

AMENDED IN SENATE MAY 29, 2014
AMENDED IN SENATE MAY 27, 2014
AMENDED IN SENATE MAY 6, 2014
AMENDED IN SENATE APRIL 29, 2014
AMENDED IN SENATE APRIL 9, 2014

SENATE BILL

No. 893

Introduced by Senator Hill

January 13, 2014

An act to amend Sections 1798.29 and 1798.82 of, and to add Title 1.81.23 (commencing with Section 1798.90.5) to Part 4 of Division 3 of, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 893, as amended, Hill. Automated license plate recognition systems: use of data.

(1) Existing law authorizes the Department of the California Highway Patrol to retain license plate data captured by license plate recognition (LPR) technology, also referred to as an automated license plate recognition (ALPR) system, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. Existing law prohibits the department from selling the data or from making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer.

Existing law authorizes the department to use LPR data for the purpose of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense, and requires the department to monitor the internal use of the data to prevent unauthorized use and to

submit to the Legislature, as a part of the annual automobile theft report, information on the department's LPR practices and usage.

This bill would impose specified requirements on an "ALPR operator," as defined, including, among others, complying with all applicable statutory and constitutional requirements and the provisions of the bill, ensuring that the information or data the ALPR operator collects is protected with certain safeguards, and ~~to implement and maintain~~ *implementing and maintaining* specified security procedures and a usage and privacy policy with respect to that information or data.

This bill would also prohibit an ALPR operator from ~~engaging in certain acts, including, among others, retaining any information or data other than the license plate number, the date and time the information or data is collected, and the location coordinates where the information or data is collected.~~ *collecting license plate data when a license plate number is not in public view.* The bill would require an ALPR operator that accesses or provides access to information or data collected through the use or operation of an ALPR system to maintain a specified record of that access.

The bill would, in addition to any other sanctions, penalties, or remedies provided by law, authorize an individual who has been harmed by a violation of these provisions to bring a civil action in any court of competent jurisdiction against a person who knowingly caused that violation.

(2) Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines "personal information" for these purposes to include an individual's first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver's license numbers, financial accounts, and medical information.

This bill would include information or data collected through the use or operation of an automated license plate recognition system, when that information or data is not encrypted *and is used in combination with an individual's name*, in the definition of "personal information" discussed above.

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

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

1 SECTION 1. Section 1798.29 of the Civil Code is amended
2 to read:

3 1798.29. (a) Any agency that owns or licenses computerized
4 data that includes personal information shall disclose any breach
5 of the security of the system following discovery or notification
6 of the breach in the security of the data to any resident of California
7 whose unencrypted personal information was, or is reasonably
8 believed to have been, acquired by an unauthorized person. The
9 disclosure shall be made in the most expedient time possible and
10 without unreasonable delay, consistent with the legitimate needs
11 of law enforcement, as provided in subdivision (c), or any measures
12 necessary to determine the scope of the breach and restore the
13 reasonable integrity of the data system.

14 (b) Any agency that maintains computerized data that includes
15 personal information that the agency does not own shall notify the
16 owner or licensee of the information of any breach of the security
17 of the data immediately following discovery, if the personal
18 information was, or is reasonably believed to have been, acquired
19 by an unauthorized person.

20 (c) The notification required by this section may be delayed if
21 a law enforcement agency determines that the notification will
22 impede a criminal investigation. The notification required by this
23 section shall be made after the law enforcement agency determines
24 that it will not compromise the investigation.

25 (d) Any agency that is required to issue a security breach
26 notification pursuant to this section shall meet all of the following
27 requirements:

28 (1) The security breach notification shall be written in plain
29 language.

30 (2) The security breach notification shall include, at a minimum,
31 the following information:

32 (A) The name and contact information of the reporting agency
33 subject to this section.

34 (B) A list of the types of personal information that were or are
35 reasonably believed to have been the subject of a breach.

1 (C) If the information is possible to determine at the time the
2 notice is provided, then any of the following: (i) the date of the
3 breach, (ii) the estimated date of the breach, or (iii) the date range
4 within which the breach occurred. The notification shall also
5 include the date of the notice.

6 (D) Whether the notification was delayed as a result of a law
7 enforcement investigation, if that information is possible to
8 determine at the time the notice is provided.

