

AMENDED IN ASSEMBLY AUGUST 17, 2006
AMENDED IN ASSEMBLY SEPTEMBER 2, 2005
AMENDED IN ASSEMBLY AUGUST 25, 2005
AMENDED IN ASSEMBLY JUNE 20, 2005
AMENDED IN SENATE MAY 27, 2005
AMENDED IN SENATE MAY 3, 2005
AMENDED IN SENATE APRIL 12, 2005
AMENDED IN SENATE MARCH 31, 2005

SENATE BILL

No. 768

Introduced by Senator Simitian
(Principal coauthor: Assembly Member Torrico)
(Coauthor: Assembly Member Evans)

February 22, 2005

An act to add *and repeal* Article 4 (commencing with Section ~~1798.9~~ *to 1798.10*) of Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, *and to add and repeal Article 13 (commencing with Section 11147) of Chapter 1 of Part 1 of Division 3 of Title 2 of the Government Code*, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 768, as amended, Simitian. Identity Information Protection Act of ~~2005~~. 2006.

(1) 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~~ 2006. ~~The~~ *Until December 31, 2012, or as otherwise specified, the act would require identification documents, except as defined and with specified exceptions, that are created, mandated, purchased, or issued by various public entities that use radio waves to broadcast personal information transmit data, or to enable personal information data to be read remotely, to meet specified requirements. The bill would provide that a person or entity that intentionally remotely reads or attempts to remotely read a person's identification document using radio waves without his or her knowledge and prior consent, or that knowingly discloses, or causes to be disclosed, operational system keys, as described, 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. The bill would further authorize declaratory or injunctive relief or a writ of mandate and attorney's fees and costs under specified circumstances.*

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 *or disclosing operational system keys* would be punishable as a misdemeanor, this bill would create a new crime, thereby imposing a state-mandated local program.

(2) *Existing law establishes in the Department of Consumer Affairs, the Office of Privacy Protection for the purpose of protecting the privacy of individuals' personal information and developing fair information practices for state agencies. Existing law establishes in the California State Library, the California Research Bureau with responsibilities to conduct research on various policy issues.*

This bill would require the California Research Bureau to submit a report to the Legislature on security and privacy for government-issued, remotely readable identification documents. The bill would require the bureau to submit the report within 270 days of

receiving a request from the Office of the pro Tempore of the Senate or the Office of the Speaker of the Assembly, or before June 30, 2007, whichever is earlier. The bill would require the bureau to establish an advisory board, to be comprised of specified government officials and representatives from industry and privacy rights organizations, to make recommendations and provide technical advice to the bureau in preparing the report.

(3) 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~~ 2006.

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 43,000 Californians reported being victims of this crime in
13 2004.~~

14 (e)
15 (b) This state has previously recognized the importance of
16 protecting the confidentiality and privacy of an individual's
17 personal information contained in identification documents such
18 as drivers' licenses.

19 ~~(d) Identification documents that use radio waves to broadcast
20 data or to enable data to be scanned secretly and remotely will
21 greatly magnify the potential risk to individual privacy, safety,
22 and financial security that can occur from unauthorized~~

1 interception and use of personal information. These identification
 2 documents will also make it possible for any person or entity
 3 with access to a reader to engage in the secret tracking of
 4 Californians on an unprecedented scale.

5 *(c) It is the intent of the Legislature that the privacy and*
 6 *security protections in this article that apply to remotely*
 7 *readable identification documents created, mandated, purchased,*
 8 *or issued by a state, county, or municipal government, or*
 9 *subdivision or agency thereof, are interim measures until*
 10 *subsequent legislation or regulations are enacted based on new*
 11 *information, including, but not limited to, information provided*
 12 *by the California Research Bureau.*

13 *(d) Notwithstanding any other provision of this act, it is the*
 14 *intent of the Legislature that the interim measures contained*
 15 *herein be replaced by a statewide legislative or regulatory*
 16 *framework in the most timely and expeditious fashion possible*
 17 *following the issuance of recommendations by the California*
 18 *Research Bureau.*

19 SEC. 3. Article 4 (commencing with Section ~~1798.9~~)
 20 ~~1798.10~~) is added to Chapter 1 of Title 1.8 of Part 4 of Division
 21 3 of the Civil Code, to read:

22

23 Article 4. Identity Documents

24

25 ~~1798.9.~~ For purposes of this article, the following definitions
 26 shall apply:

27 (a) ~~“Authentication” means the process of applying a specific~~
 28 ~~mathematical algorithm to data or identification documents, or~~
 29 ~~both, so as to accomplish either of the following:~~

30 (1) ~~Prove or establish that the data and the identification~~
 31 ~~document containing the data were issued by the responsible~~
 32 ~~issuing state or local governmental body.~~

33 (2) ~~Ensure that a reader, as defined in subdivision (l), is~~
 34 ~~permitted under California law to access such data or~~
 35 ~~identification document.~~

36 (b) ~~“Authorized reader” means a reader, as defined in~~
 37 ~~subdivision (l), that, with respect to a particular identification~~
 38 ~~document, (1) is permitted under California law to remotely read~~
 39 ~~the personal information broadcast or transmitted by that~~
 40 ~~identification document, (2) is being used for a lawful purpose;~~

1 and (3) is fully in accord with the requirements of subdivision (a)
2 of Section 1798.10.

