Study G-300 August 21, 2014

Memorandum 2014-33

State and Local Agency Access to Customer Information from Communication Service Providers: Electronic Communications Privacy Act of 1986

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.

Memorandum 2014-5 introduced the study and proposed an overall organizational plan for conducting it. The Commission approved the proposed plan.[2] This memorandum begins the second step in that plan, analysis of controlling federal statutes. It examines the Electronic Communications Privacy Act of 1986 ("ECPA").

The content of the memorandum is organized as follows:

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.

2. See Minutes (Feb. 2014), p. 4.

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.

OVERVIEW OF ECPA

The Electronic Communications Privacy Act of 1986 is a federal bill, enacted in 1986, which modernized federal statutory law governing electronic surveillance.[3] The official name of the bill is commonly used as a shorthand, to refer to the statutes that were amended or added by the bill. For the purposes of this study, the most relevant effects of ECPA are as follows:

- ECPA amended an existing statute on the interception of wire and oral communications (Chapter 119 of Title 18, also known as the "Wiretap Act" or "Title III") to make that statute applicable to electronic communications.
- ECPA added a new statute on access to stored electronic communications (Chapter 121 of Title 18, also known as the "Stored Communications Act" or "SCA").
- ECPA added a new statute on the use of pen registers and trap and trace devices (Chapter 206 of Title 18, hereafter "Pen Register Act").

This memorandum discusses each of those statutes, in their current form, at a *moderate* level of detail. (A comprehensive description of ECPA and the cases construing it would require a book-length treatment.) The point of this discussion is to give an overview of how ECPA regulates access to electronic communications and related customer records.

ECPA also added a single section on the use of mobile tracking devices (to make clear that a warrant authorizing the use of such a device can have effect outside the jurisdiction of the court that issued the warrant).[4] Because this study is limited to government access to customer information *from communication service providers*, and the use of a mobile tracking device does not require the involvement of a communication service provider, the staff believes that the

3. P.L. 99-508; 100 Stat. 1848 (1986)
4. 18 U.S.C. § 3117.

tracking device provision is beyond the scope of this study. For that reason, it is not discussed further in this memorandum.

The memorandum concludes with a discussion of the extent to which each of those statutes preempts state regulation in the same subject area. This issue is particularly important because it will determine the extent to which ECPA constrains the development of California statutes in this area.

INTERCEPTION OF WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS

The Wiretap Act governs the interception[5] of wire,[6] oral,[7] and electronic communications.[8]

Although the definition of "intercept" is not expressly limited to the acquisition of communication contents *during transmission*, that was the practical meaning of the term when it was first used in the original wiretap law. At that time, telephone calls and oral conversations were necessarily intercepted while they were occurring, because such communications were not routinely recorded and stored for later access.

Modern electronic communications are different. They are routinely stored and the stored copies can be accessed long after the process of transmission has been completed. Access to such "stored" communications is not considered to be an interception for the purposes of The Wiretap Act. Instead, it is regulated under the SCA, which is discussed further below.

---

5. 18 U.S.C. § 2510(4) ("'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.")

6. 18 U.S.C. § 2510(1) ("'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce").

7. 18 U.S.C. § 2510(2) ("'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication").

8. 18 U.S.C. § 2510(12) ("'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include — (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds").

However, it is possible to "intercept" an electronic communication in transmission, and such interceptions are governed by the Wiretap Act. The fact that the process of sending an electronic communication necessarily creates a stored copy of the communication does not bar application of the Wiretap Act:

> The term "electronic communication" includes transient electronic storage intrinsic to the transmission of such communications. Thus, an e-mail message continued to be an electronic communication during momentary intervals, intrinsic to the communication process, when the message is in transient electronic storage. Interception of electronic communication occurs with reading of transmissions as they are sent….[9]

Prohibitions

It is generally unlawful to intentionally intercept a wire, oral, or electronic communication.[10] It is also generally unlawful to disclose or use the contents[11] of a communication that are known to have been obtained through an unlawful interception or that is disclosed in order to obstruct a criminal investigation.[12] Finally, electronic communication service providers are generally prohibited from divulging the contents of communications, while they are in transmission, to anyone other than the sender or intended recipient.[13]

It is also unlawful to manufacture, sell, advertise, or deliver devices designed for surreptitious interception of wire, oral, or electronic communications.[14]

Those general prohibitions are subject to a number of exceptions. The most germane for the purposes of this study is the exception for interception by law enforcement pursuant to lawful process. The law enforcement exception is discussed in detail below.