9 (E) A general description of the breach incident, if that
10 information is possible to determine at the time the notice is
11 provided.

12 (F) The toll-free telephone numbers and addresses of the major
13 credit reporting agencies, if the breach exposed a social security
14 number or a driver's license or California identification card
15 number.

16 (3) At the discretion of the agency, the security breach
17 notification may also include any of the following:

18 (A) Information about what the agency has done to protect
19 individuals whose information has been breached.

20 (B) Advice on steps that the person whose information has been
21 breached may take to protect himself or herself.

22 (4) In the case of a breach of the security of the system involving
23 personal information defined in paragraph (2) of subdivision (g)
24 for an online account, and no other personal information defined
25 in paragraph (1) of subdivision (g), the agency may comply with
26 this section by providing the security breach notification in
27 electronic or other form that directs the person whose personal
28 information has been breached to promptly change his or her
29 password and security question or answer, as applicable, or to take
30 other steps appropriate to protect the online account with the
31 agency and all other online accounts for which the person uses the
32 same user name or email address and password or security question
33 or answer.

34 (5) In the case of a breach of the security of the system involving
35 personal information defined in paragraph (2) of subdivision (g)
36 for login credentials of an email account furnished by the agency,
37 the agency shall not comply with this section by providing the
38 security breach notification to that email address, but may, instead,
39 comply with this section by providing notice by another method
40 described in subdivision (i) or by clear and conspicuous notice

1 delivered to the resident online when the resident is connected to
2 the online account from an Internet Protocol address or online
3 location from which the agency knows the resident customarily
4 accesses the account.

5 (e) Any agency that is required to issue a security breach
6 notification pursuant to this section to more than 500 California
7 residents as a result of a single breach of the security system shall
8 electronically submit a single sample copy of that security breach
9 notification, excluding any personally identifiable information, to
10 the Attorney General. A single sample copy of a security breach
11 notification shall not be deemed to be within subdivision (f) of
12 Section 6254 of the Government Code.

13 (f) For purposes of this section, “breach of the security of the
14 system” means unauthorized acquisition of computerized data that
15 compromises the security, confidentiality, or integrity of personal
16 information maintained by the agency. Good faith acquisition of
17 personal information by an employee or agent of the agency for
18 the purposes of the agency is not a breach of the security of the
19 system, provided that the personal information is not used or
20 subject to further unauthorized disclosure.

21 (g) For purposes of this section, “personal information” means
22 ~~any~~ *either* of the following:

23 (1) An individual’s first name or first initial and last name in
24 combination with any one or more of the following data elements,
25 when either the name or the data elements are not encrypted:

26 (A) Social security number.

27 (B) Driver’s license number or California identification card
28 number.

29 (C) Account number, credit or debit card number, in
30 combination with any required security code, access code, or
31 password that would permit access to an individual’s financial
32 account.

33 (D) Medical information.

34 (E) Health insurance information.

35 (F) *Information or data collected through the use or operation*
36 *of an automated license plate recognition system, as defined in*
37 *Section 1798.90.5.*

38 (2) A user name or email address, in combination with a
39 password or security question and answer that would permit access
40 to an online account.

1 ~~(3) Information or data collected through the use or operation~~
2 ~~of an automated license plate recognition system, as defined in~~
3 ~~Section 1798.90.5, when that information or data is not encrypted.~~

4 (h) (1) For purposes of this section, “personal information”
5 does not include publicly available information that is lawfully
6 made available to the general public from federal, state, or local
7 government records.

8 (2) For purposes of this section, “medical information” means
9 any information regarding an individual’s medical history, mental
10 or physical condition, or medical treatment or diagnosis by a health
11 care professional.

12 (3) For purposes of this section, “health insurance information”
13 means an individual’s health insurance policy number or subscriber
14 identification number, any unique identifier used by a health insurer
15 to identify the individual, or any information in an individual’s
16 application and claims history, including any appeals records.

17 (i) For purposes of this section, “notice” may be provided by
18 one of the following methods:

19 (1) Written notice.

20 (2) Electronic notice, if the notice provided is consistent with
21 the provisions regarding electronic records and signatures set forth
22 in Section 7001 of Title 15 of the United States Code.

