

Calif. RFID Bill Is Unconstitutional

Several provisions in the state's Identity Information Protection Act of 2005 are unenforceable and likely to be invalidated by the courts.

July 18, 2005—California Senate Bill 682, the Identity Information Protection Act of 2005, is one of the first state legislative proposals directed at regulating RFID. Several of its provisions are unconstitutional and likely to be invalidated by the courts.

The most obvious constitutional deficiency is an ill-defined attempt to criminalize the secretive use of remote reading of RFID tags. A section of proposed Senate Bill 682 provides that: "A person or entity that knowingly or willfully remotely reads or attempts to remotely read a person's identification document using radio waves without the knowledge of that person shall be punished by imprisonment in a county jail for up to one year, a fine of not more than five thousand dollars (\$5,000), or both that fine and imprisonment."

It is important to note that SB 682 does not define the phrase "knowingly or willfully." This is a glaring omission that likely renders this section unconstitutional. A constitutional definition of a crime requires more than simply the commission of the act and a general state of mind.

Let's compare SB 682's criminal section with the crime of burglary. Section 459 of the California Penal Code declares a person guilty of the crime of burglary if he "enters a house, room, apartment, tenement, shop, warehouse, store, mill, barn, stable, outhouse or other building, tent, vessel...with intent to commit grand or petit larceny or any felony." Thus, the crime of burglary requires proof of entry, plus proof of the intent to commit a larceny or felony.

By contrast, SB 682 does not require proof of any criminal intent in addition to the secretive act of remote reading. A misguided jury could simply conclude that the crime had been proved by the act of the secretive remote reading itself. A conviction obtained under such a defective statute would be successfully reversed.

SB 682 also places onerous and unreasonable restrictions on government identification cards containing RFID tags. The cards must incorporate strong encryption and "mutual authentication." The reader must also "...reliably detect unauthorized identification documents." The proposed statute does not define how unauthorized identification documents are to be detected.

The bill prohibits the following government identification documents from containing RFID tags: driver's licenses, student identification cards, health insurance or benefit cards and public library cards. However, the proposed statute exempts numerous identification documents from regulation. These include identification documents for inmate and jail employees, firefighters or emergency medical technicians, hospital patients, toll machines, secure access to public buildings or parking, professional or business licenses, and any other such documents the legislature deems appropriate.

SB 682 dubiously extends privacy protection to a unique number transmitted by an RFID tag to a remote reader. This proposed statute is based upon the mistaken notion that the perceived privacy violation is the transmittal of that number by the RFID tag to the remote reader. This misconception is significant. By itself,

that number means nothing. Only when that number is received by the remote reader and processed further does the association between the number and the identification document become “personal.”

A court challenge to SB 682 would likely succeed. The court would strictly scrutinize the bill and issue a declaratory judgment that the bill offends the due process clauses of both the California and United States constitutions. The blanket prohibition against the use of RFID tags in many government-issued identification cards also likely affects interstate commerce, in violation of the U.S. Constitution. The broad exemptions for most identification cards currently in use leave its eventual application open to a persuasive argument that the statute may be selectively or arbitrarily enforced.

California has no state interest in regulating the use of RFID tags in government-issued identification cards. But a case could be made for the regulation or restriction of remote readers, much as both state and federal authorities regulate the use or possession of credit card skimmers. An even more compelling case could be made for the regulation of the data processors, the subject of the federal Personal Data Privacy and Security Act of 2005, recently introduced by U.S. Senators Arlen Specter and Patrick Leahy.

It appears that California has used a sledgehammer to swat the proverbial fly.

Daniel W. Perry (dan@danielperry.com) is an attorney and a former county judge in Orlando, Fla., practicing in the area of information and data privacy law. He consults with small to midsize businesses on compliance issues regarding federal and state privacy and data protection regulations.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved