

Introduced by Senator HillDecember 1, 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 34, as introduced, 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, ensuring that the information the ALPR operator collects is protected with certain safeguards, and implementing and maintaining specified security procedures and a usage and privacy policy with respect to that information.

The bill would require an ALPR operator that accesses or provides access to ALPR information to maintain a specified record of that access.

This bill would also require an “ALPR end-user,” as defined, to implement and maintain a specified usage and privacy policy.

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.

The bill would require a public agency that considers implementing a program to gather information through the use of an ALPR system to provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before it implements the program.

(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 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

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

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

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

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

24 (1) The security breach notification shall be written in plain
25 language.

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

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

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

32 (C) If the information is possible to determine at the time the
33 notice is provided, then any of the following: (i) the date of the
34 breach, (ii) the estimated date of the breach, or (iii) the date range
35 within which the breach occurred. The notification shall also
36 include the date of the notice.

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

1 (E) A general description of the breach incident, if that
2 information is possible to determine at the time the notice is
3 provided.

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

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

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

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

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

26 (5) In the case of a breach of the security of the system involving
27 personal information defined in paragraph (2) of subdivision (g)
28 for login credentials of an email account furnished by the agency,
29 the agency shall not comply with this section by providing the
30 security breach notification to that email address, but may, instead,
31 comply with this section by providing notice by another method
32 described in subdivision (i) or by clear and conspicuous notice
33 delivered to the resident online when the resident is connected to
34 the online account from an Internet Protocol address or online
35 location from which the agency knows the resident customarily
36 accesses the account.

37 (e) Any agency that is required to issue a security breach
38 notification pursuant to this section to more than 500 California
39 residents as a result of a single breach of the security system shall
40 electronically submit a single sample copy of that security breach

1 notification, excluding any personally identifiable information, to
2 the Attorney General. A single sample copy of a security breach
3 notification shall not be deemed to be within subdivision (f) of
4 Section 6254 of the Government Code.

5 (f) For purposes of this section, “breach of the security of the
6 system” means unauthorized acquisition of computerized data that
7 compromises the security, confidentiality, or integrity of personal
8 information maintained by the agency. Good faith acquisition of
9 personal information by an employee or agent of the agency for
10 the purposes of the agency is not a breach of the security of the
11 system, provided that the personal information is not used or
12 subject to further unauthorized disclosure.

13 (g) For purposes of this section, “personal information” means
14 either of the following:

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

18 (A) Social security number.

19 (B) Driver’s license number or California identification card
20 number.

21 (C) Account number, credit or debit card number, in
22 combination with any required security code, access code, or
23 password that would permit access to an individual’s financial
24 account.

25 (D) Medical information.

26 (E) Health insurance information.

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

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

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

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

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

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

8 (1) Written notice.

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

12 (3) Substitute notice, if the agency demonstrates that the cost
13 of providing notice would exceed two hundred fifty thousand
14 dollars (\$250,000), or that the affected class of subject persons to
15 be notified exceeds 500,000, or the agency does not have sufficient
16 contact information. Substitute notice shall consist of all of the
17 following:

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

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

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

24 (j) Notwithstanding subdivision (i), an agency that maintains
25 its own notification procedures as part of an information security
26 policy for the treatment of personal information and is otherwise
27 consistent with the timing requirements of this part shall be deemed
28 to be in compliance with the notification requirements of this
29 section if it notifies subject persons in accordance with its policies
30 in the event of a breach of security of the system.

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

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

36 1798.82. (a) A person or business that conducts business in
37 California, and that owns or licenses computerized data that
38 includes personal information, shall disclose a breach of the
39 security of the system following discovery or notification of the
40 breach in the security of the data to a resident of California whose

1 unencrypted personal information was, or is reasonably believed
2 to have been, acquired by an unauthorized person. The disclosure
3 shall be made in the most expedient time possible and without
4 unreasonable delay, consistent with the legitimate needs of law
5 enforcement, as provided in subdivision (c), or any measures
6 necessary to determine the scope of the breach and restore the
7 reasonable integrity of the data system.

8 (b) A person or business that maintains computerized data that
9 includes personal information that the person or business does not
10 own shall notify the owner or licensee of the information of the
11 breach of the security of the data immediately following discovery,
12 if the personal information was, or is reasonably believed to have
13 been, acquired by an unauthorized person.