For the sake of completeness, it is worth briefly noting the other statutory exceptions:

- It is not unlawful for communication service provider personnel to intercept, disclose, or use communications in the ordinary course of business.[15] Nor is it unlawful for service providers to provide

9. J. Carr & P. Bellia, *The Law of Electronic Surveillance*, 3:7 (Feb. 2014) (footnotes omitted) (hereafter "*Electronic Surveillance*").
10. 18 U.S.C. § 2511(1)(a)-(b).
11. In Chapter 119, "contents" is a defined term. See 18 U.S.C. § 2510(8) ("'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication…").
12. 18 U.S.C. § 2511(1)(c)-(e).
13. *Id.* at (3)(a).
14. 18 U.S.C. § 2512(1).
15. *Id.* at (2)(a)(i).

information, facilities, or technical assistance to persons who are properly authorized to intercept communications.[16]

- It is not unlawful for Federal Communications Commission personnel to intercept, disclose, or use communications in the normal course of their duties.[17]
- It is not unlawful for a person to intercept a communication, if that person is a party to the communication or one of the parties to the communication has given prior consent to the interception (provided that the interception is not for the purpose of committing a crime or a tort).[18]
- It is not unlawful for a federal employee to collect foreign intelligence pursuant to other specified law.[19]
- It is not unlawful to intercept or use communications that are configured so as to be readily accessible to the general public.[20]
- Use of a pen register or trap and trace device is not unlawful under the Wiretap Act.[21] Such devices are regulated under The Pen Register Act, discussed further below.
- It is not unlawful to record the fact that a wire or electronic communication occurred, in order to protect against fraud or abuse.[22]
- It is not unlawful to intercept a wire or electronic communication of a computer trespasser, as part of a lawful investigation.[23]
- It is not unlawful for an electronic communication service provider to divulge the contents of a communication to the personnel of another provider, as part of the process of transmission.[24]
- It is not unlawful for an electronic communication service provider to divulge the contents of a communication to law enforcement, if the contents were "inadvertently obtained" and appear to "pertain to the commission of a crime."[25]

Law Enforcement Interception and Use of Wire, Oral, and Electronic Communications

Section 2516 of Title 18 authorizes law enforcement personnel to intercept certain communications under specified circumstances. Section 2517 then specifies how information obtained through such an interception can be used.

16. *Id.* at (2)(a)(ii).
17. *Id.* at (2)(b).
18. *Id.* at (2)(c)-(d), (3)(b)(ii).
19. *Id.* at (2)(e)-(f).
20. *Id.* at (2)(g).
21. *Id.* at (2)(h)(i).
22. *Id.* at (2)(h)(ii).
23. *Id.* at (2)(i).
24. *Id.* at (3)(b)(iii).
25. *Id.* at (3)(b)(iv).

Section 2518 provides the procedure to be used in applying for authority to intercept communications under Section 2516. The details of those sections are summarized below.

Authority to Apply for Court Order

Section 2516(1) authorizes specified personnel of the federal Attorney General's office to make an application to a judge for an order authorizing an interception of a wire or oral communication. Such authority can only be requested if the interception "may provide or has provided evidence" of one of a lengthy list of serious federal criminal offenses.

Notably, the rules for interception of an electronic communication are less strict. Section 2516(3) authorizes any federal attorney to apply for authority to intercept an electronic communication in connection with the investigation of *any* federal felony.

Section 2516(2) addresses action by the states. It authorizes the principal prosecuting attorney of any state or of any political subdivision of a state, to apply for authority to intercept a wire, oral, or electronic communication. Application is made to a state judge of competent jurisdiction. Any authority granted by the judge must be in conformity with Section 2518 "and with the applicable State statute." The authority may only be requested if it may provide or has provided evidence of the commission of the following offenses:

> murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or any crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable state statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

Application for Court Order

An application for a court order to intercept a wire, oral, or electronic communication must be made in writing, upon oath or affirmation to a judge of competent jurisdiction.[26] It must include all of the following information:

- A statement of the applicant's authority to make the application.[27]
- The identity of the applicant.[28]

26. 18 U.S.C. § 2518(1).
27. *Id.*
28. *Id.* at (1)(a).

- A full and complete statement of the justifying facts and circumstances, including the crime being investigated, the facilities where the communication will be intercepted, the type of communication to be intercepted, and the identity of the person whose communication will be intercepted (if known).[29] There are exceptions to the requirement that a specific facility be identified, involving impracticability or the probability that the target of the application could thwart interception from a specified facility.[30]
- A statement of whether other investigative procedures have been tried and failed, are unlikely to succeed if tried, or would be too dangerous.[31]
- The period of time during which communications would be intercepted. If requesting that the authorization not automatically terminate after interception of a described communication, the application must also include a statement of probable cause to believe that additional communications of the same type will continue to occur.[32]
- A statement of facts concerning all previous applications involving any of the same persons, facilities, or places specified in the new application, and the action taken by the judge on those prior applications.[33]
- If the application is for an extension of a prior order, a statement of the results obtained thus far or a reasonable explanation for the failure to obtain results.[34]

The judge may require additional testimony or documentary evidence in support of an application.[35]

Legal Standard for Granting Authority to Intercept Communication

A judge may enter an ex parte order, as requested or modified, authorizing an interception of a wire, oral, or electronic communication, if the judge finds all of the following to be true, based on the facts submitted by the applicant:

> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;
>
> (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

29. *Id.* at (1)(b).
30. *Id.* at (11)-(12).
31. *Id.* at (1)(c).
32. *Id.* at (1)(d).
33. *Id.* at (1)(e).
34. *Id.* at (1)(f).
35. *Id.* at (2).