3 (e) ~~“Contactless identification document system” means a~~
4 ~~group of identification documents issued and operated under a~~
5 ~~single authority that use radio waves to transmit personal~~
6 ~~information remotely to readers intended to read that~~
7 ~~information. In a contactless identification document system,~~
8 ~~every reader must be able to read every identification document~~
9 ~~in the system.~~

10 (d) ~~“Cryptographic protocol” means a sequence of interactions~~
11 ~~between two parties to ensure that only authorized parties can~~
12 ~~communicate with one another.~~

13 (e) ~~“Encryption” means the process of applying a specific~~
14 ~~mathematical algorithm to data so as to protect the confidentiality~~
15 ~~of that data by rendering that data unintelligible to an~~
16 ~~unauthorized party.~~

17 (f) ~~“Identification document” means any document containing~~
18 ~~personal information that an individual uses alone or in~~
19 ~~conjunction with any other information to establish his or her~~
20 ~~identity. Identification documents specifically include, but are~~
21 ~~not limited to, the following:~~

- 22 (1) ~~Driver’s licenses or identification cards.~~
- 23 (2) ~~Identification cards for employees or contractors.~~
- 24 (3) ~~Identification cards issued by educational institutions.~~
- 25 (4) ~~Health insurance or benefit cards.~~
- 26 (5) ~~Benefit cards issued in conjunction with any~~
27 ~~government-supported aid program.~~
- 28 (6) ~~Licenses, certificates, registration, or other means to~~
29 ~~engage in a business or profession regulated by the Business and~~
30 ~~Professions Code.~~
- 31 (7) ~~Library cards issued by any public library.~~

32 (g) ~~“Key” means a string of bits of information used as part of~~
33 ~~a cryptographic algorithm used in encryption.~~

34 (h) ~~“Key establishment” means a protocol by which two~~
35 ~~parties jointly generate a key for use in a subsequent~~
36 ~~cryptographic protocol.~~

37 (i) ~~“Mutual authentication” means the use of authentication, as~~
38 ~~defined in subdivision (a), to ensure that authorized readers, as~~
39 ~~defined in subdivision (b), can reliably detect unauthorized~~

1 identification documents, and that authorized identification
2 documents can be read only by those authorized readers.

3 (j) “Personal information” includes any of the following: an
4 individual’s name, address, telephone number, e-mail address,
5 date of birth, religion, ethnicity, nationality, photograph,
6 fingerprint or other biometric identification, social security
7 number, or any other unique personal identifier or number.

8 (k) “Public key” means a form of cryptography in which the
9 key is split into two parts, a public key, which is known to all,
10 and a secret key, which is known to only one party.

11 (l) “Reader” means a scanning device that is capable of using
12 radio waves to communicate with an identification document and
13 read the personal information broadcast or transmitted by that
14 identification document.

15 (m) “Remotely” means that no physical contact between the
16 identification document and a reader is necessary in order to
17 transmit data.

18 (n) “Session” is a sequence of interactions between the
19 identification document and the reader that represents one logical
20 reading of the identification document by the reader and begins
21 when either the reader or identification document initiates
22 communication with the other and ends when either the reader or
23 identification document becomes out of range or explicitly sends
24 a message closing the session.

25 (o) “Session key” means a key used only for a single session
26 between two parties.

27 (p) “Shared secret” means a key shared between two parties
28 and no others.

29 (q) “Shield devices” mean physical or technological
30 protections available to stop the broadcast or transmission of
31 personal information programmed on or into an identification
32 document using radio waves.

33 (r) “Single episode of care” means an inpatient hospital stay
34 through discharge or specific course of therapy or treatment for
35 outpatient care.

36 (s) “Unique identifier number” means a randomly assigned
37 string of numbers that is encoded onto the identification
38 document.

39 1798.10. (a) Except as provided in subdivisions (b) and (c)
40 *subdivision (b)*, all identification documents created, mandated,

1 purchased, or issued by a state, county, or municipal government,
2 or subdivision or agency thereof, that use radio waves to transmit
3 personal information *data* or to enable personal information *data*
4 to be read remotely shall meet these requirements:

5 ~~(1) The identification document shall not transmit or enable~~
6 ~~the remote reading of any personal information other than a~~
7 ~~unique personal identifier number using radio waves.~~

8 ~~(2) (A) The identification document shall implement mutual~~
9 ~~authentication in order to prevent the transmission of information~~
10 ~~between identification documents and unauthorized readers. The~~
11 ~~mutual authentication standard shall at all times be at least as~~
12 ~~strong as any nonescrowed card authentication standard for~~
13 ~~algorithm and key parameters approved and specified by~~
14 ~~National Institute of Standards and Technology Special~~
15 ~~Publication 800-78 (NIST SP 800-78) for use after December 31,~~
16 ~~2010, or its successor if NIST SP 800-78 is amended or replaced.~~
17 ~~Proprietary encryption shall not be used. In the event that the~~
18 ~~card authentication standard used in an identification document is~~
19 ~~found to be no longer capable of protecting against the~~
20 ~~transmission of information between identification documents~~
21 ~~and unauthorized readers, a stronger card authentication standard~~
22 ~~that will ensure protection shall be implemented. Either a~~
23 ~~shared-secret or public-key cryptographic protocol may be used~~
24 ~~for mutual authentication.~~

25 ~~(B) The identification document shall also implement key~~
26 ~~establishment, so that if mutual authentication is successful, the~~
27 ~~identification document and the authorized reader shall derive a~~
28 ~~session key at least 16 bytes long for use with the~~
29 ~~secure-messaging encryption required under paragraph (3) of~~
30 ~~subdivision (a).~~

31 ~~(3) The identification document shall implement strong~~
32 ~~encryption to protect against the unauthorized reading of~~
33 ~~information transmitted between the identification document and~~
34 ~~reader after mutual authentication as described in paragraph (2)~~
35 ~~of subdivision (a) is concluded. This encryption shall not use~~
36 ~~proprietary encryption, and shall at all times be at least as strong~~
37 ~~as, or use, an approved nonescrowed encryption standard for~~
38 ~~algorithm and key parameters specified in Federal Information~~
39 ~~Processing Standards Publication 140-2 Annex A (FIPS Pub.~~
40 ~~140-2 Annex A) or its successor if FIPS Pub. 140-2 Annex A is~~

1 amended or replaced. In the event that the encryption standard
2 used in an identification document is found to be no longer
3 capable of protecting against the unauthorized reading of
4 transmitted information, a stronger encryption standard that will
5 ensure protection against the unauthorized reading of transmitted
6 information shall be implemented.