14 (c) The notification required by this section may be delayed if
15 a law enforcement agency determines that the notification will
16 impede a criminal investigation. The notification required by this
17 section shall be made promptly after the law enforcement agency
18 determines that it will not compromise the investigation.

19 (d) A person or business that is required to issue a security
20 breach notification pursuant to this section shall meet all of the
21 following requirements:

22 (1) The security breach notification shall be written in plain
23 language.

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

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

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

30 (C) If the information is possible to determine at the time the
31 notice is provided, then any of the following: (i) the date of the
32 breach, (ii) the estimated date of the breach, or (iii) the date range
33 within which the breach occurred. The notification shall also
34 include the date of the notice.

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

38 (E) A general description of the breach incident, if that
39 information is possible to determine at the time the notice is
40 provided.

1 (F) The toll-free telephone numbers and addresses of the major
2 credit reporting agencies if the breach exposed a social security
3 number or a driver's license or California identification card
4 number.

5 (G) If the person or business providing the notification was the
6 source of the breach, an offer to provide appropriate identity theft
7 prevention and mitigation services, if any, shall be provided at no
8 cost to the affected person for not less than 12 months, along with
9 all information necessary to take advantage of the offer to any
10 person whose information was or may have been breached if the
11 breach exposed or may have exposed personal information defined
12 in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

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

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

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

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

32 (5) In the case of a breach of the security of the system involving
33 personal information defined in paragraph (2) of subdivision (h)
34 for login credentials of an email account furnished by the person
35 or business, the person or business shall not comply with this
36 section by providing the security breach notification to that email
37 address, but may, instead, comply with this section by providing
38 notice by another method described in subdivision (j) or by clear
39 and conspicuous notice delivered to the resident online when the
40 resident is connected to the online account from an Internet

1 Protocol address or online location from which the person or
2 business knows the resident customarily accesses the account.

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

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

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

28 (h) For purposes of this section, “personal information” means
29 either of the following:

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

33 (A) Social security number.

34 (B) Driver’s license number or California identification card
35 number.

36 (C) Account number, credit or debit card number, in
37 combination with any required security code, access code, or
38 password that would permit access to an individual’s financial
39 account.

40 (D) Medical information.

1 (E) Health insurance information.

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

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

8 (i) (1) For purposes of this section, “personal information” does
9 not include publicly available information that is lawfully made
10 available to the general public from federal, state, or local
11 government records.

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

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

21 (j) For purposes of this section, “notice” may be provided by
22 one of the following methods:

23 (1) Written notice.

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

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

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

35 (B) Conspicuous posting of the notice on the Internet Web site
36 page of the person or business, if the person or business maintains
37 one.

38 (C) Notification to major statewide media.

39 (k) Notwithstanding subdivision (j), a person or business that
40 maintains its own notification procedures as part of an information

1 security policy for the treatment of personal information and is
2 otherwise consistent with the timing requirements of this part, shall
3 be deemed to be in compliance with the notification requirements
4 of this section if the person or business notifies subject persons in
5 accordance with its policies in the event of a breach of security of
6 the system.

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

9

10 TITLE 1.81.23. COLLECTION OF LICENSE PLATE
11 INFORMATION
12

13 1798.90.5. The following definitions shall apply for purposes
14 of this title:

15 (a) “Automated license plate recognition end-user” or “ALPR
16 end-user” means a person that accesses or uses ALPR information,
17 but does not include a transportation agency when subject to
18 Section 31490 of the Streets and Highways Code.

19 (b) “Automated license plate recognition information,” or
20 “ALPR information” means information or data collected through
21 the use of an ALPR system.

22 (c) “Automated license plate recognition operator” or “ALPR
23 operator” means a person that operates an ALPR system, or that
24 stores or maintains ALPR information, but does not include a
25 transportation agency when subject to Section 31490 of the Streets
26 and Highways Code.

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

32 (e) “Person” includes a law enforcement agency, government
33 agency, private entity, or individual.

34 (f) “Public agency” means and includes every state agency and
35 every local agency.

36 1798.90.51. An ALPR operator shall do all of the following:

37 (a) (1) Ensure that ALPR information is protected with
38 reasonable operational, administrative, technical, and physical
39 safeguards to ensure its confidentiality and integrity.

1 (2) Implement and maintain reasonable security procedures and
2 practices in order to protect ALPR information from unauthorized
3 access, destruction, use, modification, or disclosure.