23 (3) Substitute notice, if the agency demonstrates that the cost
24 of providing notice would exceed two hundred fifty thousand
25 dollars (\$250,000), or that the affected class of subject persons to
26 be notified exceeds 500,000 persons, or the agency does not have
27 sufficient contact information. Substitute notice shall consist of
28 all of the following:

29 (A) Email notice when the agency has an email address for the
30 subject persons.

31 (B) Conspicuous posting of the notice on the agency’s Internet
32 Web site page, if the agency maintains one.

33 (C) Notification to major statewide media and the Office of
34 Information Security within the Department of Technology.

35 (j) Notwithstanding subdivision (i), an agency that maintains
36 its own notification procedures as part of an information security
37 policy for the treatment of personal information and is otherwise
38 consistent with the timing requirements of this part shall be deemed
39 to be in compliance with the notification requirements of this

1 section if it notifies subject persons in accordance with its policies
2 in the event of a breach of security of the system.

3 (k) Notwithstanding the exception specified in paragraph (4) of
4 subdivision (b) of Section 1798.3, for purposes of this section,
5 “agency” includes a local agency, as defined in subdivision (a) of
6 Section 6252 of the Government Code.

7 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

8 1798.82. (a) Any person or business that conducts business
9 in California, and that owns or licenses computerized data that
10 includes personal information, shall disclose any breach of the
11 security of the system following discovery or notification of the
12 breach in the security of the data to any resident of California
13 whose unencrypted personal information was, or is reasonably
14 believed to have been, acquired by an unauthorized person. The
15 disclosure shall be made in the most expedient time possible and
16 without unreasonable delay, consistent with the legitimate needs
17 of law enforcement, as provided in subdivision (c), or any measures
18 necessary to determine the scope of the breach and restore the
19 reasonable integrity of the data system.

20 (b) Any person or business that maintains computerized data
21 that includes personal information that the person or business does
22 not own shall notify the owner or licensee of the information of
23 any breach of the security of the data immediately following
24 discovery, if the personal information was, or is reasonably
25 believed to have been, acquired by an unauthorized person.

26 (c) The notification required by this section may be delayed if
27 a law enforcement agency determines that the notification will
28 impede a criminal investigation. The notification required by this
29 section shall be made after the law enforcement agency determines
30 that it will not compromise the investigation.

31 (d) Any person or business that is required to issue a security
32 breach notification pursuant to this section shall meet all of the
33 following requirements:

34 (1) The security breach notification shall be written in plain
35 language.

36 (2) The security breach notification shall include, at a minimum,
37 the following information:

38 (A) The name and contact information of the reporting person
39 or business subject to this section.

1 (B) A list of the types of personal information that were or are
2 reasonably believed to have been the subject of a breach.

3 (C) If the information is possible to determine at the time the
4 notice is provided, then any of the following: (i) the date of the
5 breach, (ii) the estimated date of the breach, or (iii) the date range
6 within which the breach occurred. The notification shall also
7 include the date of the notice.

8 (D) Whether notification was delayed as a result of a law
9 enforcement investigation, if that information is possible to
10 determine at the time the notice is provided.

11 (E) A general description of the breach incident, if that
12 information is possible to determine at the time the notice is
13 provided.

14 (F) The toll-free telephone numbers and addresses of the major
15 credit reporting agencies if the breach exposed a social security
16 number or a driver’s license or California identification card
17 number.

18 (3) At the discretion of the person or business, the security
19 breach notification may also include any of the following:

20 (A) Information about what the person or business has done to
21 protect individuals whose information has been breached.

22 (B) Advice on steps that the person whose information has been
23 breached may take to protect himself or herself.

24 (4) In the case of a breach of the security of the system involving
25 personal information defined in paragraph (2) of subdivision (h)
26 for an online account, and no other personal information defined
27 in paragraph (1) of subdivision (h), the person or business may
28 comply with this section by providing the security breach
29 notification in electronic or other form that directs the person whose
30 personal information has been breached promptly to change his
31 or her password and security question or answer, as applicable, or
32 to take other steps appropriate to protect the online account with
33 the person or business and all other online accounts for which the
34 person whose personal information has been breached uses the
35 same user name or email address and password or security question
36 or answer.