7 (4) In order to ensure that the holder of the identification
8 document affirmatively consents to each reading of the
9 identification document, each identification document shall
10 implement at least one of the following privacy safeguards:

11 (1) *In order to prevent duplication, forgery, or cloning of the*
12 *identification document, the identification document shall*
13 *incorporate tamper-resistant features.*

14 (2) *In order to determine to a reasonable certainty that the*
15 *identification document was legitimately issued by the issuing*
16 *entity, is not cloned, and is authorized to be read, the*
17 *identification document and authorized reader, in conjunction*
18 *with related, functionally integrated software, shall implement an*
19 *authentication process.*

20 (3) *If personally identifiable information is transmitted*
21 *remotely from the identification document, the identification*
22 *document and authorized reader, in conjunction with related,*
23 *functionally integrated software, shall not only meet the*
24 *requirements of paragraph (2) but also shall implement mutual*
25 *authentication in order to prevent the transmission of personally*
26 *identifiable information between identification documents and*
27 *unauthorized readers.*

28 (4) *If personally identifiable information is transmitted*
29 *remotely from the identification document, the identification*
30 *document shall make the data unreadable and unusable by an*
31 *unauthorized person through means such as encryption of the*
32 *data during transmission, access controls, data association,*
33 *encoding, obfuscation, or any other measures, or combination of*
34 *measures, that are effective to ensure the confidentiality of the*
35 *data transmitted between the identification document and*
36 *authorized reader.*

37 (5) *If personally identifiable information is transmitted*
38 *remotely from the identification document, the identification*
39 *document shall implement an access control protocol that*
40 *enables the holder to exercise direct control over any*

1 *transmission of the data using radio waves. This requirement*
2 *may be satisfied by the implementation of one or more means*
3 *including, but not limited to, the following:*

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

10 ~~(B) A shield device that, when used to protect the~~
11 ~~identification document, can prevent any communication of data~~
12 ~~using radio waves between the identification document and any~~
13 ~~reader under any circumstances.~~

14 ~~(C)~~

15 (B) A data-carrying device, such as an integrated circuit or
16 computer chip, that is normally not remotely readable, accessible,
17 or otherwise operational under any circumstances, and only
18 remotely readable, accessible, or operational while being
19 temporarily switched on or otherwise intentionally activated by a
20 person in physical possession of the identification document. The
21 device shall only be remotely readable while the person
22 intentionally ~~uses the switch intending that enables~~ the
23 identification document *to be read.*

24 (C) *Another access control protocol that enables the holder to*
25 *exercise direct control over any transmission of the data using*
26 *radio waves, not including a detachable shield device or bag.*

27 (6) *If a unique personal identifier number that is used to*
28 *provide an individual with access to more than one type of*
29 *application or service is transmitted remotely from the*
30 *identification document, the issuing entity of the identification*
31 *document shall do one or more of the following, commensurate*
32 *with the sensitivity of the applications:*

33 (A) *Implementing a secondary verification and identification*
34 *procedure that does not use radio waves, including, but not*
35 *limited to, the manual entry of a personal identification number*
36 *on a keypad or the placement of an authorized individual at*
37 *locations at which the identification document is to be read for a*
38 *purpose other than facilitating secured access to a secured*
39 *public building or parking area, in order to determine the*
40 *authenticity of the document or the identity of the person.*

1 (B) Implementing the security protections described in
2 paragraph (3).

3 (C) Implementing the security protections described in
4 paragraph (4).

5 (D) Implementing the security protections described in
6 paragraph (5).

7 (7) If the identification document remotely transmits a unique
8 personal identifier number for the purposes of recording the
9 attendance of a pupil at a public school, the issuing entity of the
10 identification document shall meet the requirements of
11 paragraph (6).

12 (8) If the identification document remotely transmits a unique
13 personal identifier number for the purposes of accessing public
14 transit services, is issued to a member of the public, as defined in
15 Section 6252 of the Government Code, and is either required by
16 the issuing public entity or confers a benefit that is unique to that
17 class of remotely readable identification document, the issuing
18 entity of the identification document shall meet the requirements
19 of paragraph (6).

20 (5)

21 (9) The issuing entity of ~~an~~ the identification document shall
22 communicate in writing to the person to whom the document is
23 issued at or before the time the document is issued, all of the
24 following:

25 (A) That the identification document can transmit ~~a unique~~
26 ~~personal identifier number data~~ or enable ~~that number data~~ to be
27 read remotely without his or her knowledge.

28 (B) That countermeasures, such as shield devices *or switches*,
29 may be used to help the person control the risk that his or her
30 ~~unique personal identifier number data~~ will be ~~broadcast or~~ read
31 remotely without his or her knowledge.

32 (C) ~~The location of all readers used or intended to be used by~~
33 ~~the issuing authority to read the unique personal identifier~~
34 ~~number on the identification document. Alternatively, the issuing~~
35 ~~authority may satisfy this reader-location notice requirement by~~
36 ~~doing both of the following:~~

37 (i) ~~Providing each document holder with a general description~~
38 ~~of the locations or types of locations where readers are used, such~~
39 ~~as all agency building entrances and exits.~~

1 ~~(ii) Posting or displaying a clear and conspicuous sign,~~
2 ~~placard, poster, or other similar written notice at each reader's~~
3 ~~actual location stating that the issuing authority has placed an~~
4 ~~identification document reader at that location, the reader is~~
5 ~~being used to read identification documents remotely using radio~~
6 ~~waves, and the commonly understood name of each document.~~

7 *(C) The location of readers used or intended to be used by the*
8 *issuing authority to read the data on the identification document.*
9 *This requirement shall be satisfied by doing one or more of the*
10 *following:*

11 *(i) Posting or displaying a clear and conspicuous sign,*
12 *placard, poster, or other similar written notice at each reader's*
13 *actual location indicating that the issuing authority has placed*
14 *an identification document reader at that location, that the*
15 *reader is being used to read identification documents remotely*
16 *using radio waves, and the commonly understood name of each*
17 *document.*

18 *(ii) Providing each document holder with a list of the location*
19 *of all readers used or intended to be used by the issuing authority*
20 *to read the data on the identification document.*

21 *(iii) Providing each document holder with a direct Internet*
22 *link to a Web page that clearly and conspicuously lists the*
23 *location of all readers used or intended to be used by the issuing*
24 *authority to read the data on the identification document. This*
25 *Web page shall be updated regularly.*

26 *(D) All circumstances under which the issuing authority plans*
27 *or intends to read the identification document and the reasons*
28 *behind those circumstances.*

29 ~~(E)~~

30 *(E) Any information, such as time and location, that is being*
31 *collected or stored regarding the individual in a database at the*
32 *time the identification document is being read.*