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.[36]

The requirements set out above exceed the general "probable cause" requirement for the issuance of a search warrant under Federal Rule of Criminal Procedure 41. In particular, subsection (c) requires the government to demonstrate that other alternative methods of obtaining evidence were unsuccessful or would be unlikely to succeed or too dangerous. Because the interception warrant requires more than a general federal search warrant, it is sometimes referred to as a "super-warrant."

Content of Order Granting Authority to Intercept Communication

An order granting authority to intercept a wire, oral, or electronic communication is required to state the identity of the person whose communications will be intercepted (if known), the communication facilities to be used, the type of communication to be intercepted and the criminal offense to which it relates, the identity of the intercepting agency and the person who authorized the application, and the period of time during which interception is authorized (including a statement on whether authority will automatically terminate when the first described communication is intercepted).[37]

The order must also require cooperation from the affected communication service provider, which is entitled to compensation of its reasonable expenses.[38] The order can also direct a provider to comply with the requirements of the Communications Assistance for Law Enforcement Act (discussed later in this memorandum).[39]

Duration and Extension

As a general rule, authorization to intercept a wire, oral, or electronic communication does not continue "longer than is necessary to achieve the

36. *Id.* at (3).
37. *Id.* at (4).
38. *Id.*
39. *Id.*

objective of the authorization, nor in any event longer than thirty days."[40] On application, the court can extend the authorization for one or more additional periods of the same duration.[41]

Minimization

An authorized interception "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception" under the Wiretap Act.[42] The "cases interpreting this minimization provision are not entirely clear, nor consistent."[43] In general, courts have held that law enforcement must stop monitoring a communication that is not relevant to the investigation, after a reasonable opportunity to evaluate its pertinence.[44]

Reporting

An order authorizing interception of a wire, oral, or electronic communication may require that the intercepting agency provide the judge with reports showing what progress has been made toward the objective of the interception and the need for continuing interception.[45]

Emergency Exception

In certain circumstances, law enforcement may intercept a wire, oral, or electronic communication without first obtaining an authorizing court order. This may be done if (1) law enforcement determines that there is an emergency that requires the interception to occur before an order could be obtained with due diligence, (2) there are grounds upon which an authorizing order could be entered, and (3) an application for an authorizing order is made within 48 hours after the interception begins.[46]

For this purpose, the requisite emergency situation must involve one or more of the following:

- Immediate danger of death or serious physical injury to any person.
- Conspiratorial activities threatening the national security interest.

40. *Id.* at (5).
41. *Id.*
42. *Id.*
43. *Electronic Surveillance, supra* note 9, at 5:15 (footnote omitted).
44. *Id.* at 5:15-21.
45. *Id.* at (6).
46. *Id.* at (7).

- Conspiratorial activities characteristic of organized crime.[47]

An interception conducted pursuant to this emergency exception must end immediately when the communication being sought has been obtained or the court denies the requested order, whichever comes first.[48]

If the court denies the application for authority, or the application is never made, the interception is treated as a violation of the chapter.[49]

Recording

The contents of intercepted communications are required to be recorded (if possible), in a form that will prevent alteration. On expiration of the period of authorization, the recordings must be made available to the judge. They are held by the court, under seal. Duplicates may be made for use by law enforcement.[50]

Inventory and Notice

Within a reasonable time (not to exceed 90 days) after an authorizing order and any extension of the order has terminated, or after a judge has denied an application for authority under the emergency exception described above, an "inventory" shall be served on the persons named in the order and on any other party to an intercepted communication as the judge orders, in the interests of justice.[51]

The inventory document must provide notice of the interception, including the date and period of interception, and whether any communications were actually intercepted. The judge may also order, in the interests of justice, that portions of the intercepted communications be provided.[52]

On an ex parte showing of good cause, a judge may postpone service of the inventory.[53]

Appeal of Denial

If the judge denies an application for an order authorizing interception, the United States has an express right to appeal that decision.[54]

---

47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.* at (8)(a).
51. *Id.* at (8)(d).
52. *Id.*
53. *Id.*
54. 18 U.S.C. § 2518(10)(b). The appeal provision makes no mention of a right of appeal by state law enforcement.

Use of Lawfully Intercepted Communications

An investigative or law enforcement officer who lawfully obtains the contents of an interception of a wire, oral, or electronic communication can disclose those contents to another investigative or law enforcement officer to the extent appropriate to the proper performance of official duties.[55] Such contents can also be used by the investigative or law enforcement officer in the proper performance of official duties.[56] The same is true even if the officer intercepts communications relating to offenses other than those specified in the order authorizing interception.[57]

Any person who lawfully received the contents of an intercepted communication or evidence derived from the interception may disclose the contents or derivative evidence while giving testimony under oath or affirmation in any proceeding under the authority of the federal government, a state, or a political subdivision of a state.[58] However, if an officer intercepts communications relating to offenses other than those specified in the order authorizing interception, the contents of the interception and derivative evidence can only be introduced into evidence in a proceeding if a judge determines, on subsequent application, that the contents were otherwise intercepted in accordance with the Wiretap Act.[59]

