Study G-300 December 1, 2014

Memorandum 2014-55

State and Local Agency Access to Customer Information from Communication Service Providers: California Privacy Statutes

In 2013, the Legislature enacted Senate Concurrent Resolution 54 (Padilla), which directs the Commission[1] to make recommendations to revise the statutes that govern the access of state and local government agencies to customer information from communications service providers. The revisions are intended to do all of the following:

(1) Modernize the law.
(2) Protect customers' constitutional rights.
(3) Enable state and local agencies to protect public safety.
(4) Clarify procedures.

In conducting the study, the Commission is first analyzing existing law that affects government access to customer information from communication service providers. Memorandum 2014-50 began the discussion of relevant state statutory law, by examining the California Invasion of Privacy Act and the California Wiretap Act. This memorandum continues the discussion of state statutory law, by surveying other state statutes that might have some relevance to the study.

In preparing this memorandum, the staff searched broadly for state statutes that touch on consumer privacy and consulted secondary sources that describe state privacy laws. The staff is confident that it found most, if not all, of the statutes that are relevant to this study. However, it seems unlikely that the staff located every California statute that touches on some aspect of privacy. Such statutes are too various in form and expression for the staff to be certain that all

1. Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

have been discovered. **The staff invites comment on whether there are any other relevant privacy statutes that should be included in this analysis.**

To assess whether a state privacy statute is relevant to this study, the staff considered whether the statute satisfies the following criteria:

- The statute restricts disclosure of customer information.
- The restriction could apply to a communication service provider.
- The restriction could apply to government access.

Statutes that meet all of those criteria are discussed under the heading "Applicable Disclosure Restrictions."

Some statutes restrict disclosure of customer information, but the restriction does not appear to be applicable to government access to information held by communication service providers. Those statutes are not relevant to the current study. They are briefly summarized under the heading "Inapplicable Disclosure Restrictions."

Finally, there are privacy-related statutes that do not actually restrict the disclosure of private information. These statutes are also not relevant to our study. For the sake of completeness, those statutes are briefly noted, under the heading "No Restriction on Disclosure."

The contents of this memorandum are organized as follows:

The Commission invites public input on the matters discussed in this memorandum and any other point that is relevant to this study. Any interested person or group can submit formal comment to the Commission, either in writing or at a meeting. The staff is also open to receiving informal input, and is willing to meet with any interested group.

APPLICABLE DISCLOSURE RESTRICTIONS

State statutes that could restrict government access to customer information of communication service providers are described below.

Reader Privacy Act

The Reader Privacy Act ("RPA") was enacted in 2011. It established a fairly robust system of protection for the customer information of a book service provider.[2]

> "Book service" means a service that, as its primary purpose, provides the rental, purchase, borrowing, browsing, or viewing of books. "Book service" does not include a store that sells a variety of consumer products when the book service sales do not exceed 2 percent of the store's total annual gross sales of consumer products sold in the United States.[3]

A "provider" is a commercial entity that provides book service.[4]

2. Civ. Code §§ 1798.90-1798.90.05; 2011 Cal. Stat. ch. 424.
3. Civ. Code § 1798.90(b)(2).
4. *Id.* at (b)(6).

Prohibitions

The RPA generally prohibits a provider from knowingly disclosing the personal information of a user of its services to a government entity.[5]

The defined term "personal information" is not limited to information that identifies the user. It also includes "any information that relates to, or is capable of being associated with, a particular user's access to or use of a book service or a book, in whole or in partial form."[6] The term "book" includes electronic and audio files (but does not include magazines, newspapers, and other serials).[7] The term "personal information" expressly includes IP addresses.[8] Thus, any information that would reveal what books a customer has accessed would fall within the scope of the prohibition. This would include electronic books accessed over the Internet.

Exceptions Generally

The RPA provides exceptions for disclosure under the following circumstances:

- Disclosure to any person pursuant to the user's express consent.[9]
- Disclosure to law enforcement pursuant to court order.[10]
- Disclosure to an entity other than law enforcement pursuant to court order.[11]
- Disclosure required by an emergency.[12]
- Disclosure of evidence of crime against provider.[13]
- Disclosure of evidence of child sexual exploitation, pursuant to a search warrant.[14]

5. *Id.* at (c).
6. *Id.* at (b)(5).
7. *Id.* at (b)(1).
8. *Id.* at (b)(5).
9. *Id.* at (c)(3).
10. *Id.* at (c)(1).
11. *Id.* at (c)(2).
12. *Id.* at (c)(4) ("A provider may disclose personal information of a user to a government entity, if the government entity asserts, and the provider in good faith believes, that there is an imminent danger of death or serious physical injury requiring the immediate disclosure of the requested personal information and there is insufficient time to obtain a court order. The government entity seeking the disclosure shall provide the provider with a written statement setting forth the facts giving rise to the emergency upon request or no later than 48 hours after seeking disclosure.").
13. *Id.* at (c)(5).
14. Civ. Code § 1798.90.05.

The exceptions relating to court-ordered government access are discussed further below.