33 ~~(6) The issuing authority of any identification document shall~~
34 ~~provide annual notice to the person to whom the document is~~
35 ~~issued of any changes in the location of readers or the~~
36 ~~information collected or stored in the database if changes have~~
37 ~~occurred.~~

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

39 ~~(1) An identification document that is part of a contactless~~
40 ~~identification document system used by a state, county, or~~

1 ~~municipal government, or subdivision or agency thereof that is~~
2 ~~operational and in use prior to January 1, 2006, if all of the~~
3 ~~following apply:~~

4 ~~(A) The identification document is not used for any purpose~~
5 ~~other than the purpose or purposes of the system on the effective~~
6 ~~date of this article.~~

7 ~~(B) The identification document does not transmit using radio~~
8 ~~waves a greater amount, type, or types of information than the~~
9 ~~identification document in use on the effective date of this article.~~

10 ~~(C) The identification document is not issued to any group or~~
11 ~~category of people that was not issued the identification~~
12 ~~document on the effective date of this article.~~

13 *(1) Any contactless identification document system that began*
14 *implementation prior to January 1, 2007, or for which a state,*
15 *county, or municipal government request for proposal has been*
16 *publicly issued prior to September 30, 2006, or for which a*
17 *contract has been executed prior to September 30, 2006.*

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

25 (3) An identification document issued to a person employed
26 by a state prison, county jail, or juvenile facility operated by the
27 Division of Juvenile Facilities in the Department of Corrections
28 and Rehabilitation if the document is not removed from the
29 facility and the requirements of paragraph-~~(5)~~ (9) of subdivision
30 (a) apply.

31 (4) An identification document issued to a ~~firefighter or~~
32 ~~emergency medical technician if the document is used only while~~
33 ~~the firefighter or emergency medical technician law enforcement~~
34 ~~officer or emergency response personnel if the document is used~~
35 ~~only while the law enforcement officer or emergency response~~
36 ~~personnel is on active duty and the requirements of paragraph-~~(5)~~~~
37 ~~(9) of subdivision (a) apply.~~

38 (5) An identification document issued to a patient who is in
39 the care of a government-operated *or government-owned*

1 hospital, ambulatory surgery center, or oncology or dialysis
2 clinic if all of the following requirements are met:

3 (A) The identification document is valid for only a single
4 episode of care.

5 (B) The identification document may be removed and
6 reattached when used on a nonemergency outpatient.

7 (C) The identification document ~~complies with paragraph (1)~~
8 ~~of subdivision (a)~~ *does not transmit or enable the remote reading*
9 *using radio waves of personally identifiable information.*

10 (D) The patient returning for a new episode of care is assigned
11 a new unique *personal* identifier number.

12 (E) The patient *or the person who has been legally entrusted*
13 *to make medical decisions on behalf of the patient* is notified, in
14 writing, that the identification document transmits ~~personal~~
15 ~~information~~ *data* using radio waves.

16 (F) The patient is not compelled or encouraged to wear, or
17 keep on his or her person, the identification document beyond the
18 facility property.

19 (6) *An identification document issued to a person who is in the*
20 *care of a skilled nursing facility operated or owned by the*
21 *government, if all of the following requirements are met:*

22 (A) *The patient has been diagnosed by a doctor with dementia*
23 *or other cognitive impairment that involves substantial limitation*
24 *in function.*

25 (B) *The identification document does not transmit or enable*
26 *the remote reading using radio waves of personally identifiable*
27 *information.*

28 (C) *The patient or the person who has been legally entrusted*
29 *to make medical decisions on behalf of the patient* is notified, in
30 writing, that the identification document transmits *data* using
31 radio waves.

32 (D) *The patient is not compelled or encouraged to wear or*
33 *keep on his or her person the identification document beyond the*
34 *facility property.*

35 (E) *The patient or the person who has been legally entrusted*
36 *to make medical decisions on behalf of the patient* has consented
37 *to the issuance of the identification document.*

38 ~~(6)~~

39 (7) An identification document issued to a patient by
40 emergency medical services for triage or medical care during a

1 disaster and immediate hospitalization or immediate outpatient
2 care directly related to a disaster, as defined by the local
3 emergency medical services agency organized under Section
4 1797.200 of the Health and Safety Code.

5 ~~(7) An identification document issued to a person for the~~
6 ~~limited purpose of collecting funds for the use of a toll bridge,~~
7 ~~such as the FasTrak system, if the requirements of paragraphs (1)~~
8 ~~and (5) of subdivision (a) are met.~~

9 (8) An identification document that is issued to a person for
10 the limited purpose of facilitating secured access by the
11 identification document holder to a secured public building or
12 parking area, if the requirements of ~~paragraphs (1) and (5)~~
13 *paragraph (9)* of subdivision (a) are met *and the identification*
14 *document does not transmit or enable the remote reading using*
15 *radio waves of personally identifiable information.*

16 (9) A license, certificate, registration, or other authority for
17 engaging in a business or profession regulated under the Business
18 and Professions Code, if the requirements of ~~paragraphs (1), (4),~~
19 ~~and (5) paragraph (9)~~ of subdivision (a) are met *and the*
20 *identification document does not transmit or enable the remote*
21 *reading using radio waves of personally identifiable information.*

22 ~~(10) An identification document for which the Legislature~~
23 ~~determines that the standards of subdivision (a) of Section~~
24 ~~1798.10 do not apply because of the existence of a compelling~~
25 ~~state interest and that there is no means less intrusive to the~~
26 ~~individual's privacy and security to achieve the compelling state~~
27 ~~interest.~~

28 (e) ~~(1) Except for identification documents listed in~~
29 ~~subdivision (b), the following identification documents created,~~
30 ~~mandated, purchased, or issued by a state, county, or municipal~~
31 ~~government, or subdivision or agency thereof, shall not use radio~~
32 ~~waves to transmit personal information or to enable personal~~
33 ~~information to be read remotely:~~

34 ~~(A) Drivers' licenses or identification cards issued pursuant to~~
35 ~~Section 13000 of the Vehicle Code.~~