There are also provisions authorizing use of lawfully intercepted communication contents in foreign intelligence, counter-intelligence, and foreign intelligence sharing, and to counter a grave threat from foreign powers, saboteurs, terrorists, or foreign intelligence agents.[60]

Limitations on Use of Intercepted Communications

The contents of a lawfully intercepted communication cannot be introduced into evidence in a proceeding unless all parties receive a copy of the application, as well as the order authorizing the interception, at least 10 days before the proceeding.[61] The judge may waive the 10-day period if it was not possible to provide notice to a party in that time period and the party was not prejudiced.[62]

55. 18 U.S.C. § 2517(1).
56. *Id.* at (2).
57. *Id.* at (5).
58. *Id.* at (3).
59. *Id.* at (5).
60. *Id.* at (6)-(8).
61. 18 U.S.C. § 2518(9).
62. *Id.*

Also, a privileged communication does not lose its privileged status as a consequence of being lawfully intercepted.[63] For example, a confidential attorney-client communication remains protected by the attorney-client privilege even if it is disclosed to law enforcement personnel through interception.

Remedies for Violations

As discussed, the Wiretap Act generally prohibits the interception, disclosure, and use of intercepted contents, subject to a number of specific exceptions. This part of the memorandum discusses the remedies available for a violation of the requirements and prohibitions of the Wiretap Act.

The remedies and sanctions provided in the Wiretap Act are the exclusive remedies for a violation of the chapter. However, this does not limit the remedies that might be available if a statutory violation also violates the Constitution.[64]

Injunction

The United States Attorney General may bring an action to enjoin a felony violation of the Wiretap Act.[65]

Suppression and Admissibility of Evidence

Before any "trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof," an "aggrieved person"[66] may move to suppress the contents of an interception or evidence derived from those contents. The aggrieved person may base the suppression motion on any of the following grounds:

> (i) the communication was unlawfully intercepted;
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
> (iii) the interception was not made in conformity with the order of authorization or approval.[67]

The statute does not expressly provide for suppression as a remedy for a *post*-interception violation (e.g., the failure to provide recordings of intercepted

63. 18 U.S.C. § 2517(4).
64. 18 U.S.C. § 2518(10)(c).
65. 18 U.S.C. § 2521.
66. 18 U.S.C. § 2510(11) ("'aggrieved person' means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed…").
67. 18 U.S.C. § 2518(10)(a).

communications to the court for custody under seal). But many courts have suppressed evidence for such a violation and found a way to justify that result.[68]

Upon the filing of a suppression motion, the judge has discretion to allow the aggrieved person to inspect portions of the intercepted communication.[69]

If the motion is granted, the contents of the intercepted communication and derivative evidence are treated as having been obtained in violation of the Wiretap Act.[70] The United States is authorized to appeal a decision granting a suppression motion.[71]

A pre-trial motion to suppress evidence is not the only means to exclude unlawfully intercepted data and derivative evidence. In addition, such evidence may be inadmissible under a provision that bars the admission of intercepted communication contents and derivative evidence where "disclosure of that information would be in violation of this chapter."[72]

Civil Action Generally

In general, a person whose communication is intercepted, disclosed, or intentionally used in violation of the Wiretap Act, *by a person other than the United States*, may bring a civil action seeking any of the following types of relief:

> (1) such preliminary and other equitable or declaratory relief as may be appropriate;
> (2) damages … and punitive damages in appropriate cases; and
> (3) a reasonable attorney's fee and other litigation costs reasonably incurred.[73]

There is a two year limitations period for such civil actions.[74]

In general, recoverable damages are the greater of (1) the actual damages of the plaintiff plus any profits made by the violator as a result of the violation, or (2) $100 per day of violation, or (3) $10,000.[75]

There is a much more lenient damage calculation formula for certain offenses involving the unauthorized interception of unscrambled and unencrypted

68. *Electronic Surveillance, supra* note 9, at 6:36.
69. *Id.*
70. *Id.*
71. 18 U.S.C. § 2518(10)(b). The appeal provision makes no mention of a right of appeal by state law enforcement.
72. 18 U.S.C. § 2515.
73. 18 U.S.C. § 2520(a)-(b).
74. *Id.* at (e).
75. *Id.* at (c)(1).

satellite and radio communications.[76] A person who commits such an offense is also subject to a civil enforcement suit by the federal government. In such a suit, the government may seek an injunction or the imposition of a $500 civil fine.[77]

Civil Action Against United States

Any person who is aggrieved by a willful violation of the Wiretap Act by the United States may bring a civil against the United States for money damages.[78] Damages are assessed to be the greater of $10,000 or actual damages, plus litigation costs.[79] Special procedures for such an action are specified in the statute.[80]

Administrative Discipline

An officer of the United States who willfully or intentionally violates the chapter may be subject to administrative discipline.[81]

Criminal Penalty

A person who violates the general prohibitions in the Wiretap Act may be punished by a fine, imprisoned for not more than five years, or both.[82]

However, certain offenses relating to the interception of unscrambled and unencrypted satellite communications can only be punished criminally if they were for financial gain.[83]

Defenses

A person has a complete defense to civil and criminal liability under the Wiretap Act if the person acted in good faith reliance on any of the following:

> (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
> (2) a request of an investigative or law enforcement officer under [the emergency exception discussed above]; or
> (3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;[84]

76. *Id.* at (c)(2).
77. 18 U.S.C. § 2511(5).
78. 18 U.S.C. § 2712(a).
79. *Id.*
80. *Id.* at (b), (e).
81. 18 U.S.C. § 2520(f). See also 18 U.S.C. § 2712(c).
82. 18 U.S.C. § 2511(4)(a).
83. *Id.* at (4)(b).
84. 18 U.S.C. § 2520(d).