Disclosure to Law Enforcement

A provider may disclose a user's personal information to law enforcement if presented with a court order that meets specified criteria:

- The court finds probable cause to believe that the requested information is relevant to an investigated offense and finds one of the general grounds for issuance of a warrant under Penal Code Section 1524.[15]
- The court finds that law enforcement has a "compelling interest" in obtaining the requested information.[16]
- The court finds that the requested information "cannot be obtained" by "less intrusive means."[17]
- Law enforcement gives the provider sufficient advance notice to give an opportunity to contest the issuance of the order.[18]
- Law enforcement provides contemporaneous notice to the user (unless the court finds a "strong showing of necessity" to delay notice by up to 90 days).[19]

In effect, this is a "super warrant" requirement, because it imposes an elevated standard ("compelling interest") and requires the exhaustion of other methods of obtaining the information.

Disclosure to Government Entity Other Than Law Enforcement

A provider can disclose user information to a government entity other than law enforcement in two circumstances:

- Pursuant to a court order relating to an "offense under investigation" by the government entity.[20]
- Pursuant to a court order "in a pending action brought by the government entity…."[21]

In both cases, the court order must meet criteria similar to those that govern a law enforcement warrant: a finding of "compelling interest," a finding that the

15. Civ. Code § 1798.90(c)(1)(A).
16. *Id.* at (c)(1)(B).
17. *Id.* at (c)(1)(C).
18. *Id.* at (c)(1)(D).
19. *Id.* at (c)(1)(E).
20. *Id.* at (c)(2)(A).
21. *Id.* at (c)(2)(B).

information cannot be obtained by less intrusive means, notice to the provider with an opportunity to quash, and notice to the user.[22] However, the user notice required in this context is stricter than the notice required for a law enforcement order — information obtained pursuant to the court order cannot be used until the book service user has had at least 35 days notice and an opportunity to quash the order.[23]

Remedies

In general, evidence obtained in violation of the RPA is not admissible in a civil or administrative proceeding.[24] Because this exclusion rule does not apply to criminal proceedings, it does not implicate the Truth-in-Evidence rule in Section 28 of Article 1 of the California Constitution.

In addition, a provider who violates the RPA is subject to specified civil penalties.[25] "Objectively reasonable" reliance on a warrant or court order is a complete defense to a civil action for a violation of the RPA.[26]

Scope of Application

For the purposes of the RPA, a "book" is "paginated or similarly organized content" in any format, including electronic files and audio (but excluding serials, such as newspapers and magazines).[27] Thus, in addition to hard copy, the term "book" would seem to include web-based texts, served pdf files, e-books, and audio readings of texts. A provider is a commercial entity whose primary purpose is to provide opportunities to rent, purchase, borrow, browse, or view books.[28]

It is not entirely clear that an entity that provides book service is necessarily a "communication service provider." Certainly, a book service facilities the flow of information, but it provides a one-way flow rather than the back-and-forth of communication between two parties. That said, it seems possible that an online book service provider could also provide services that are clearly communication-related, and those communication services could be blended with book services in some inextricable way. For that reason, it would be

22. *Id.*
23. *Id.* at (c)(2)(B)(iv).
24. *Id.* at (f).
25. *Id.* at (g).
26. *Id.* at (h).
27. *Id.* at (b)(1).
28. *Id.* at (b)(2), (6).

prudent to assume that a book service provider can be a communication service provider within the scope of this study.

Video Sales or Rentals

Civil Code Section 1799.3 generally prohibits a person who provides "video recording" sales and rentals from disclosing "any personal information or the contents of any record, including sales or rental information," to any person other than the subject of the information.

Exceptions

There are a number of exceptions to the general prohibition, including exceptions for the consent of the subject, discovery in a civil action, a search warrant, disclosure to taxing agencies for tax purposes, and use for unspecified "commercial purposes."[29]

Notably, the section also includes a very relaxed exception for disclosure to law enforcement. The prohibition does not apply to "a disclosure to a law enforcement agency when required for investigations of criminal activity, unless that disclosure is prohibited by law."[30] It is not clear that this exception has any real effect, because federal law requires a search warrant for disclosure of video viewing records to law enforcement.[31] That stricter requirement probably preempts the looser standard in Section 1799.3.

Scope of Application

The prohibition described above relates to the sale or rental of "video recordings." That term may be broad enough to include streaming video over the Internet.

The staff did not find any California appellate case discussing the scope of Section 1799.3. However, the provision was amended on the Commission's recommendation in 2009.[32] The modernizing amendment replaced a reference to "video cassette" with the technology-neutral term, "video recording." That legislative history adds weight to the likelihood that Section 1799.3 would be construed to apply to streaming video services.

29. Civ. Code § 1799.3(b).
30. *Id.* at (b)(3).
31. See 18 U.S.C. § 2710(b).
32. 2009 Cal. Stat. ch. 88, § 14; *Technical and Minor Substantive Statutory Corrections: References to Recording Technology*, 37 Cal. L. Revision Comm'n Reports 211 (2007).

If the section applies to Internet streaming services, then it probably applies to communication service providers within the scope of the current study.