37 (5) In the case of a breach of the security of the system involving
38 personal information defined in paragraph (2) of subdivision (h)
39 for login credentials of an email account furnished by the person
40 or business, the person or business shall not comply with this

1 section by providing the security breach notification to that email
2 address, but may, instead, comply with this section by providing
3 notice by another method described in subdivision (j) or by clear
4 and conspicuous notice delivered to the resident online when the
5 resident is connected to the online account from an Internet
6 Protocol address or online location from which the person or
7 business knows the resident customarily accesses the account.

8 (e) A covered entity under the federal Health Insurance
9 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d
10 et seq.) will be deemed to have complied with the notice
11 requirements in subdivision (d) if it has complied completely with
12 Section 13402(f) of the federal Health Information Technology
13 for Economic and Clinical Health Act (Public Law 111-5).
14 However, nothing in this subdivision shall be construed to exempt
15 a covered entity from any other provision of this section.

16 (f) Any person or business that is required to issue a security
17 breach notification pursuant to this section to more than 500
18 California residents as a result of a single breach of the security
19 system shall electronically submit a single sample copy of that
20 security breach notification, excluding any personally identifiable
21 information, to the Attorney General. A single sample copy of a
22 security breach notification shall not be deemed to be within
23 subdivision (f) of Section 6254 of the Government Code.

24 (g) For purposes of this section, “breach of the security of the
25 system” means unauthorized acquisition of computerized data that
26 compromises the security, confidentiality, or integrity of personal
27 information maintained by the person or business. Good faith
28 acquisition of personal information by an employee or agent of
29 the person or business for the purposes of the person or business
30 is not a breach of the security of the system, provided that the
31 personal information is not used or subject to further unauthorized
32 disclosure.

33 (h) For purposes of this section, “personal information” means
34 ~~any~~ *either* of the following:

35 (1) An individual’s first name or first initial and last name in
36 combination with any one or more of the following data elements,
37 when either the name or the data elements are not encrypted:

38 (A) Social security number.

39 (B) Driver’s license number or California identification card
40 number.

1 (C) Account number, credit or debit card number, in
2 combination with any required security code, access code, or
3 password that would permit access to an individual's financial
4 account.

5 (D) Medical information.

6 (E) Health insurance information.

7 (F) *Information or data collected through the use or operation*
8 *of an automated license plate recognition system, as defined in*
9 *Section 1798.90.5.*

10 (2) A user name or email address, in combination with a
11 password or security question and answer that would permit access
12 to an online account.

13 ~~(3) Information or data collected through the use or operation~~
14 ~~of an automated license plate recognition system, as defined in~~
15 ~~Section 1798.90.5, when that information or data is not encrypted.~~

16 (i) (1) For purposes of this section, "personal information" does
17 not include publicly available information that is lawfully made
18 available to the general public from federal, state, or local
19 government records.

20 (2) For purposes of this section, "medical information" means
21 any information regarding an individual's medical history, mental
22 or physical condition, or medical treatment or diagnosis by a health
23 care professional.

24 (3) For purposes of this section, "health insurance information"
25 means an individual's health insurance policy number or subscriber
26 identification number, any unique identifier used by a health insurer
27 to identify the individual, or any information in an individual's
28 application and claims history, including any appeals records.

29 (j) For purposes of this section, "notice" may be provided by
30 one of the following methods:

31 (1) Written notice.

32 (2) Electronic notice, if the notice provided is consistent with
33 the provisions regarding electronic records and signatures set forth
34 in Section 7001 of Title 15 of the United States Code.

35 (3) Substitute notice, if the person or business demonstrates that
36 the cost of providing notice would exceed two hundred fifty
37 thousand dollars (\$250,000), or that the affected class of subject
38 persons to be notified exceeds 500,000 persons, or the person or
39 business does not have sufficient contact information. Substitute
40 notice shall consist of all of the following:

1 (A) Email notice when the person or business has an email
2 address for the subject persons.

3 (B) Conspicuous posting of the notice on the Internet Web site
4 page of the person or business, if the person or business maintains
5 one.

6 (C) Notification to major statewide media.

7 (k) Notwithstanding subdivision (j), a person or business that
8 maintains its own notification procedures as part of an information
9 security policy for the treatment of personal information and is
10 otherwise consistent with the timing requirements of this part, shall
11 be deemed to be in compliance with the notification requirements
12 of this section if the person or business notifies subject persons in
13 accordance with its policies in the event of a breach of security of
14 the system.