The provisions referenced in (3) appear to encompass all of the numerous specific exceptions to chapter's general prohibitions, which were summarized earlier in this memorandum.

Contempt

A violation of certain procedures governing law enforcement interception pursuant to court authorization is punishable as contempt.[85] Those requirements include the obligation to record intercepted communications and provide the recordings to the judge for retention under seal,[86] and the requirement that an inventory be served on the subject of an interception within a specified period after the interception order terminates.[87]

Confiscation of Devices

Devices that are used, sent, carried, manufactured, assembled, possessed, sold or advertised in violation of the relevant provisions of the Wiretap Act can be seized and forfeited to the United States.[88]

Statistical Reporting

The federal courts and the office of the United States Attorney General are required to prepare annual reports compiling specified statistics about the interception of wire, oral, and electronic communications under the Wiretap Act.[89]

Communications Assistance for Law Enforcement Act

The Communications Assistance for Law Enforcement Act ("CALEA")[90] generally requires that "telecommunications carriers" design and maintain their equipment so as to enable law enforcement officials to conduct lawful electronic surveillance. The Wiretap Act contains a small number of provisions relating to the enforcement of CALEA.[91]

85. 18 U.S.C. § 2518(8)(c).
86. *Id.* at (8)(a)-(b).
87. *Id.* at (8)(d).
88. 18 U.S.C. § 2513.
89. 18 U.S.C. § 2519.
90. 50 U.S.C. § 1801 *et seq.*
91. 18 U.S.C. § 2522.

The SCA governs the disclosure of the contents of stored electronic communications and metadata about the customers of communication providers. Chapter 121 is often referred to as the "Stored Communications Act."

The statute extends different levels of protection to different types of data. The terminology used to establish those distinctions is discussed below.

Terminology

Key terminological points include (1) the distinction between an electronic communication service ("ECS") and a remote computing service ("RCS") and (2) the distinction between a "public" RCS and a nonpublic RCS.

ECS v. RCS

The Stored Communications Act draws a distinction between two types of electronic data services: an electronic communication service ("ECS") and a remote computing service ("RCS").

The term "electronic communication service" has the same meaning as in the Wiretap Act:

> "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications ….[92]

The term "electronic communication" is also drawn from the Wiretap Act:

> "[E]lectronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds ….[93]

92. 18 U.S.C. § 2510(14). See also 18 U.S.C. § 2711(1) (expressly making definitions in Section 2510 applicable to Chapter 121).

93. 18 U.S.C. § 2510(12). See also 18 U.S.C. § 2711(1) (expressly making definitions in Section 2510 applicable to Chapter 121).

For purposes of the Stored Communications Act, the term "remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system …."[94]

Very generally, then, an ECS is a system used to send and receive communications on behalf of a customer (e.g., an email service), while an RCS is a system used to store and/or process customer data. An online cloud storage service would seem to be a clear example of an RCS used for storage.

Importantly, RCS is limited to services that are provided to the "public," and it includes not only computer storage services, but also "processing services." Professor Orin Kerr suggests that "processing services" were included in the definition of RCS because some businesses used to outsource their data-processing tasks, before widespread availability of powerful desktop computers and software.[95]

One potential difficulty with the ECS-RCS dichotomy is that the delivery and receipt of electronic communications also involves the creation and storage of copies. To partially resolve that difficulty, the Stored Communications Act provides that ECS can include a copy of a message that is in "electronic storage."[96] That term is defined narrowly:

> (17) "electronic storage" means—
> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication ….

Consequently, a stored communication that does not fall within the above definition of "electronic storage" would instead be deemed in the "computer storage" provided by an RCS.

Applying those concepts, some courts have held that an email message remains in "electronic storage" (i.e., within ECS status) only until it has been opened. Once the message has been opened, any further storage is no longer

94. 18 U.S.C. § 2711(2).
95. Kerr, *A User's Guide to the Stored Communications Act — and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1, 7 (2004).
96. See, e.g., 18 U.S.C. § 2702(a) (prohibiting ECS disclosure of message content "while in electronic storage by that service").