California Right to Financial Privacy Act

The California Right to Financial Privacy Act ("CRFPA")[33] restricts government access to customer[34] financial records[35] held by financial institutions.[36] The CRFPA applies to record access by state and local agencies, and to law enforcement investigations.[37] (As noted in a prior memorandum, access to financial records is also regulated by federal law.[38])

The purpose of the CRFPA is to

> clarify and protect the confidential relationship between financial institutions and their customers and to balance a citizen's right of privacy with the governmental interest in obtaining information for specific purposes and by specified procedures as set forth in this chapter.[39]

Prohibitions

State and local government may not, in connection with a civil or criminal investigation (whether or not related to formal judicial or administrative proceedings), *request* customer financial records from a financial institution, unless (1) the records are described with particularity, (2) the records are consistent with the scope and requirements of the investigation, and (3) a specified exception applies.[40]

Conversely, a financial institution may not *provide* financial records to state or local government if it knows or has reasonable cause to believe that the records were requested in connection with a civil or criminal investigation of a customer (whether or not related to formal judicial or administrative proceedings), unless a specified exception applies.[41]

33. Gov't Code §§ 7460-7493.
34. Gov't Code § 7465(d).
35. *Id*. at (b).
36. *Id*. at (a).
37. *Id*. at (h).
38. See 12 U.S.C. § 3401 *et seq.*; Memorandum 2014-34, p. 12.
39. *Id*. at (c).
40. Gov't Code § 7470(a).
41. Gov't Code § 7471(a).

Exceptions

There are exceptions to the general prohibitions in the following circumstances:

- The customer has given express consent, in writing. Government must give the customer notice when acting pursuant to this exception.[42]
- Government is acting pursuant to an administrative subpoena or summons. The subpoena or summons must also be served on the customer, at least 10 days before obtaining the records.[43] Such service can be waived or shortened on court order (during which time the financial institution cannot notify the customer of the request).[44] The customer may move to quash the subpoena or summons.[45]
- Government is acting pursuant to a search warrant. The financial institution must provide the requested records within 10 days, unless the court specifies otherwise.[46] The financial institution may notify the customer of the search, unless the court has ordered otherwise.[47]
- Government is acting pursuant to a judicial subpoena or subpoena duces tecum. The subpoena must be served on the financial institution and customer (or government must demonstrate due diligence in attempting to serve the customer).[48] The customer may move to quash within 10 days after service.[49]
- Government is acting pursuant to a grand jury subpoena.[50] The subpoena must be served on the financial institution and customer (or government must demonstrate due diligence in attempting to serve the customer).[51] The customer may move to quash within 10 days after service.[52]

A financial institution may also disclose customer financial records to government if it believes it has been the victim of a crime and the records are relevant to that crime.[53]

42. Gov't Code § 7473(d).
43. Gov't Code § 7474(a).
44. *Id.* at (b).
45. *Id.* at (d).
46. Gov't Code § 7475.
47. *Id*.
48. Gov't Code § 7476(a)(1).
49. *Id*. at (a)(2).
50. *Id*. at (b).
51. *Id*.
52. *Id*.
53. *Id*. at (d).

Scope of Application

Many financial institutions provide online services to their customers. Some aspects of these services could be classified as "communication" services (e.g., online chat, proprietary messaging systems, and the like). It therefore seems possible that a financial institution could be a "communication service provider" with respect to some types of online customer service. If so, a state or local agency request to access information about a customer's use of such services would seem to fall within the scope of the Commission's study.

Confidentiality of Medical Information Act

The Confidentiality of Medical Information Act ("CMIA")[54] regulates the use and disclosure of patient information by a provider of health care. (As noted in a prior memorandum, access to medical records is also regulated by federal law.[55])

Prohibitions

For the purposes this study, the most relevant element of the CMIA is a general prohibition on provider disclosure of patient information (without first obtaining valid authorization).[56] There are also a few provisions that govern the use or disclosure of health records in specific circumstances.[57]

Exceptions

Most of the exceptions to the prohibitions described above are not relevant to this study, because they govern the disclosure of patient information to entities other than state or local government agencies.[58]

However, there are exceptions for requests made by government entities. They include exceptions for requests made by the following means:

> (1) By a court pursuant to an order of that court.
> (2) By a board, commission, or administrative agency for purposes of adjudication pursuant to its lawful authority.
> …
> (4) By a board, commission, or administrative agency pursuant to an investigative subpoena issued under Article 2 (commencing

54. Civ. Code §§ 56-56.37.
55. See P.L. 104-191 (1996); Memorandum 2014-34, pp. 3-6.
56. Civ. Code § 56.10(a). See also Civ. Code §§ 56.11-56.15 (valid authorization).
57. See, e.g., Civ. Code §§ 56.104 (outpatient psychotherapist treatment), 56.106 (minor patient of psychotherapist), 56.16 (specified information about patient in acute care hospital), 56.17 (genetic test results), 56.20-56.245 (employer-maintained health records), 56.26 (third party administrators), 56.265 (insurers).
58. See, e.g., Civ. Code §§ 56.10(c), 56.1007, 56.103, 56.105, 56.16, 56.27, 56.30.

with Section 11180) of Chapter 2 of Part 1 of Division 3 of Title 2 of the Government Code.

…

(6) By a search warrant lawfully issued to a governmental law enforcement agency.

…

(8) By a coroner, when requested in the course of an investigation by the coroner's office for the purpose of identifying the decedent or locating next of kin, or when investigating deaths that may involve public health concerns, organ or tissue donation, child abuse, elder abuse, suicides, poisonings, accidents, sudden infant deaths, suspicious deaths, unknown deaths, or criminal deaths, or upon notification of, or investigation of, imminent deaths that may involve organ or tissue donation pursuant to Section 7151.15 of the Health and Safety Code, or when otherwise authorized by the decedent's representative. Medical information requested by the coroner under this paragraph shall be limited to information regarding the patient who is the decedent and who is the subject of the investigation or who is the prospective donor and shall be disclosed to the coroner without delay upon request.[59]

There are also exceptions for any disclosure that is "specifically required by law,"[60] for a disclosure that is required as part of discovery in a judicial or administrative proceeding,[61] and for disclosure required as part of discovery in arbitration.[62] In addition, there are specific exceptions that only apply to particular types of prohibitions.[63]

Importantly, the entire CMIA is inapplicable to a law enforcement request for patient medical records that is conducted pursuant to Penal Code Sections 1543 to 1545.[64] Those sections are discussed in the next segment of this memorandum.