36 ~~(B) Identification cards issued to students in K-12 schools.~~

37 ~~(C) Health insurance, health benefit, and benefit cards issued~~
38 ~~in conjunction with any government-supported aid program.~~

39 ~~(D) Library cards issued by any public library.~~

1 ~~(2) This subdivision shall become inoperative on January 1,~~
2 ~~2009, unless a later enacted statute deletes or extends that date.~~

3 1798.11. Except as provided in subdivision (d), a state,
4 county, or municipal government, or subdivision or agency
5 thereof, that creates, mandates, purchases, or issues an
6 identification document in compliance with subdivision (a) of
7 Section 1798.10 ~~or a third party with whom the governmental~~
8 ~~agency has a bona fide business relationship:~~

9 (a) ~~Shall not, under any circumstances, disclose the keys~~
10 ~~required by paragraph (2) any operational system keys used~~
11 ~~pursuant to paragraphs (3) and (4) of subdivision (a) of Section~~
12 ~~1798.10, either publicly or to any nongovernmental entity or~~
13 ~~other third party, including, but not limited to, contractors,~~
14 ~~officers, and employees of other government agencies, that is not~~
15 ~~authorized under subdivision (d).~~

16 (b) ~~Shall take all reasonable measures to keep the keys~~
17 ~~required by paragraph (2) any operational system keys used~~
18 ~~pursuant to paragraphs (3) and (4) of subdivision (a) of Section~~
19 ~~1798.10 secure and unavailable to any third party that is not~~
20 ~~authorized under subdivision (d).~~

21 (c) ~~Shall not, under any circumstances, act in any way to allow~~
22 ~~a third party that is not authorized under subdivision (d) to read~~
23 ~~the personal information broadcast or data transmitted remotely~~
24 ~~by the identification document using radio waves.~~

25 ~~(d) A state, county, or municipal government, or a political~~
26 ~~subdivision or agency thereof, and a single third party with~~
27 ~~whom the governmental agency has entered into a contract,~~
28 ~~either for operation, monitoring, or technical assistance, may~~
29 ~~disclose the keys to each other and allow each other to read the~~
30 ~~personal information broadcast or transmitted remotely by the~~
31 ~~identification document using radio waves. A single third party~~
32 ~~with whom the governmental entity has entered into a contract~~
33 ~~shall agree to the following conditions:~~

34 ~~(1) The third party shall adopt procedures restricting access to~~
35 ~~the keys, and these procedures shall be designed to secure the~~
36 ~~keys from tampering and unauthorized access. These procedures~~
37 ~~shall include administrative, technical, and physical safeguards to~~
38 ~~protect against any reasonably anticipated threats or hazards to~~
39 ~~the privacy of the information, and unauthorized uses or~~
40 ~~disclosures of the information.~~

1 ~~(2) The third party shall not transmit the keys to any other~~
2 ~~person or entity.~~

3 ~~(3) Any person or entity who receives a disclosure pursuant to~~
4 ~~this exception is subject to the prohibition of subdivision (a). All~~
5 ~~information received pursuant to this exception shall be~~
6 ~~destroyed when the purpose of the disclosure is completed.~~

7 ~~(4) Any person may bring a civil action against a~~
8 ~~governmental entity whenever the governmental entity, third~~
9 ~~party entity with whom the governmental entity has entered into~~
10 ~~a contract, or third party with whom the governmental entity has~~
11 ~~a bona fide business relationship fails to comply with the~~
12 ~~provisions of this section, or any rule promulgated thereunder, in~~
13 ~~such a way as to have an adverse effect on a person. For purposes~~
14 ~~of this paragraph, “adverse effect” includes, but is not limited to,~~
15 ~~any time a third party that enters into a bona fide business~~
16 ~~relationship pursuant to this subdivision, subsequently discloses~~
17 ~~that information to another person, regardless of whether~~
18 ~~economic harm occurred.~~

19 *(d) A state, county, or municipal government, or subdivision*
20 *or agency thereof, that creates, mandates, purchases, or issues*
21 *an identification document in compliance with subdivision (a) of*
22 *Section 1798.10 may disclose any operational system keys used*
23 *pursuant to paragraphs (3) and (4) of subdivision (a) of Section*
24 *1798.10 to authorized third parties that in the stream of*
25 *commerce have a bona fide business relationship with the*
26 *agency, or its contractors or subcontractors, and that are*
27 *necessary to the operation, testing, or installation of the*
28 *identification system, and to emergency response personnel for*
29 *the sole purposes of locating and identifying a person or persons*
30 *in the case of a disaster, as defined by the local Emergency*
31 *Medical Services agency organized under Section 1797.200 of*
32 *the Health and Safety Code.*

33 *(1) Any authorized third party that receives a disclosure*
34 *pursuant to this exception is subject to the prohibitions of*
35 *subdivisions (a) to (c), inclusive.*

36 *(2) Any authorized third party that receives a disclosure*
37 *pursuant to this exception shall adopt procedures restricting*
38 *access to the operational system keys and securing the keys from*
39 *tampering and unauthorized access. These procedures shall*
40 *include administrative, technical, and physical safeguards to*

1 *protect against any reasonably anticipated threats or hazards to*
2 *the privacy of the information, and unauthorized uses or*
3 *disclosures of the information.*

4 *(3) All information received pursuant to this exception shall be*
5 *destroyed when the purpose of the disclosure is completed.*

6 *1798.115. A person or entity that knowingly discloses, or*
7 *causes to be disclosed, the operational system keys described in*
8 *Section 1798.11 in violation of Section 1798.11 shall be punished*
9 *by imprisonment in a county jail for up to one year, a fine of not*
10 *more than five thousand dollars (\$5,000), or both that fine and*
11 *imprisonment.*

12 *1798.12. A state, county, or municipal government, or a*
13 *political subdivision or agency thereof, that uses radio waves to*
14 ~~*broadcast personal information or to enable personal information*~~
15 ~~*transmit data or to enable data*~~ *to be read remotely pursuant to*
16 *subdivision (a) of Section 1798.10 or the single third party entity*
17 ~~*authorized third parties*~~ *with whom the governmental entity has*
18 ~~*entered into a contract or third party with whom the*~~
19 ~~*governmental entity has*~~ *a bona fide business relationship shall*
20 *not disclose any personal information, data or information*
21 *regarding the location of a person derived from the use of the*
22 *radio waves, or the keys required by paragraph (2) of subdivision*
23 ~~*(a) of Section 1798.10, unless the disclosure is required pursuant*~~
24 ~~*to a search warrant.*~~ *comports with any of the following:*

