

AMENDED IN ASSEMBLY JUNE 23, 2005

AMENDED IN ASSEMBLY JUNE 15, 2005

AMENDED IN SENATE MAY 11, 2005

AMENDED IN SENATE MAY 4, 2005

AMENDED IN SENATE MARCH 31, 2005

SENATE BILL

No. 682

Introduced by Senator Simitian

February 22, 2005

An act to add Article 4 (commencing with Section 1798.9) to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 682, as amended, Simitian. Identity Information Protection Act of 2005.

Existing law, the Information Practices Act of 1977, regulates the collection and disclosure of personal information regarding individuals by state agencies, except as specified. The intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the act is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains.

This bill would enact the Identity Information Protection Act of 2005. The act would require identification documents, *except as specified*, that are created, mandated, purchased, or issued by various public entities, and that contain a contactless integrated circuit or other device that uses radio waves to broadcast personal information or to enable personal information to be read remotely, to meet specified

requirements. The bill would provide 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 his or her knowledge shall be punished by imprisonment in a county jail for up to one year, a fine of not more than \$5,000, or both that fine and imprisonment.

In addition, because the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the Information Practices Act of 1977, which would include this act, is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains, and because remotely reading or attempting to remotely read a person's identification document without his or her knowledge would be punishable as a misdemeanor, this bill would create a new crime, thereby imposing a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: yes.

The people of the State of California do enact as follows:

1 SECTION 1. This act shall be known and may be cited as the
2 Identity Information Protection Act of 2005.

3 SEC. 2. The Legislature hereby finds and declares all of the
4 following:

5 (a) The right to privacy is a personal and fundamental right
6 protected by Section 1 of Article I of the California Constitution
7 and by the United States Constitution. All individuals have a
8 right of privacy in information pertaining to them.

9 (b) Easy access to the information found on drivers' licenses
10 and other similar identification documents facilitates the crime of
11 identity theft, a crime that is a major concern in California. More
12 than ~~39,000~~ 43,000 Californians reported being victims of this
13 crime in ~~2003~~ 2004.

1 (c) This state has previously recognized the importance of
2 protecting the confidentiality and privacy of an individual’s
3 personal information contained in identification documents such
4 as drivers’ licenses.

5 (d) The inclusion in identification documents of contactless
6 integrated circuits or other devices that use radio waves to
7 broadcast data or to enable data to be scanned secretly and
8 remotely will greatly magnify the potential risk to individual
9 privacy, safety, and financial security that can occur from
10 unauthorized interception and use of personal information. The
11 inclusion of those devices will also make it possible for any
12 person or entity with access to a reader to engage in the secret
13 tracking of Californians on an unprecedented scale.

14 SEC. 3. Article 4 (commencing with Section 1798.9) is added
15 to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code,
16 to read:

17
18 Article 4. Identity Documents

19
20 1798.9. For purposes of this article, the following definitions
21 shall apply:

22 (a) “Authentication” means the process of applying a specific
23 mathematical algorithm to data or identification documents, or
24 both, so as to accomplish either of the following:

25 (1) Prove or establish that the data and the identification
26 document containing the data, including any contactless
27 integrated circuit in the identification document, were issued by
28 the responsible issuing state or local governmental body.

29 (2) Ensure that a reader, as defined in subdivision (h), is
30 permitted under California law to access such data or
31 identification document.

32 (b) “Authorized reader” means a reader, as defined in
33 subdivision (h), that, with respect to a particular identification
34 document, (1) is permitted under California law to remotely read
35 the personal information broadcast or transmitted by that
36 identification document, (2) is being used for a lawful purpose,
37 and (3) is fully in accord with the requirements of subdivision (a)
38 of Section 1798.10.

1 (c) “Contactless integrated circuit” means a data carrying unit,
2 such as an integrated circuit or computer chip, that can be read
3 remotely.

4 (d) “Encryption” means the process of applying a specific
5 mathematical algorithm to data so as to protect the confidentiality
6 of that data by rendering that data unintelligible to an
7 unauthorized party.

8 (e) “Identification document” means any document containing
9 personal information that an individual uses alone or in
10 conjunction with any other information to establish his or her
11 identity. Identification documents specifically include, but are
12 not limited to, the following:

13 (1) Driver’s licenses or identification cards.

14 (2) Identification cards for employees or contractors.

15 (3) Identification cards issued by educational institutions.

16 (4) Health insurance or benefit cards.

17 (5) Benefit cards issued in conjunction with any
18 government-supported aid program.

19 (6) Licenses, certificates, registration, or other means to
20 engage in a business or profession regulated by the Business and
21 Professions Code.

22 (7) Library cards issued by any public library.

23 (f) “Mutual authentication” means the use of authentication, as
24 defined in subdivision (a), to ensure that authorized readers, as
25 defined in subdivision (b), can reliably detect unauthorized
26 identification documents, and that authorized identification
27 documents can be read only by those authorized readers.