Scope of Application

The general prohibition on disclosure of protected patient information applies to a "provider of health care,"[65] a "health care service plan,"[66] or a "contractor."[67]

---

59. Civ. Code § 56.10(b).
60. *Id.* at (b)(9).
61. *Id.* at (b)(3).
62. *Id.* at (b)(5).
63. See, e.g., Civ. Code §§ 56.104(d) (outpatient psychotherapist treatment), 56.20(c)(1) (employer-maintained health records).
64. Civ. Code § 56.30(g).
65. Civ. Code § 56.05(m) ("'Provider of health care' means any person licensed or certified pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code; any person licensed pursuant to the Osteopathic Initiative Act or the Chiropractic Initiative Act; any person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code; any clinic, health dispensary, or health facility licensed pursuant to Division 2 (commencing with Section 1200) of the Health and Safety Code. 'Provider of health care' does not

Could such an entity ever be a "communication services provider" within the scope of the Commission's study? Perhaps, with regard to any communication services that the entity provides. Some healthcare providers operate communication systems for use by their patients. Patients may be able to log onto the provider's website and send private messages to a doctor, fill prescriptions, access test results, download medical records, and make appointments. In areas where medical facilities are inconveniently remote, providers may use online chat or videoconferencing to "meet" with patients.

With regard to such services, a medical provider could be considered a communication service provider within the scope of the current study.

Medical Record Disclosure Under the Penal Code

As noted above, the CMIA does not apply to medical records that are disclosed to law enforcement pursuant to Penal Code Sections 1543 to 1545. The rules for access under those sections are discussed below.

Disclosure

Penal Code Section 1543 establishes three circumstances in which a health care facility may disclose unprivileged patient records to a law enforcement agency.[68] Disclosure is permitted (1) with the patient's prior written consent,[69] (2) pursuant to a search warrant,[70] or (3) pursuant to a court order that is based on "good cause."[71]

In assessing whether there is "good cause" under the third rule, a court must balance the public's interest, the need for disclosure, and any injury to the patient, the patient-practitioner relationship, or the patient's treatment. The court

---

include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code.").

66. Civ. Code § 56.05(g) ("'Health care service plan' means any entity regulated pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code).").

67. Civ. Code § 56.05(d) ("'Contractor' means any person or entity that is a medical group, independent practice association, pharmaceutical benefits manager, or a medical service organization and is not a health care service plan or provider of health care. 'Contractor' does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code or pharmaceutical benefits managers licensed pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code").

68. Penal Code § 1545(b) (i.e., the Attorney General, a district attorney, or an agency of state government authorized by statute to investigate or prosecute law violations).

69. Penal Code § 1543(a)(1).

70. *Id.* at (a)(3).

71. *Id.* at (a)(2).

must also determine that there is a reasonable likelihood that the records will provide material information or evidence of substantial value in connection with an investigation or prosecution.[72]

A disclosure order must include terms limiting disclosure and dissemination of information, to prevent unnecessary and overbroad disclosure and dissemination.[73]

Ordinarily, a health care facility must be given advance notice and an opportunity to appear and be heard when medical records are requested.[74] However, that notice can be delayed by up to 30 days on a showing that notice would "seriously impede" an investigation.[75]

Scope of Application

As discussed above in connection with the CMIA, a health care provider could be considered to be a communication service provider with respect to some types of services. In those circumstances, disclosure of medical records under Penal Code Section 1543 could fall within the scope of the current study.

Telephone Customer Right of Privacy

Public Utilities Code Sections 2891 to 2894.10 provide miscellaneous protections for the privacy of telephone and telegraph company customers. Some of those protections are irrelevant to the current study, because they do not relate to the disclosure of customer records to government.[76] However, there is a provision that generally restricts the disclosure of certain customer information. It is discussed below.

Prohibitions

Public Utilities Code Section 2891 generally prohibits a "telephone or telegraph corporation" from disclosing specified information, regarding a residential subscriber, to any other person or corporation. While the term "person" is not defined to include a government entity,[77] the section includes

72. *Id.*
73. *Id.* at (d).
74. *Id.* at (c).
75. Penal Code § 1544.
76. E.g., Pub. Util. Code §§ 2891.1(a) (selling or licensing residential subscriber lists), (b) inclusion of customer information in directory), 2891.2 (caller ID), 2892 (911 service), 2893 (caller *ID*), 2894.10 (phone solicitation).
77. See Pub. Util. Code § 205 ("'Person' includes an individual, a firm, and a copartnership.").

language that expressly addresses disclosures to government.[78] This strongly suggests that the section's prohibition was intended to apply to a disclosure to government.