25 *(a) The disclosure is made pursuant to an exigent*
26 *circumstance and all of the following occurs:*

27 *(1) The information that is requested is necessary to locate*
28 *and respond to a person who is in immediate danger of death or*
29 *serious bodily injury or a minor who is in immediate danger.*

30 *(2) The information that is disclosed solely regards the*
31 *location of a person or an identification document and the time*
32 *at which that person was or is at that location.*

33 *(3) The request by emergency response personnel to a*
34 *governmental entity to which this section applies includes, at a*
35 *minimum, all of the following information:*

36 *(A) The name and title of the emergency response personnel.*

37 *(B) The office location and telephone number for the*
38 *emergency response personnel.*

1 (C) *The name and telephone number of the emergency*
2 *response personnel's supervisor or the person who has the*
3 *ultimate operational responsibility at the time.*

4 (D) *The assertion by the emergency response personnel that*
5 *an exigent circumstance exists.*

6 (4) *The governmental entity provides the emergency response*
7 *personnel with the requested location information upon*
8 *verification of the information required by paragraph (3) with*
9 *the emergency response personnel's supervisor or the person*
10 *who has ultimate operational responsibility at the time. No*
11 *governmental entity, or official or employee thereof, shall be*
12 *subject to liability when it acts in a reasonable manner upon*
13 *receiving the information required by paragraph (3).*

14 (5) *The governmental entity maintains for a period of not less*
15 *than one year all requests from public safety or emergency*
16 *response agencies for location information that are made under*
17 *exigent circumstances.*

18 (6) *Individuals whose location information has been released*
19 *pursuant to this subdivision are notified in writing by the*
20 *governmental entity within a reasonable period of time that their*
21 *information has been released and the notice shall include the*
22 *information required in paragraph (3). The notification required*
23 *by this paragraph may be delayed if a law enforcement agency*
24 *determines that the notification will impede a criminal*
25 *investigation. The notification required by this paragraph shall*
26 *be made after the law enforcement agency determines that it will*
27 *not compromise the investigation.*

28 (7) *The location information obtained as the result of a*
29 *request pursuant to this section is used solely for the purpose of*
30 *rendering emergency aid by emergency response personnel to*
31 *the person during the exigent circumstances forming the basis of*
32 *the request.*

33 (b) *The disclosure is made pursuant to a request by law*
34 *enforcement personnel in the course of a legitimate investigation*
35 *and the information is derived only from the use of employee*
36 *identification documents to facilitate secured access to public*
37 *buildings or parking areas.*

38 (c) *The disclosure is required pursuant to a search warrant.*

39 1798.125. *Any interested person may institute proceedings*
40 *against a governmental entity for injunctive or declaratory relief*

1 *or a writ of mandate in any court of competent jurisdiction for*
2 *the purpose of preventing or stopping any violation of this*
3 *article, if all of the following occurs:*

4 *(a) The person provides to the governmental entity, written*
5 *notice of the alleged violation by certified mail.*

6 *(b) The governmental entity fails, for at least 30 days after*
7 *receipt of that written notice, to fix the alleged violation, to*
8 *comply with the provisions of the article, and to inform the*
9 *demanding party in writing of its actions to fix the alleged*
10 *violation or its decision not to correct the alleged violation.*

11 *1798.126. (a) In any proceedings brought pursuant to*
12 *Section 1798.125, the court may assess against the governmental*
13 *entity reasonable attorney's fees and other litigation costs*
14 *reasonably incurred in any proceedings under this article in*
15 *which the complainant has prevailed.*

16 *(b) Nothing in this section affects or is intended to limit or*
17 *supplant any other remedies that may be available in law or*
18 *equity.*

19 *1798.13. ~~A~~(a) Except as provided in subdivisions (b) and*
20 *(c), a person or entity that intentionally remotely reads or*
21 *attempts to remotely read a person's identification document*
22 *issued pursuant to Section 1798.10 using radio waves, for the*
23 *purpose of reading that person's identification document without*
24 *the knowledge of that person that person's knowledge and prior*
25 *consent, shall be punished by imprisonment in a county jail for*
26 *up to one year, a fine of not more than five thousand dollars*
27 *(\$5,000), or both that fine and imprisonment.*

28 *(b) Subdivision (a) shall not apply to:*

29 *(1) The reading of a person's identification document for*
30 *triage or medical care during a disaster and immediate*
31 *hospitalization or immediate outpatient care directly related to a*
32 *disaster, as defined by the local Emergency Medical Services*
33 *agency organized under Section 1797.200 of the Health and*
34 *Safety Code.*

35 *(2) The reading of a person's identification document by a*
36 *health care professional for reasons relating to the health or*
37 *safety of that person or an identification document issued to a*
38 *patient by emergency services.*

39 *(3) The reading of an identification document of a person who*
40 *is incarcerated in the state prison or a county jail, detained in a*

1 juvenile facility operated by the Division of Juvenile Facilities in
2 the Department of Corrections and Rehabilitation, or housing in
3 a mental health facility, pursuant to a court order after having
4 been charged with a crime, or to a person pursuant to a
5 court-ordered electronic monitoring.

6 (4) Law enforcement or government personnel who need to
7 read a lost identification document when the owner is
8 unavailable for notice, knowledge, or consent, or those parties
9 specifically authorized by law enforcement or government
10 personnel for the limited purpose of reading a lost identification
11 document when the owner is unavailable for notice, knowledge,
12 or consent.

13 (5) Law enforcement personnel who need to read a person's
14 identification document after an accident in which the person is
15 unavailable for notice, knowledge, or consent.

16 (6) Law enforcement personnel who need to read a person's
17 identification document pursuant to a search warrant.

18 (7) A person or entity that in the course of operating its own
19 contactless identification document system inadvertently reads or
20 collects data from another contactless identification document
21 system, provided that the inadvertently received data comports
22 with all of the following:

23 (A) The data is not disclosed to any other party.

