Republican Caucus
Happy Chastain, State & Consumer Affairs
Dan Jones, Office of Homeland Security