The protected information includes a subscriber's calling patterns, credit or other financial information, a description of services received by the subscriber, and demographic information.[79] Consent to disclosure under Section 2891 is also a prerequisite to a subpoena duces tecum for personal records of a consumer that are held by a telephone corporation.[80]

Exceptions

The prohibition described above is subject to a number of exceptions, including a general exception for disclosure pursuant to the subscriber's consent.[81] Most of those exceptions are not relevant to the current study, because they relate to business needs or emergency response.[82]

However, there is an express exception for "[i]nformation provided to a law enforcement agency in response to lawful process."[83] Presumably lawful process includes any legally authorized law enforcement access, including a general search warrant, subpoena, or other expressly authorized means.[84]

A violation of Section 2891 is grounds for a civil suit.[85] However, there is a complete defense against such an action for

> an interexchange telephone corporation, a local exchange telephone corporation, or a provider of commercial mobile radio service, as defined in Section 216.8, in good faith compliance with the terms of a state or federal court warrant or order or administrative subpoena issued at the request of a law enforcement official or other federal, state, or local governmental agency for law enforcement purposes….[86]

Scope of Application

It is clear that a telephone or telegraph company is a "communication service provider" and would therefore fall within the scope of this study. While the

78. See, e.g., Pub. Util. Code § 2891(d)(6). See also Pub. Util. Code § 2894.
79. Pub. Util. Code § 2891(a).
80. Code Civ. Proc. § 1985.3(f).
81. Pub. Util. Code § 2891(a)-(c).
82. *Id.* at (d).
83. *Id.* at (d)(6).
84. See, e.g., Pub. Util. Code § 588 (release of telephone customer information in connection with child abduction investigation).
85. *Id.* at (e).
86. Pub. Util. Code § 2894.

statute could be clearer, it does appear that Section 2891 applies to a disclosure of customer information to law enforcement. It is less clear that the section would apply to other types of government entities.

Student Records

Education Code Sections 49061 to 49085 regulate the maintenance, use, and disclosure of student records. (As noted in a prior memorandum, access to student records is also regulated by federal law.[87]) Many of the Education Code provisions govern record-keeping practices and parental access to student records, topics that are not relevant to the current study. However, the statutes also include prohibitions on disclosure that could affect government access to student records.

Prohibitions

A school district is generally not permitted to disclose student records without parental consent or a judicial order.[88] There are numerous exceptions to that general rule, which are discussed further below. There are also miscellaneous prohibitions that govern specific types of disclosures.[89]

Exceptions

There are a number of exceptions to the general prohibition noted above. Most relate to educational administration and would not affect government access to student records.[90] There are also exceptions for consent,[91] emergency,[92] and other miscellaneous matters.

For the purposes of this study, the relevant exceptions are those that allow government access to student records. These include a general exception for law enforcement to serve a "proper police purpose,"[93] an exception for a law enforcement investigation related to declaring the student a ward of the court or proving a probation violation,[94] and various investigations relating to truancy and child welfare.[95]

---

87. See 20 U.S.C. § 1232g; Memorandum 2014-34, pp. 10-11.
88. Educ. Code § 49076(a).
89. Educ. Code §§ 49073(c) (directory information of homeless student), 49037.5 (student phone numbers), 49076(a)(4)(E) (information protected by other law).
90. See, e.g., Educ. Code § 49076(a)(1)(A)-(H).
91. Educ. Code § 49075.
92. Educ. Code § 49076(a)(2)(A).
93. Educ. Code § 49076.5.
94. Educ. Code § 49076(a)(1)(I).
95. *Id.* at (a)(1)(G)-(H), (J), (N).

As a general matter, student records "shall be furnished in compliance with a court order or a lawfully issued subpoena."[96]

Scope of Application

Many schools provide proprietary messaging systems that allow students and parents to check grades online and send email messages to teachers and administrators. Such systems would seem to be communication services. With respect to such services, a school could be seen as a communication service provider within the scope of the current study.

Pending Law

In 2014, the Legislature enacted Senate Bill 1177 (Steinberg). The bill would create new regulatory protection of student data that is collected and used by the "operators" of companies providing online services (which includes websites and other online systems) to K-12 schools. The bill was signed by the Governor and its provisions will become operative on January 1, 2016.[97]

The new law includes a prohibition on operator disclosure of student data that the operator has collected, with certain specified exceptions. These include exceptions "to respond to and participate in the judicial process" and "to protect the safety of others."[98] There is also a provision stating that the section does not limit the authority of law enforcement to obtain information from an operator "as authorized by law or pursuant to an order of a court of competent jurisdiction."

The regulated operators could be communication service providers within the scope of this study.

Information Privacy Act of 1977

The Information Privacy Act of 1977 ("IPA")[99] regulates state agency collection and use of personal information.

Prohibitions

The IPA includes a general prohibition on an agency's disclosure of personal information in its records.[100]

96. Educ. Code §§ 49077-49078.
97. 2014 Cal. Stat. ch. 839.
98. Bus. & Prof. Code § 22584(b)(4)(C)-(D).
99. Civ. Code § 1798 *et seq*.
100. Civ. Code § 1798.24.

Exceptions

There are a number of exceptions to the general disclosure prohibition. Most are not relevant to the current study, because they do not affect government access to records.

However, there are exceptions that directly affect government access. These include a blanket exception for law enforcement access[101] and an exception for an investigation of the custodian agency's own wrongdoing.[102]

Scope of Application

It is possible that a state agency can also be a communication service provider. For example, state universities routinely provide email and other communication services to their students and alumni. With regard to such services, the agency would seem to fall within the scope of the current study.