15 SEC. 3. Title 1.81.23 (commencing with Section 1798.90.5)
16 is added to Part 4 of Division 3 of the Civil Code, to read:

17

18 TITLE 1.81.23. COLLECTION OF LICENSE PLATE
19 INFORMATION

20

21 1798.90.5. The following definitions shall apply for purposes
22 of this title:

23 (a) “ALPR operator” means a person that uses or operates an
24 ALPR system, or accesses, stores, or maintains information or data
25 collected through the use or operation of an ALPR system, but
26 does not include the Department of the California Highway Patrol
27 when subject to Section 2413 of the Vehicle Code or a
28 transportation agency when subject to Section 31490 of the Streets
29 and Highways Code.

30 (b) “Automated license plate recognition system” or “ALPR
31 system” means a system of one or more mobile or fixed cameras
32 combined with computer algorithms to read and convert images
33 of registration plates and the characters they contain into
34 computer-readable data.

35 (c) “Person” includes a law enforcement agency, government
36 agency, private entity, or individual.

37 (d) “Public agency” means and includes every state agency and
38 every local agency.

39 1798.90.51. An ALPR operator shall do all of the following:

1 (a) Comply with all applicable statutory and constitutional
2 requirements and this title.

3 (b) (1) Ensure that the information or data collected through
4 the use or operation of the ALPR system is protected with
5 reasonable operational, administrative, technical, and physical
6 safeguards to ensure its confidentiality and integrity.

7 (2) Implement and maintain reasonable security procedures and
8 practices appropriate for the nature of the information or data
9 collected, in order to protect the information or data from
10 unauthorized access, destruction, use, modification, or disclosure,
11 and to ensure compliance with this title.

12 (c) Implement and maintain a usage and privacy policy in order
13 to ensure that the information or data collected through the use or
14 operation of the ALPR system is consistent with respect for
15 individuals’ privacy and civil liberties. The usage and privacy
16 policy shall be available in writing, and, if the ALPR operator has
17 an Internet Web site, the usage and privacy policy shall be posted
18 conspicuously on that Internet Web site.

19 1798.90.52. An ALPR operator shall not ~~do either of the~~
20 ~~following:~~ *collect license plate data when a license plate number*
21 *is not in public view.*

22 ~~(a) Retain any information or data other than the license plate~~
23 ~~number, the date and time the information or data is collected, and~~
24 ~~the location coordinates where the information or data is collected.~~
25 ~~This information or data shall not be collected if the license plate~~
26 ~~number is not in public view.~~

27 ~~(b) (1) Trespass or otherwise enter upon private property to~~
28 ~~collect information or data for commercial purposes through the~~
29 ~~use or operation of an ALPR system without first obtaining written~~
30 ~~consent from the owner of the private property, or the owner’s~~
31 ~~designated agent.~~

32 ~~(2) This subdivision shall only apply if the ALPR operator is a~~
33 ~~private entity that operates an ALPR system for commercial~~
34 ~~purposes.~~

35 1798.90.53. If an ALPR operator accesses or provides access
36 to information or data collected through the use or operation of an
37 ALPR system, the ALPR operator shall maintain a record of that
38 access. At a minimum, the record shall include, but not be limited
39 to, all of the following:

40 (a) The date and time the information or data is accessed.

1 (b) The person who accesses the information or data.

2 (c) The purpose for accessing the information or data.

3 ~~1798.90.54. Information or data collected through the use or~~
4 ~~operation of an ALPR system shall not be the sole basis for~~
5 ~~establishing probable cause to obtain a search or arrest warrant.~~

6 ~~1798.90.55.~~

7 *1798.90.54.* (a) In addition to any other sanctions, penalties,
8 or remedies provided by law, an individual who has been harmed
9 by a violation of this title may bring a civil action in any court of
10 competent jurisdiction against a person who knowingly caused
11 that violation.

12 (b) The court may award all of the following:

13 (1) Actual damages, but not less than liquidated damages in the
14 amount of two thousand five hundred dollars (\$2,500).

15 (2) Punitive damages upon proof of willful or reckless disregard
16 of the law.

17 (3) Reasonable attorney's fees and other litigation costs
18 reasonably incurred.

19 (4) Other preliminary and equitable relief as the court determines
20 to be appropriate.