28 (g) “Personal information” includes any of the following: an
29 individual’s name, address, telephone number, e-mail address,
30 date of birth, religion, ethnicity, nationality, photograph,
31 fingerprint or other biometric identification, social security
32 number, or any other unique personal identifier or number.

33 (h) “Reader” means a scanning device that is capable of using
34 radio waves to communicate with a contactless integrated circuit
35 or other device using radio waves and read the personal
36 information broadcast or transmitted by that integrated circuit or
37 other device.

38 (i) “Remotely” means that no physical contact between the
39 integrated circuit or device and a reader is necessary in order to
40 transmit data.

1 (j) “Shield devices” mean physical or technological
2 protections available to stop the broadcast or transmission of
3 personal information programmed on or into a contactless
4 integrated circuit or other devices using radio waves.

5 (k) “Unique identifier number” means a random string of
6 numbers that is encoded onto the contactless integrated circuit or
7 other device.

8 1798.10. (a) Except as provided in subdivisions (b) and (c),
9 all identification documents created, mandated, purchased, or
10 issued by a state, county, or municipal government, or
11 subdivision or agency thereof that contain a contactless
12 integrated circuit or other device that uses radio waves to
13 broadcast personal information or to enable personal information
14 to be read remotely shall meet these requirements:

15 (1) The identification document shall not contain, transmit, or
16 enable the remote reading of; any personal information other than
17 a unique personal identifier number in or from its contactless
18 integrated circuit or other device that uses radio waves.

19 (2) The identification document shall implement strong
20 encryption to protect against the unauthorized reading of
21 transmitted information. The confidentiality provided by that
22 encryption shall at all times be at least as strong as RSA
23 encryption using a key length of 1024 bit as understood on the
24 effective date of this article. In the event that this standard is
25 cracked and hence no longer capable of protecting against the
26 unauthorized reading of transmitted information, the
27 identification document shall implement a stronger encryption
28 standard that will ensure protection against the unauthorized
29 reading of transmitted information.

30 (3) The identification document shall implement mutual
31 authentication to protect against the unauthorized transmission of
32 information from the identification document to unauthorized
33 readers. The protection provided by that mutual authentication
34 shall at all times and at a minimum incorporate the highest
35 standards of active mutual authentication contained in *the*
36 *document issued by the International Organization for Standards*
37 *known as the Common Criteria ISO 15408* or its equivalent as
38 subsequently updated. The identification document shall in no
39 case incorporate a lower standard for active mutual

1 authentication than the highest standard articulated by Common
2 Criteria ISO 15408 at the time of the effective date of this article.

3 (4) In order to ensure that the holder of the identification
4 document affirmatively consents to each reading of the
5 identification document, each identification document shall
6 implement at least one of the following privacy safeguards:

7 (A) An access control protocol requiring the optical or other
8 ~~non-radio~~ *nonradio* frequency reading of information from the
9 identification document prior to each transmission or broadcast
10 of data using radio waves, without which the identification
11 document will not transmit or broadcast personal information
12 using radio waves.

13 (B) A shield device that, when used to protect the
14 identification document, can prevent any communication of data
15 using radio waves between the contactless integrated circuit and
16 any reader under any circumstances.

17 (C) A contactless integrated circuit or other device that is
18 normally not remotely readable, accessible, or otherwise
19 operational under any circumstances, and only remotely readable,
20 accessible, or operational while being temporarily switched on or
21 otherwise intentionally activated by a person in physical
22 possession of the identification document. ~~Any such~~ *The device*
23 ~~must~~ *shall* only be remotely readable while the person
24 intentionally uses the switch intending that the identification
25 document be read.

26 (5) The issuing entity of an identification document shall
27 communicate in writing to the person to whom the document is
28 issued, all of the following:

29 (A) That the identification document contains a contactless
30 integrated circuit or device that can broadcast a unique personal
31 identifier number or enable that number to be read remotely
32 without his or her knowledge.

33 (B) That countermeasures, such as shield devices, may be used
34 to help the person control the risk that his or her unique personal
35 identifier number will be broadcast or read remotely without his
36 or her knowledge.

37 (C) The location of all readers used or intended to be used by
38 the issuing authority or by any other entity known to that
39 authority to read the unique personal identifier number on the
40 identification document.

1 (D) Any information that is being collected at the time the
2 contactless integrated circuit or other device is read or that is
3 being stored regarding the individual in a database.

4 (E) Additional annual notice shall be communicated in writing
5 of any new shield devices in existence or changes in the location
6 of readers or the information collected or stored in the database.