24 (B) The data is not used for any purpose.

25 (C) The data is not stored or is promptly destroyed.

26 (c) Nothing in this section shall affect the existing rights of law
27 enforcement to access data stored electronically on drivers'
28 licenses.

29 (d) The penalties set forth in paragraph (a) are independent
30 of, and do not supersede, any other penalties provided by state
31 law, and in the case of any conflict, the greater penalties shall
32 apply.

33 1798.135. For purposes of this article, the following
34 definitions shall apply:

35 (a) "Access controls" means granting or denying permission
36 to access information.

37 (b) "Authentication" means the process of applying a
38 machine-readable process to data or identification documents, or
39 both, so as to accomplish either of the following:

1 (1) Establish that the data and the identification document
2 containing the data were issued by the responsible issuing state
3 or local governmental body.

4 (2) Ensure that a reader, as defined in subdivision (p), is
5 permitted under California law to access that data or
6 identification document.

7 (c) “Authorized reader” means a reader, as defined in
8 subdivision (p), that, with respect to a particular identification
9 document, (1) is permitted under California law to remotely read
10 the data transmitted by that identification document, (2) is being
11 used for a lawful purpose, and (3) is fully in accord with the
12 requirements of subdivision (a) of Section 1798.10.

13 (d) “Contactless identification document system” means a
14 group of identification documents issued and operated under a
15 single authority that use radio waves to transmit data remotely to
16 readers intended to read that data. In a contactless identification
17 document system, every reader must be able to read every
18 identification document in the system.

19 (e) “Data” means information stored on an identification
20 document in machine-readable form including, but not limited to,
21 personally identifiable information and other unique personal
22 identifier numbers.

23 (f) “Data association” means storing information in separate
24 locations so that the information is not resident in a single
25 location and is not usable if only one of such locations is
26 accessed.

27 (g) “Emergency response personnel” means any of the
28 following:

29 (1) “Emergency medical technician,” as defined in Sections
30 1797.80 and 1797.82 of the Health and Safety Code.

31 (2) “Firefighter,” as defined in Section 1797.182 of the Health
32 and Safety Code.

33 (3) “Mobile intensive care nurse,” as defined in Section
34 1797.56 of the Health and Safety Code.

35 (4) “Paramedic,” as defined in Section 1797.84 of the Health
36 and Safety Code.

37 (5) “Peace officer,” as defined in Sections 830.1 and 830.2 of
38 the Penal Code.

39 (h) “Encoding” means use of a mechanism that allows the
40 message elements to be substituted for other elements.

1 (i) “Encryption” means the protection of data in electronic
2 form in storage or while being transmitted using an encryption
3 algorithm implemented within a cryptographic module that has
4 been adopted or approved by the National Institute of Standards
5 and Technology, the Institute of Electrical and Electronics
6 Engineers, Inc., the Internet Engineering Task Force, the
7 International Organization for Standardization, the Organization
8 for the Advancement of Structured Information Standards, or any
9 other similar standards setting body, rendering that data
10 indecipherable in the absence of associated cryptographic keys
11 necessary to enable decryption of that data. That encryption
12 shall include appropriate management and safeguards of those
13 keys to protect the integrity of the encryption.

14 (j) “Exigent circumstance” means a reasonable belief by
15 emergency response personnel that either of the following
16 situations exists:

17 (1) There is immediate danger of death or serious bodily
18 injury to the person whose location information is being sought
19 or to another individual who could be located through the
20 reading of that identification document.

21 (2) There is immediate danger to a minor whose location
22 information is being sought or to another minor who could be
23 located through the reading of that identification document.

24 (k) (1) “Identification document” means any document
25 containing data that is issued to an individual and which that
26 individual, and only that individual, uses alone or in conjunction
27 with any other information for the primary purpose of
28 establishing his or her identity. Identification documents
29 specifically include, but are not limited to, the following:

30 (A) Driver’s licenses or identification cards issued pursuant to
31 Section 13000 of the Vehicle Code.

32 (B) Identification cards for employees or contractors.

33 (C) Identification cards issued by educational institutions.

34 (D) Health insurance or benefit cards.

35 (E) Benefit cards issued in conjunction with any
36 government-supported aid program.

37 (F) Licenses, certificates, registration, or other means to
38 engage in a business or profession regulated by the Business and
39 Professions Code.

40 (G) Library cards issued by any public library.

1 (2) *Identification documents do not include devices issued to*
2 *persons for the limited purpose of collecting funds for the use of*
3 *a toll bridge or toll road, such as devices used by the FasTrak*
4 *system, if the device is not issued for the exclusive use of an*
5 *individual and does not transmit or enable the remote reading*
6 *using radio waves of personally identifiable information.*

7 (l) *“Key” means a string of bits of information used as part of*
8 *a cryptographic algorithm used in encryption.*

9 (m) *“Mutual authentication” means a process by which*
10 *identification documents and authorized readers securely*
11 *challenge each other to verify authenticity and authorization of*
12 *both readers and documents before any data is exchanged,*
13 *except such data as is necessary to carry out mutual*
14 *authentication. Mutual authentication accomplishes both of the*
15 *following:*

16 (1) *Authorized readers, as defined in subdivision (c), can*
17 *accurately assess whether the identification document and data*
18 *stored are issued by the responsible issuing state or local*
19 *governmental body to an authorized holder.*

20 (2) *Authorized identification documents can accurately assess*
21 *whether a reader accessing them is authorized to read the*
22 *documents, and authorized to then access data stored on the*
23 *documents.*

24 (n) *“Obfuscation of information” means the transformation of*
25 *information without the use of an encryption algorithm or key*
26 *into a form in which the information is rendered unusable or*
27 *unreadable.*

28 (o) *“Personally identifiable information” includes any of the*
29 *following data elements to the extent that they are used alone or*
30 *in conjunction with any other information to identify an*
31 *individual:*

32 (1) *First or last name.*

33 (2) *Address.*

34 (3) *Telephone number.*

35 (4) *E-mail address.*

36 (5) *Date of birth.*

37 (6) *Driver’s license number or California identification card*
38 *number.*

1 (7) Any unique personal identifier number contained or
2 encoded on a driver's license or identification card issued
3 pursuant to Section 13000 of the Vehicle Code.