Vehicle Data Recorders

Vehicle Code Section 9951 regulates the use of a vehicle "recording device," which it defines as follows:

> As used in this section, "recording device" means a device that is installed by the manufacturer of the vehicle and does one or more of the following, for the purpose of retrieving data after an accident:
> (1) Records how fast and in which direction the motor vehicle is traveling.
> (2) Records a history of where the motor vehicle travels.
> (3) Records steering performance.
> (4) Records brake performance, including, but not limited to, whether brakes were applied before an accident.
> (5) Records the driver's seatbelt status.
> (6) Has the ability to transmit information concerning an accident in which the motor vehicle has been involved to a central communications system when an accident occurs.[103]

Prohibitions

Section 9951 generally prohibits access to the data stored on a recording device.

101. *Id.* at (*o*).
102. *Id.* at (p).
103. Gov't Code § 9951(b).

Exceptions

There are a number of exceptions to the general prohibition, including exceptions for customer consent, vehicle maintenance, and an "order of a court having jurisdiction to issue the order."[104]

Scope of Application

The term "recording device" includes a device designed to send notice of an accident to a central communication system, presumably for the dispatch of an emergency response. Such a system could be seen as a communication service. If so, the disclosure of accident information to law enforcement could involve government access to customer information of a communication service provider, in which case it would be within the scope of the current study.

Records Held by Attorney, Doctor, Psychotherapist, or Clergy Member

Penal Code Section 1524(c) provides a special procedure for the issuance of a warrant that is used to obtain records that are "in the possession or under the control of" an attorney, doctor, psychotherapist, or clergy member (unless such a person is reasonably suspected of engaging in a crime related to the requested records).

When issuing the warrant, the court must appoint a special master to accompany law enforcement when the warrant is served. If requested records are not produced, the special master will conduct any search that may be necessary to locate the records. If the holder of a requested record asserts that the record should not be disclosed, the special master will seal that record and present it to the court for a hearing on the issue.[105] The apparent purpose is to shield potentially privileged material from disclosure to law enforcement.

It is not clear whether Section 1524(c) would apply to the records of a professional listed above, if the records are held by a communication service provider on the professional's behalf. In such a situation, the records are not in the professional's possession and may not be sufficiently under the professional's control.

In *PSC Geothermal Services Co. v. Superior Court*,[106] the court held that Section 1524 does not apply to records held by consultants that are hired by attorneys, because such records are neither in the attorney's possession, nor under the

104. *Id.* at (c).
105. Penal Code § 1524(c)-(d).
106. 25 Cal. App. 4th 1697 (1994).

attorney's control. The staff did not find any cases discussing whether the same limitation applies to a protected professional's records that are held by a third party for the professional's exclusive use.

Regardless of whether Sec

Journalist Records

Penal Code Section 1524(g) provides that no warrant may be issued for records described in Evidence Code Section 1070. That Evidence Code provision protects specified members of the press from contempt for refusing to disclose sources or "unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public."[107]

> "[U]npublished information" includes information not disseminated to the public by the person from whom disclosure is sought, whether or not related information has been disseminated and includes, but is not limited to, all notes, outtakes, photographs, tapes or other data of whatever sort not itself disseminated to the public through a medium of communication, whether or not published information based upon or related to such material has been disseminated.[108]

The protection provided by Section 1524(g) is not limited to information that is possessed by a journalist. Consequently, it may apply to information that is being held by a communication service provider on behalf of a journalist customer. In that case, the provision would be relevant to the current study. The staff did not find any published California case construing that aspect of Section 1524(g). (As noted in a prior memorandum, access to journalist records is also regulated by federal law.[109])

INAPPLICABLE DISCLOSURE RESTRICTIONS

State statutes that restrict the disclosure of private information, but are not applicable to communication service provider disclosures to government, are described below.

Use of Medical Information in Direct Marketing

Civil Code Section 1798.91 restricts the collection of customer medical information for use in direct marketing. While it does limit the disclosure of such

107. Evid. Code § 1070(a)-(b).
108. *Id.* at (c).
109. See 42 U.S.C. § 2000aa; Memorandum 2014-34, pp. 8-10.

information, it only applies to disclosure for marketing purposes. Consequently, it would not seem to apply to a government request for customer information.

Electrical or Natural Gas Usage Data

Civil Code Section 1798.98 prohibits a business from disclosing customer electrical and natural gas usage data to a third party, unless the disclosure is otherwise required or authorized under federal or state law. The provision has no specific exception for law enforcement access.

Similar prohibitions (and exceptions) are provided in Public Utilities Code Sections 8380 and 8381.

It is difficult to imagine how electrical or natural gas use data could be considered customer information of a communication service provider. It is true that utilities are moving towards the use of wireless "smart meters," but the use of such internal communication technology does not seem to provide enough of a rationale to consider a power company to be a communication service provider.

Business Records

Civil Code Section 1799.1 generally prohibits a bookkeeping company from disclosing client records to third parties. Among the exceptions to that rule are exceptions for access pursuant to a court order or a search warrant.

The staff does not see any significant likelihood that a bookkeeping company would be considered a communication service provider.

Tax Returns

Civil Code Section 1799.1a generally prohibits the disclosure of data drawn from tax returns and schedules that are submitted by a consumer in connection with a financial or other business-related transaction. Among the exceptions to that rule are exceptions for access pursuant to a court order or a search warrant.