7 (b) Subdivision (a) shall not apply to:

8 (1) An identification document that is part of a contactless
9 integrated system used by a state, county, or municipal
10 government, or subdivision or agency thereof that is operational
11 and in use prior to January 1, 2006, if all of the following apply:

12 (A) The system is not used for any purpose other than the
13 purpose or purposes of the system on the effective date of this
14 article.

15 (B) The amount, type, or types of information stored,
16 broadcast, or transmitted by the contactless integrated circuit is
17 the same as, or less or fewer than, on the effective date of this
18 article.

19 (C) The contactless integrated circuit is being issued to the
20 same group or groups as, or fewer or smaller groups of people
21 than, were issued the contactless integrated circuit on the
22 effective date of this article.

23 (2) An identification document issued to a person who is
24 incarcerated in the state prison or a county jail, detained in a
25 juvenile facility operated by the Division of Juvenile Facilities in
26 the Department of Corrections and Rehabilitation, or housed in a
27 mental health facility, pursuant to a court order after having been
28 charged with a crime, or to a person pursuant to court-ordered
29 electronic monitoring.

30 (3) An identification document issued to a person employed
31 by a state prison, county jail, or juvenile facility operated by the
32 Division of Juvenile Facilities in the Department of Corrections
33 and Rehabilitation if the document is not removed from the
34 facility and the requirements of paragraph~~(4)~~ (5) of subdivision
35 (a) apply.

36 (4) An identification document issued to a firefighter *or*
37 *emergency medical technician* if the document is used only while
38 the firefighter *or emergency medical technician* is on active duty
39 and the requirements of paragraph~~(4)~~ (5) of subdivision (a)
40 apply.

1 (5) An identification document issued to a patient who is in
2 the care of a government-operated hospital, ambulatory surgery
3 center, or oncology or dialysis clinic if the document is ~~(1) (A)~~
4 valid for only a single episode of care, ~~(2) (B)~~ removed from the
5 patient at the time the patient is discharged, and ~~(3) (C)~~ contains
6 no personal information other than a unique identifier number,
7 and a patient returning for a new episode of care is assigned a
8 new unique identifier number.

9 (6) An identification document issued to a patient by
10 emergency medical services for triage or medical care during a
11 disaster and immediate hospitalization or immediate outpatient
12 care directly related to a disaster, as defined by the local
13 Emergency Medical Services agency organized under Section
14 1797.200 of the Health and Safety Code.

15 (7) *An identification document issued to a person for the*
16 *limited purpose of collecting funds for the use of a toll bridge,*
17 *such as the FasTrak system, if the requirements of paragraphs*
18 *(1), (4), and (5) of subdivision (a) are met.*

19 (8) *An identification document that is issued to a person for*
20 *the limited purpose of facilitating secured access by the*
21 *identification document holder to a secured public building or*
22 *parking area, if the requirements of paragraphs (1), (4), and (5)*
23 *of subdivision (a) are met.*

24 (9) *A license, certificate, registration, or other authority for*
25 *engaging in a business or profession regulated under the*
26 *Business and Professions Code, if the requirements of*
27 *paragraphs (1), (4), and (5) of subdivision (a) are met.*

28 (10) *An identification document for which the Legislature*
29 *determines that the standards of subdivision (a) of Section*
30 *1798.10 do not apply because of the existence of a compelling*
31 *state interest and that there is no means less intrusive to the*
32 *individual's privacy and security to achieve the compelling state*
33 *interest.*

34 (c) Except for identification documents listed in subdivision
35 (b), the following identification documents created, mandated,
36 purchased, or issued by a state, county, or municipal government,
37 or subdivision or agency thereof, shall not contain a contactless
38 integrated circuit or other device that uses radio waves to
39 broadcast personal information or to enable personal information
40 to be read remotely:

1 (1) Drivers' licenses or identification cards *issued pursuant to*
2 *Section 13000 of the Vehicle Code.*

3 (2) Identification cards issued to students by educational
4 institutions, including but not limited to, all K-12 schools, the
5 University of California, California State Universities, and the
6 community colleges.

7 (3) Health insurance, health benefit, and benefit cards issued
8 in conjunction with any government-supported aid program.

9 (4) Library cards issued by any public library.

10 1798.12. A person or entity that knowingly or willfully
11 remotely reads or attempts to remotely read a person's
12 identification document using radio waves, without the
13 knowledge of that person shall be punished by imprisonment in a
14 county jail for up to one year, a fine of not more than five
15 thousand dollars (\$5,000), or both that fine and imprisonment.

16 SEC. 4. No reimbursement is required by this act pursuant to
17 Section 6 of Article XIII B of the California Constitution because
18 the only costs that may be incurred by a local agency or school
19 district will be incurred because this act creates a new crime or
20 infraction, eliminates a crime or infraction, or changes the
21 penalty for a crime or infraction, within the meaning of Section
22 17556 of the Government Code, or changes the definition of a
23 crime within the meaning of Section 6 of Article XIII B of the
24 California Constitution.