"temporary" or "incidental to … transmission." At that point, any further storage of the opened message is the sort of storage provided by an RCS.[97]

However, there is a split of authority on that issue. In *Theofel v. Farey-Jones*, the court held that a copy of an opened email had been retained by the ISP as a "backup." Consequently, the message was in "electronic storage" under the backup clause in the governing definition. Thus, access to the opened email was governed by the provisions that apply to an ECS service.[98]

A 2013 bill, SB 467 (Leno), would have largely erased the ECS-RCS distinction in California, requiring a warrant for law enforcement access to both types of data. The Legislature approved the bill on a nearly unanimous basis, but it was vetoed by Governor Brown.

Service to the "Public"

It is important to note that the definition of "remote computing service" is limited to an entity that provides service to the "public." This includes any company that offers services to the public generally (e.g., Gmail).

It does not include an entity that provides service solely on the basis of some special relationship between the entity and the users of the service. For example, a company that provides email service to its employees as an incident of employment would not be providing service to the "public" and so would not be an RCS with regard to its employees.[99] This makes some sense given the special status of an employer with regard to employer-provided resources.

More problematically, some people contend that when a university provides Internet accounts to its students, it is not providing an RCS. This is because the university is providing the services pursuant to a special relationship, rather than to the public generally. If that is correct, the law denies RCS protections to university student accounts.[100] (The law would still apply to a university account, to the extent that it is being used to send or receive email or provide other ECS services.)

Prohibitions

The following conduct is generally unlawful:

---

97. Office of Legal Education, Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 120 (2009) (and cases cited therein).
98. 359 F.3d 1066, 1075-77 (9th Cir. 2004).
99. *Office of Legal Education*, *supra* note 97, at 119-20.
100. Kerr, *supra* note 95, at 22.

- For any person to intentionally access an ECS facility, without authorization or in excess of authorization, to obtain, alter, or prevent authorized access to a wire or electronic communication that is in electronic storage.[101]
- For an ECS provider to knowingly divulge, to any person or entity, the contents of a communication that is in electronic storage with the ECS.[102]
- For an RCS provider to knowingly divulge, to any person or entity, the contents of any communication that is "carried or maintained" on the RCS on behalf of a customer or subscriber.[103]
- For an ECS or RCS provider to knowingly divulge, to any person or entity, a record or other information pertaining to a customer or subscriber of the RCS.[104]

Furthermore, any willful disclosure of a record lawfully obtained by law enforcement pursuant to the Stored Communications Act is deemed to be a violation of the Act, unless (1) the disclosure was made in the proper performance of official functions or (2) the disclosed information had previously been lawfully disclosed by the government or by the plaintiff in a civil action relating to the disclosure.[105]

There are numerous exceptions to the general prohibitions in the bulleted list above. The most relevant for the purposes of this study are the exceptions relating to government access.

Before turning to the government access exceptions, it is worth briefly noting the other miscellaneous statutory exceptions.

It is not unlawful for a person to *access an electronic communication facility* without authority or in excess of lawful authority in the following circumstances:

- The access was authorized by the communication service provider.[106]
- The access was by a user, to the user's own communications.[107]
- The access was authorized in connection with specified provisions authorizing the disclosure or interception of communication content.[108]

101. 18 U.S.C. § 2701(a).
102. 18 U.S.C. § 2702(a)(1).
103. *Id.* at (a)(2).
104. *Id.* at (a)(3).
105. 18 U.S.C. § 2707(g).
106. 18 U.S.C. § 2701(c)(1).
107. *Id.* at (c)(2).
108. *Id.* at (c)(3).

It is not unlawful for a provider to divulge the *contents* of an ECS or RCS communication in the following circumstances:

- To the addressee or intended recipient of the communication.[109]
- Pursuant to a court order authorizing interception of communications under the Wiretap Act.[110]
- Pursuant to specified exceptions governing interception of communications under the Wiretap Act.[111]
- With the lawful consent of the originator or recipient.[112]
- To a person involved in forwarding the communication to its destination.[113]
- As an incident of service or as necessary to protect the rights or property of the provider.[114]
- To the National Center for Missing and Exploited Children, in connection with a specified report.[115]
- To law enforcement, if the contents were inadvertently obtained and appear to pertain to the commission of a crime.[116]
- To government, in the good faith belief that an emergency involving danger of death or serious injury requires disclosure without delay.[117]

Nor is it unlawful for a provider to divulge *customer information* (not including the contents of a communication) in the following circumstances:

- With the lawful consent of the subscriber or customer.[118]
- As an incident of service or as necessary to protect the rights or property of the provider.[119]
- To the National Center for Missing and Exploited Children, in connection with a specified report.[120]
- To government, in the good faith belief that an emergency involving danger of death or serious injury requires disclosure without delay.[121]

109. 18 U.S.C. § 2702(b)(1).
110. *Id.* at (b)(2).
111. *Id.*
112. *Id.* at (b)(3).
113. *Id.* at (b)(4).
114. *Id.* at (b)(5).
115. *Id.* at (b)(6).
116. *Id.* at (b)(7).
117. *Id.* at (b)(8).
118. *Id.* at (c)(2).
119. *Id.* at (c)(3).
120. *Id.* at (c)(5).
121. *Id.* at (c)(4).

- To any person other than a governmental entity.[122]

Note that the last exception removes any restriction on the disclosure of customer non-content data to private parties.