It seems very unlikely that a communication service provider would ever require that a customer provide tax records for the types of transactions governed by Section 1799.1a.

Insurance Information

The Insurance Information and Privacy Protection Act ("IIPPA") regulates the collection, use, and disclosure of personal information by specified types of insurance institutions, agents, and insurance support organizations.[110]

Most of the provisions of the IIPPA are not relevant to the current study, because they do not regulate information disclosure. Instead, those provisions regulate data collection,[111] notice to customers,[112] customer access to their own data,[113] data use,[114] and data security.[115]

However, there are provisions that prohibit the disclosure of customer information.[116] The general prohibition on disclosure is subject to numerous exceptions. Most relate to business operation needs, but there are also exceptions for disclosure to "law enforcement or other governmental authority pursuant to law,"[117] disclosure that is "otherwise permitted by law,"[118] and disclosure "in response to a facially valid administrative or judicial order, including a search warrant or subpoena."[119]

Although those prohibitions would apply to disclosure of customer information to government, they do not appear to be relevant to this study because insurance entities are not communication service providers.

Electronic Toll Collection

Streets and Highways Code Section 31490 regulates transportation agency[120] use of personal information associated with electronic toll collection services. Transportation agencies are generally prohibited from disclosing such information to any other person. Exceptions to the prohibition include (1) disclosure to law enforcement pursuant to a search warrant, and (2) disclosure to law enforcement without a warrant if delay would cause an adverse result.[121] The staff does not see any reason to view a transportation agency as a communication service provider.

---

110. Ins. Code §§ 791-791.29.
111. Ins. Code §§ 791.03, 791.11.
112. Ins. Code §§ 791.04-791.07, 791.28.
113. Ins. Code §§ 791.08-791.10.
114. Ins. Code § 791.12.
115. Ins. Code § 791.29.
116. Ins. Code §§ 791.13, 791.27.
117. Ins. Code § 791.13(f).
118. *Id*. at (g).
119. *Id*. at (h).
120. Sts. & Hy. Code § 31490(*l*).
121. *Id.* at (e).

Electronic Surveillance of Rental Vehicles

Civil Code Section 1936(*o*) generally prohibits a vehicle rental company from using electronic surveillance devices to obtain information about a customer's use of a vehicle. There are a handful of exceptions to the prohibition, including one for disclosure to law enforcement pursuant to a subpoena or search warrant.[122] The staff does not see any way that a car rental company would be considered a communication service provider.

Supermarket Club Card Disclosure Act of 1999

The Supermarket Club Card Disclosure Act of 1999 Regulates the collection and use of customer information in connection with supermarket club cards.[123] The statute prohibits the disclosure of a cardholder's personally identifying information. The staff does not believe that a supermarket could be a communication service provider within the scope of the current study.

Social Security Numbers

Civil Code Sections 1798.85 to 1798.89 restricts the public display of social security numbers (except as otherwise required by law). While these provisions do apply to communication service providers, they regulate the broad public display of information, rather than specific government requests for disclosure of the information.

Potential Targets of Harassment

There are a number of provisions that prohibit the public posting or other disclosure of identifying information about persons who are potential targets of harassment or violence.[124] These provisions are about preventing the general public disclosure of such information and do not directly address government access issues.

Department of Motor Vehicles Records

There are a number of provisions in the Vehicle Code that regulate Department of Motor Vehicles record-keeping.[125] In general, driving records held

122. Civ. Code § 1936(o)(2).
123. Civ. Code §§ 1749.60-1749.66.
124. See, e.g., Civ. Code §§ 1798.79.8-1798.79.95 (domestic violence victim); Gov't Code §§ 6208.1-6208.2 (domestic or sexual violence victims), 6218-6218.5 (reproductive healthcare providers); Penal Code § 964 (crime victims and witnesses).
125. See, e.g., Veh. Code §§ 1808, 1808.2, 1808.21, 1808.24, 1808.4, 1808.45-1808.5.

by the DMV are public.[126] That general rule is subject to a number of exceptions.[127] (As noted in a prior memorandum, access to DMV records is also regulated by federal law.[128])

The staff does not believe that the DMV is a communication service provider within the scope of the current study.

Driver's License Data

Civil Code Section 1798.90.1 regulates the use of information that is gained by swiping the magnetic strip on a driver's license. While the statute limits the permissible uses of such information, it does not contain any express prohibition on disclosure that would seem to affect government access.

Workplace Surveillance

Labor Code Section 435 prohibits audio or video recording of employees in workplace restrooms and locker rooms, unless authorized by court order. It also restricts the use of any recordings that are made. Employees are not customers. Consequently, Section 435 should not have any effect on government access to customer information of communication service providers.

Subpoena of Consumer Records

Code of Civil Procedure Section 1985.3 provides a special procedure for a subpoena duce tecum, requesting consumer records held by specified entities (medical provider, financial institution, insurance company, attorney, accountant, telephone corporation that is a public utility, and a private school).

Because Section 1985.3 only applies to civil actions, it is not the type of government access at issue in this study.[129]

NO RESTRICTION ON DISCLOSURE

State statutes that affect privacy, but do not directly restrict the disclosure of private information to a third party, are listed below:

- **Security of Private Customer Records.**[130] Requires that businesses safeguard the security of private customer information in their records, provide notice of security breaches affecting such

126. Veh. Code § 1808(a).
127. See, e.g., Veh. Code § 1808(d), (e).
128. See 18 U.S.C. § 2721 *et seq.*; Memorandum 2014-34, p. 12.
129. Minutes (Feb. 2014), p. 4 (study does not include examination of discovery rules).
130. Civ. Code §§ 1798.80-1798.84.

information, and notify customers when private information is used by third parties for direct marketing. It does not impose any prohibitions on disclosure.