4 (b) (1) Implement and maintain a usage and privacy policy in
5 order to ensure that the collection of ALPR information is
6 consistent with respect for individuals' privacy and civil liberties.
7 The usage and privacy policy shall be available in writing, and, if
8 the ALPR operator has an Internet Web site, the usage and privacy
9 policy shall be posted conspicuously on that Internet Web site.

10 (2) The usage and privacy policy shall, at a minimum, include
11 all of the following:

12 (A) The authorized purposes for using ALPR systems and
13 collecting ALPR information.

14 (B) A description of the employees and independent contractors
15 who are authorized to use ALPR systems, to collect ALPR
16 information, and to access ALPR information. The policy shall
17 identify the training requirements necessary for those authorized
18 employees and independent contractors.

19 (C) A description of how the use of ALPR systems will be
20 monitored to ensure compliance with all applicable privacy laws
21 and a process for periodic system audits, including audits of the
22 access log required by Section 1798.90.52.

23 (D) A description of reasonable measures that will be used to
24 ensure the accuracy of ALPR information and a process to correct
25 data errors.

26 (E) A description of how the ALPR operator will comply with
27 the security procedures and practices implemented and maintained
28 pursuant to subdivision (b).

29 (F) The length of time ALPR information will be stored or
30 retained.

31 (G) The official custodian, or owner, of ALPR information and
32 which employees and independent contractors have the
33 responsibility and accountability for implementing subdivision (b)
34 and this subdivision.

35 (H) The purpose of, and process for, sharing or disseminating
36 ALPR information with other persons.

37 1798.90.52. If an ALPR operator accesses or provides access
38 to ALPR information, the ALPR operator shall maintain a record
39 of that access. At a minimum, the record shall include all of the
40 following:

- 1 (a) The date and time the information is accessed.
- 2 (b) The license plate number or other data elements used to
- 3 query the ALPR database or system.
- 4 (c) The person who accesses the information.
- 5 (d) The purpose for accessing the information.

6 1798.90.53. (a) An ALPR end-user shall implement and
7 maintain a usage and privacy policy in order to ensure that the
8 access and use of ALPR information is consistent with respect for
9 individuals' privacy and civil liberties. The usage and privacy
10 policy shall be available in writing, and, if the ALPR end-user has
11 an Internet Web site, the usage and privacy policy shall be posted
12 conspicuously on that Internet Web site.

13 (b) The usage and privacy policy shall, at a minimum, include
14 all of the following:

15 (1) The authorized purposes for accessing and using ALPR
16 information.

17 (2) A description of the employees and independent contractors
18 who are authorized to access and use ALPR information. The
19 policy shall identify the training requirements necessary for those
20 authorized employees and independent contractors.

21 (3) A description of how the access and use of ALPR
22 information will be monitored to ensure compliance with all
23 applicable privacy laws and a process for periodic system audits.

24 (4) The length of time ALPR information will be retained by
25 the ALPR end-user and the process the ALPR end-user will utilize
26 to determine if and when to destroy the retained ALPR information.

27 (5) The official custodian of ALPR information.

28 (6) The purpose of, and process for, sharing or disseminating
29 ALPR information with other persons.

30 (7) A description of how the end-user will implement reasonable
31 security measures to secure ALPR information from unauthorized
32 access, destruction, use, modification, or disclosure.

33 1798.90.54. (a) In addition to any other sanctions, penalties,
34 or remedies provided by law, an individual who has been harmed
35 by a violation of this title may bring a civil action in any court of
36 competent jurisdiction against a person who knowingly caused
37 that violation.

38 (b) The court may award a combination of any one or more of
39 the following:

- 1 (1) Actual damages, but not less than liquidated damages in the
- 2 amount of two thousand five hundred dollars (\$2,500).
- 3 (2) Punitive damages upon proof of willful or reckless disregard
- 4 of the law.
- 5 (3) Reasonable attorney’s fees and other litigation costs
- 6 reasonably incurred.
- 7 (4) Other preliminary and equitable relief as the court determines
- 8 to be appropriate.
- 9 1798.90.55. Notwithstanding any other law or regulation, a
- 10 public agency that considers implementing a program to gather
- 11 information through the use of an ALPR system shall provide an
- 12 opportunity for public comment at a regularly scheduled public
- 13 meeting of the governing body of the public agency before it
- 14 implements the program.

O