Government Access Exceptions

There are also a number of exceptions for government access to stored data. In each of these exceptions, a provider is *compelled* to provide information of a specified type when a government entity presents the specified type of authorization. The charts below shows the relevant requirements for ECS, RCS, and noncontent customer data for both ECS and RCS. Where a chart shows more than one form of authorization, any of the listed forms is sufficient.

Content of ECS Communication	Form of Authorization
In Electronic Storage 180 Days or Fewer	• Search warrant[123]
In Electronic Storage More Than 180 Days, Without Prior Notice to Customer	• Search warrant[124]
In Electronic Storage More Than 180 Days, With Prior Notice to Customer	• Administrative subpoena • Grand jury or trial subpoena • Court order per § 2703(d)[125]

Content of RCS Data	Form of Authorization
Without Prior Notice to Customer	• Search warrant[126]
With Prior Notice to Customer	• Administrative subpoena • Grand jury or trial subpoena • Court order per § 2703(d)[127]

122. *Id.* at (c)(6).
123. 18 U.S.C. § 2703(a).
124. *Id.* at (a) & (b)(1)(A).
125. *Id.* at (a) & (b)(1)(B)
126. *Id.* at (b)(1)(A).
127. *Id.* at (b)(1)(B).

Non-Content Customer Information	Form of Authorization
Generally	• Search warrant • Court order per § 2703(d), • Consent of the customer • Telemarketing fraud request[128]
Specified Subset	• Search warrant • Court order per § 2703(d) • Consent of the customer, • Telemarketing fraud request • Administrative subpoena[129]

Some details of the requirements summarized above are discussed further below.

Warrant

Where the Stored Communications Act requires a warrant, it specifies a "warrant issued under the Federal Rules of Criminal Procedure" or "an equivalent State warrant."[130] While such a warrant must be grounded on probable cause, it is not subject to all of the requirements that govern a "super-warrant" for interception of communications under the Wiretap Act (as discussed earlier).

Administrative Subpoena

In some cases, the Stored Communications Act permits the use of an administrative subpoena to compel the disclosure of stored electronic communications. Such a subpoena must be authorized by a federal or state statute.[131] According to a 2005 Department of Justice report, there were approximately 335 statutes that authorize federal agencies to use administrative subpoenas.[132]

An administrative subpoena allows "executive branch agencies to issue a compulsory request for documents or testimony without prior approval from a grand jury, court, or other judicial entity."[133] While an administrative subpoena

128. *Id.* at (c)(1).
129. *Id.* at (c)(2).
130. See, e.g., 18 U.S.C. § 2703(a). See also Fed. R. Crim. P. 41.
131. See, e.g., 18 U.S.C. § 2703(b)(B)(i).
132. Office of Legal Policy, United States Department of Justice, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities* 5 (2002).
133. *Id.* at 6.

does not require prior judicial approval, its validity can be contested in court. In reviewing an administrative subpoena, the court does not require a showing of probable cause. Instead, a different standard applies:

> In *United States v. Powell*, [379 U.S. 48, 58 (1964)] the Court articulated the deferential standard for judicial review of administrative enforcement actions in a four-factor evaluation of "good faith" issuance, requiring that: (1) the investigation is conducted pursuant to a legitimate purpose, (2) the information requested under the subpoena is relevant to that purpose, (3) the agency does not already have the information it is seeking with the subpoena, and (4) the agency has followed the necessary administrative steps in issuing the subpoena. … The federal courts have construed the *Powell* factors broadly, allowing greater flexibility for government action.[134]

The use of an administrative subpoena to compel the production of documents has been held to be consistent with the requirements of the Fourth Amendment to the United States Constitution.[135] In large part, this is because the recipient of an administrative subpoena has an opportunity to challenge the subpoena in court before complying:

> While the Fourth Amendment protects people "against unreasonable searches and seizures," it imposes a probable cause requirement only on the issuance of warrants. Thus, unless subpoenas are warrants, they are limited by the general reasonableness standard of the Fourth Amendment (protecting the people against "unreasonable searches and seizures"), not by the probable cause requirement.
>
> A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things. To preserve advantages of speed and surprise, the order is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion. Because this intrusion is both an immediate and substantial invasion of privacy, a warrant may be issued only by a judicial officer upon a demonstration of probable cause -- the safeguard required by the Fourth Amendment.
>
> A subpoena, on the other hand, commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.

134. *Id.* at 11 (footnotes omited).
135. See Donovan v. Lone Steer, 464 U.S. 408 (1984).

> In short, the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues, whereas the issuance of a subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded. And while a challenge to a warrant questions the actual search or seizure under the probable cause standard, a challenge to a subpoena is conducted through the adversarial process, questioning the reasonableness of the subpoena's command.[136]

That explanation makes sense if the person who is served with the subpoena is also the person whose privacy is to be invaded. In such a case, the notice and opportunity to be heard before producing the subpoenaed records provides the adversarial protection described above.