- **Online Privacy Protection Act of 2003.**[131] Requires commercial websites and online service providers that collect personal information to post and abide by a specified privacy policy.
- **Wireless Network Devices.**[132] Requires consumer warnings regarding security risks associated with wireless network devices.
- **Personal Information Collected on Internet.**[133] When state government agencies collect personal information on the Internet, the agency must make specified disclosures to users.
- **Inmate Access to Personal Information.**[134] Inmates in county jail or state prison and juvenile offenders cannot be employed in jobs that give access to personal information of private individuals.
- **Information Disclosed to PUC.**[135] Information that is disclosed to the Public Utilities Commission by a public utility (which could include a communication service provider) is generally not open to public inspection.

CONCLUSION

The staff sees two general questions that are raised by the discussion above:

(1) What is a "communication service provider?"
(2) How can the proposed law be drafted to avoid conflicts with existing statutory privacy protections?

Those questions are discussed below.

Communication Service Provider

From the beginning of this study, the staff has noted the importance and difficulty of understanding what is meant by "communication service provider."[136] That issue lies at the foundation of the study, because it is used by the Legislature in framing the scope of the Commission's work.[137]

That is why the discussion above draws a distinction between statutes that could regulate communication service providers, and those that apparently could not. The former are relevant to the study; the latter are not.

131. Bus. & Prof. Code §§ 22575-22579.
132. Bus. & Prof. Code §§ 22948.5-22948.7.
133. Gov't Code § 11015.5.
134. Penal Code §§ 4017.1 & 5071; Welf. & Inst. Code § 219.5.
135. Pub. Util. Code § 583.
136. See Memorandum 2014-5, pp. 5-6.
137. 2013 Cal. Stat. res. ch. 115 (SCR 54 (Padilla)).

In drawing that distinction, the staff is mindful that the Commission has not adopted any precise definition of the term "communication service provider." Instead, the staff has been making qualitative judgments based on the overall character of a type of service. To what extent does it involve customer communication? A telephone company is clearly a communication service provider; a car rental company is probably not.

This leaves some room for line-drawing uncertainty. But ultimately, the staff is not too concerned about that possibility. While the concept of communication service provider was important in the initial phase of this study, when considering which issues the Commission will need to resolve, it may be mostly irrelevant in the second phase of the study, when the Commission drafts proposed legislation to resolve those issues.

That is because the Commission could draft the proposed legislation to focus on particular *types of information*, rather than the nature of the entity that holds the information. For example, the proposed law could include a rule that specifies a substantive standard and procedure for government access to stored email messages. Such a rule would need to be precise in defining what it means by "email." But there would be no need to address the character of the entity that holds the information. The same rule would apply to *any* entity that provides email service, regardless of whether it is an Internet Service Provider, a healthcare provider, a social networking service, a public school, etc. Under that drafting approach, the meaning of "communication service provider" would be irrelevant.

That drafting approach would also guarantee that the proposed law applies consistently across the board, without any gaps for entities that fall short of being "communication service providers." The approach would also avoid the uncertainty and disputes that seem inevitable if the Commission were to use some concept of "communication service provider" to limit the application of the proposed law.

Coordination with Statutory Privacy Protections

This memorandum and Memorandum 2014-34 illustrate the large variety of statutory privacy protections that exist in state and federal law. Each is framed to address its own particular policy context, often in areas of law that the Commission has not been directed to study. In drafting proposed legislation in

this study, the Commission should be careful not to undermine or supersede any of those existing protections.

Because of the number and variety of those existing statutes, which are likely to continue to change and grow in number over time, it would be extremely difficult to coordinate the proposed law with each provision individually.

Instead, it would make sense to address such statutes globally, with a blanket disclaimer. The Commission's proposal could include a provision expressly stating that the requirements of the proposed law supplement, rather than replace, any other requirements of law. Thus, if law enforcement wishes to obtain email messages that a suspect exchanged with a doctor, using the proprietary email system provided by a healthcare provider, more than one statute would apply to that request. Law enforcement would need to meet the requirements of the proposed law governing email messages, as well as the federal and state statutes governing access to medical records.

That would not be much different from the current situation. Under existing law, if law enforcement wishes to obtain medical records, it would need to consider the general law governing search warrants, as well as any special privacy requirements applicable to healthcare records.

In practice, that should not be too onerous. In most cases, the specific privacy laws contain exceptions for government access pursuant to lawful process. In the example above, the use of a warrant to obtain email would trigger statutory exceptions for both the federal[138] and state[139] medical record privacy laws.

What's Next?

This memorandum concludes the first broad phase of the study, summarizing relevant federal and state law, both constitutional and statutory. The next memorandum will begin the second phase of the work — preparing proposed legislation. The first step in that phase will be to make general policy decisions about the objectives and structure of the proposed law. Once the Commission makes those decisions, drafting can begin.

Respectfully submitted,

Brian Hebert
Executive Director

138. 45 C.F.R. § 164.512(f)(1)(ii)(A).
139. Civ. Code § 56.10(b)(6).