4 (8) Bank, credit card, or other financial institution account
5 number.

6 (9) Credit or debit card number.

7 (10) Any unique personal identifier number contained or
8 encoded on a health insurance, health benefit, or benefit card
9 issued in conjunction with any government-supported aid
10 program.

11 (11) Religion.

12 (12) Ethnicity or nationality.

13 (13) Photograph.

14 (14) Fingerprint or other biometric identification.

15 (15) Social security number.

16 (p) "Reader" means a scanning device that is capable of using
17 radio waves to communicate with an identification document and
18 read the data transmitted by that identification document.

19 (q) "Remotely" means that no physical contact between the
20 identification document and a reader is necessary in order to
21 transmit data using radio waves.

22 (r) "Shield devices" mean physical or technological
23 protections available to stop the transmission of data
24 programmed on or into an identification document using radio
25 waves.

26 (s) "Single episode of care" means an inpatient hospital stay
27 through discharge or specific course of therapy or treatment for
28 outpatient care.

29 (t) "Unique personal identifier number" means a randomly
30 assigned string of numbers or symbols that is encoded onto the
31 identification document and is intended to identify the
32 identification document that has been issued to a particular
33 individual.

34 1798.136. The provisions of this article shall become
35 inoperative on December 31, 2012, or when alternative statewide
36 regulations pertaining to the privacy and security of remotely
37 readable identification documents are enacted or promulgated
38 pursuant to later legislation, whichever is earlier.

1 *SEC. 4. Article 13 (commencing with Section 11147) is added*
2 *to Chapter 1 of Part 1 of Division 3 of Title 2 of the Government*
3 *Code, to read:*

4
5 *Article 13. Report on Security and Privacy for*
6 *Government-Issued Identification Documents*
7

8 *11147. The California Research Bureau in the California*
9 *State Library, within 270 days of receiving a request from the*
10 *Office of the President pro Tempore of the Senate or the Office of*
11 *the Speaker of the Assembly, or before June 30, 2007, whichever*
12 *is earlier, shall submit to the Legislature a report on security and*
13 *privacy for government-issued, remotely readable identification*
14 *documents.*

15 *11147.1. In preparing the report required by Section 11147,*
16 *the bureau shall, at a minimum, do all of the following:*

17 *(a) Establish an advisory board that makes recommendations,*
18 *provides technical advice, answers bureau questions, and*
19 *outlines the strengths and weaknesses of potential approaches to*
20 *privacy and security proposals for government-issued, remotely*
21 *readable identification documents. The advisory board shall be*
22 *composed of all of the following members:*

23 *(1) The State Chief Information Officer or his or her designee.*

24 *(2) The chief of the Office of Privacy Protection or his or her*
25 *designee.*

26 *(3) The Attorney General or his or her designee.*

27 *(4) A representative from the Office of Emergency Services.*

28 *(5) A representative from either the University of California or*
29 *the California State University system.*

30 *(6) A representative from the Department of Motor Vehicles.*

31 *(7) A representative from the California State Information*
32 *Security Office.*

33 *(8) A representative selected by the bureau from the*
34 *California School Boards Association.*

35 *(9) A representative selected by the bureau from city or county*
36 *government.*

37 *(10) One representative selected by the bureau, from each of*
38 *the following industries:*

39 *(A) Remotely readable identification card manufacturers.*

40 *(B) Remotely readable identification chip manufacturers.*

1 (C) Remotely readable identification reader manufacturers.

2 (D) Remotely readable component manufacturers.

3 (E) Enterprise or network information technology companies.

4 (11) Five representatives selected by the bureau from among
5 privacy rights groups, including, but not limited to, the American
6 Civil Liberties Union, the Electronic Frontier Foundation, and
7 the Privacy Rights Clearing House.

8 (12) Other representatives selected by the bureau that would
9 be necessary for the bureau to complete the report required by
10 Section 11147.

11 (b) Review and document existing state and federal laws
12 relating to privacy, security, and safeguards for remotely
13 readable identification documents.

14 (c) Review privacy and security safeguards and technologies
15 that are currently available or in development for remotely
16 readable identification documents.

17 (d) Review best practices that have been established or that
18 are under consideration to prevent identity theft, privacy
19 invasion, and criminal use of personal and other data to
20 determine their applicability to government-issued identification
21 documents.

22 (e) Consider requirements for a privacy impact assessment
23 and a security risk assessment conducted by issuing entities that
24 would clearly define what personal information is to be
25 collected, how the information will and could be used, who may
26 and who could access the information, how the information will
27 be protected from unauthorized access, and how an individual
28 may control use of and update his or her information.

29 (f) Identify, develop, and evaluate options for the Legislature
30 to review and consider for action for a legislative and regulatory
31 framework that would ensure the safety and security of
32 information contained on remotely readable identification
33 documents and the privacy of the individuals to whom the
34 documents are issued.

35 11147.2. The bureau shall be solely responsible for preparing
36 the report required by this article. The report shall include
37 information, suggestions, and comments from the advisory
38 board. In making recommendations, the bureau shall maintain
39 an approach that, when appropriate, is neutral with respect to
40 specific technologies and methods, shall consider the multitude

1 *of ways of ensuring privacy and security, and shall consider the*
2 *impact of any recommendations on innovation. The report may*
3 *include additional research and commentary that the bureau*
4 *believes is necessary to prepare a complete and thorough report.*

5 *11147.3. The provisions of this article shall become*
6 *inoperative on December 31, 2012, or when alternative statewide*
7 *regulations pertaining to the privacy and security of remotely*
8 *readable identification documents are enacted or promulgated*
9 *pursuant to later legislation, whichever is earlier.*

10 ~~SEC. 4.~~

11 *SEC. 5.* No reimbursement is required by this act pursuant to
12 Section 6 of Article XIII B of the California Constitution because
13 the only costs that may be incurred by a local agency or school
14 district will be incurred because this act creates a new crime or
15 infraction, eliminates a crime or infraction, or changes the
16 penalty for a crime or infraction, within the meaning of Section
17 17556 of the Government Code, or changes the definition of a
18 crime within the meaning of Section 6 of Article XIII B of the
19 California Constitution.