Identity Information Protection Act (SB 30):
Setting the Record Straight

Myth: RFID chips have been used around the world for many years with no instances of breach or identity theft.
Fact: The personal information on RFID chips can be read at a distance without an individual ever knowing that it has been read or who has read it. If insecure RFID technology is used in state-issued identification documents, the private information of millions of Californians could be stolen without a trace. RFID technology has been cracked many times, all over the world.

- Cracked the California State Capitol identification cards and gained access to member-only, secure entrances (2006)
- Cracked the VeriChip - the RFID chip approved for implantation in humans (2006)
- Cracked the RFID chips used in the Dutch and British e-passport (2006)
- Cracked the RFID chips in the Exxon Mobil gasoline-payment passes (2005)
- Cracked the RFID chips used in automobile key fob anti-theft devices (2005)

Cracks of RFID technology have very real consequences. Law enforcement officials suspect that criminals have stolen two of soccer superstar David Beckham's custom BMW automobiles by preying upon the vulnerabilities of their RFID security systems. Thieves simply read and spoofed the information on the inadequately protected RFID chip in Beckham's key fob and drove away with his cars.

The electronics industry admits that RFID technology without proper protections is very vulnerable and creates risks to privacy, personal security, and public safety. In January 2006, they told the US Department of State and the Department of Homeland Security the following about the use of RFID technology in government identification documents without the type of protections delineated in SB 30[1]:

- "highly susceptible to forgery." (American Electronics Association, AeA)
- "A potential illicit hacker could very easily read (again, from a distance) the unique ID contained…and easily create a duplicate." (AeA)
- "Perversely maximize the possibility…of an illicit actor 'tracking' a person at very long ranges…would potentially threaten individual U.S. citizen privacy." (AeA)
- Basic RFID technology does not have necessary technological protections to eliminate the risk of terrorists, criminals, or illegal aliens…spoofing or counterfeiting PASS cards to enter the United States undetected." (Smart Card Alliance)

Myth: The requirements in SB 30 are equivalent to locking in the 8-track tape.
Fact: Claiming that SB 30 stifles technology is tantamount to saying that requiring airbags or seatbelts in cars stifles automobile innovation.

- **SB 30 is outcome-based and technology neutral. Industry is encouraged to innovate and use whatever type of technology leads to increased safety.** For example, 1798.10(a)(1)- Tamper Resistant Features: "In order to prevent duplication, forgery, or cloning of the identification document, the identification document shall incorporate tamper-resistant features."
- **Companies already produce compliant chips and the standards are similar to what companies advocate to the federal government.** (See January 2006 AeA and Smart Card Alliance Government Letters).
- **Industry leaders (including AeA and the Information Technology Association of America (ITAA) went neutral on the identical bill last year because SB 30 is reasonable legislation that makes sense for Californians and for companies.** People will feel safer buying and using RFID technology if they do not have to worry that they are risking their privacy, personal security, and financial safety.

[1] http://www.aeanet.org/governmentaffairs/AeA_Letter_Jan_30_2006.asp; ://www.smartcardalliance.org/pages/publications-whti

Myth: RFID chips do not transmit any personal information, just a number.
Fact: RFID chips transmit whatever personal information is encoded on them, from a name and address to a social security number.

RFID chips are tiny computer chips that can be encoded with any information. Without proper technological protections, such as those included in SB 30, whatever information is on the chip can then be read at a distance without anyone ever knowing it has been read. All someone has to do to track you, steal your information, or copy your Capitol badge is read the number on the RFID. But, RFID chips can also be encoded with much more than a number and without SB 30, there is no guidance on what types of safeguards are necessary to protect this information.

SB 30 provides basic protections for any California ID containing an RFID tag: tamper resistant features to prevent forgery and cloning; some type of authentication process to ensure that the card is legitimate and the reader is authorized, and notice that the ID contains an RFID tag so people can take their own steps to protect personal information. See 1798.10(a)(1-3). SB 30 also includes additional layers of protection if the tag is encoded with other types of personal information, such as name, address or social security number. See 1798.10(a)(4-6).

Myth: RFID chips can only be read from a few inches away.
Fact: **The information on RFID chips can be read much farther away than the "intended" read range quoted by manufacturers.**

The U.S. State Department demonstrated that a passive RFID chip, intended by the manufacturer to read from 4 inches away, could actually be read from 2-3 feet away. A May 2005 report released by the Government Accountability Office found that passive RFID tags can read at up 20 feet.[2] In August 2005, Los Angeles-based Flexilis read an RFID chip from 69 feet away.

It is the strength of the reader that determines the read-range of the tag. While the manufacturer's reader might only read the tag from a few inches, other people who want to do harm can use more powerful readers to access information from a distance, without a person's knowledge. Just last summer, a computer security consultant walked the halls of the Sacramento Capitol and was able read several Senate and Assembly entry badges with a reader stowed in his bag, without anyone ever knowing.

Readers will only continue to get more powerful and that is why the technology-neutral, outcome-based standard in SB 30, requiring that RFID chips in our identification documents are able to differentiate between authorized readers and rogue readers, is so important. See 1798.10(a)(2).

Myth: RFID chips are "passive" and that makes them safe.
Fact: The information on passive RFID chips can still be read from several feet away- leading to significant privacy, safety, and security concerns.

The only difference between an "active" chip and a "passive" chip is that a passive chip does not have its own power source. A passive RFID chip waits to automatically transmit its information until a reader "wakes it up" by sending it power through a radio frequency. But, since you can buy a reader off the internet for just a few hundred dollars and read the information from passive chips from several feet away, the privacy, safety, and security concerns are no different between active and passive chips.

For more information on SB 30 and the privacy, personal security, and public safety issues related to the use of RFID technology in state-issued identification documents, please see www.aclunc.org/tech.

[2] GAO-05-551, "Information Security Radio Frequency Identification Technology in the Federal Government." United States Government Accountability Office. Released May 2005. http://www.gao.gov/new.items/d05551.pdf