It is not clear that this would be true if a subpoena is served on a service provider and demands the production of *customer* records. In that case, the immediate notice and opportunity to challenge is given to the provider, who does not have the same privacy issues at stake as a customer. Unless the customer also receive notice and a chance to challenge the subpoena, the argument for Fourth Amendment reasonable seems less convincing.

As noted in the preceding chart, an administrative subpoena can only be used to compel the disclosure of the content of customer records if prior notice is given to the customer. That would seem to address the concern discussed above, by insuring that the customer has an opportunity for judicial review before private information is disclosed. However, the "prior" notice to customers can be delayed by 90 days or more with court approval, which is authorized where prior notice would jeopardize an investigation in specified ways (see the discussion of "Delayed Notice" below).[137] In such cases, the customer does not have an opportunity to challenge the subpoena before it operates.

Recall, however, that the Fourth Amendment generally does not apply to information voluntarily provided to a third party.[138] The scenario described above necessarily involves records held by a third party (the service provider) on behalf of the customer. This may explain why Congress was willing to permit the use of an administrative subpoena in a situation where the person whose records are to be disclosed may not have notice of the subpoena before it operates.

---

136. *In re* Subpoena Duces Tecum, 228 F.3d 341, 347-48 (4th. Cir. 2000) (citations omitted).
137. 18 U.S.C. §§ 2703(b), 2705.
138. See Memorandum 2014-13, pp. 10-14.

But there is no third party exception to the search and seizure provision of the California Constitution.[139] This suggests that use of subpoenas without prior notice to the target of the subpoena could be problematic in California.

Grand Jury or Trial Subpoena

In some cases the Stored Communications Act permits the use of a federal or state grand jury or trial subpoena to compel the disclosure of stored electronic communications.

The United States Supreme Court has held that the Fourth Amendment does not bar the use of a subpoena to demand the production of records (i.e., a subpoena *duces tecum*).

> We think it quite clear that the search and seizure clause of the Fourth Amendment was not intended to interfere with the power of courts to compel, through a subpoena *duces tecum*, the production, upon a trial in court, of documentary evidence.[140]

That said, a particular subpoena could violate the Fourth Amendment if it were so broadly or indiscriminately framed as to be *unreasonable*.[141]

Under governing federal and California law, a person who is served with a subpoena *duces tecum* issued by a grand jury or a trial court can move to quash or modify the subpoena on the grounds that it is unreasonable.[142] This provides the same sort of pre-disclosure judicial review that has been cited in explaining why the use of an administrative subpoena does not offend the Fourth Amendment.

Court Order Under Section 2703(d)

As shown in the preceding chart, the Stored Communications Act sometimes authorizes the use of a court order issued under Section 2703(d) to compel the production of stored electronic records. To obtain such an order, the government must offer "specific and articulable facts showing that there are reasonable

139. *Id.* at 14-17.
140. Hale v. Henkel, 201 U.S. 43, 73 (1906).
141. *Id.* at 76-77.
142. See Fed. R. Crim. Proc. 17(c)(2) (court may quash or modify federal subpoena if compliance would be unreasonable or oppressive); City of Woodlake v. Tulare County Grand Jury, 197 Cal. App. 4th 1293, 1297-98 (2011) (California grand jury subpoena subject to motion to quash); Pacific Lighting Leasing Co. v. Superior Court, 60 Cal. App. 3d 552, 568 (1976) (California criminal trial subpoena subject to motion to quash and *in camera* judicial review to determine reasonableness). The rules governing civil trials are not cited here, because courts have held that the SCA rules on the use of trial subpoenas apply only to criminal trials. See, e.g., *In re* Subpoena Duces Tecum to AOL, Inc. 550 F. Supp. 2d 606, 611 (E.D. Va. 2008) ("The Court finds State Farm's argument unpersuasive because § 2703 pertains exclusively to criminal investigations, not civil discovery matters such as this.")

grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[143] State law is expressly permitted to preclude the issuance of such an order in a state court.[144] The service provider may move to quash or modify the order on the grounds that the request is "unusually voluminous" or would otherwise impose an "undue burden on the provider."

As with the subpoenas discussed above, an order pursuant to Section 2703(d) can only be issued with "prior" notice to the customer of the communication service provider. Again, however, such notice can be delayed by 90 days or more on order of the court, if prior notice would lead to specified "adverse results" (see the discussion of "Delayed Notice" below). Thus, such orders can be issued without *actual* prior notice to the customer. For that reason, it is not clear that an order under Section 2703(d) would provide a customer with any meaningful opportunity to challenge the order before private information is disclosed.

Delayed Notice

Although some of the procedures in the Stored Communications Act are contingent on giving prior notice to the affected customer, the Act also expressly provides for such notice to be delayed by up to 90 days if prior notification would produce any of the following "adverse results:"

> (A) endangering the life or physical safety of an individual;
> (B) flight from prosecution;
> (C) destruction of or tampering with evidence;
> (D) intimidation of potential witnesses; or
> (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.[145]

The 90-day delay can be extended, by additional 90-day periods, on application to the court.[146]

In addition, the government may obtain a court order commanding a service provider not to notify its customer of a warrant, court order, or subpoena issued under the SCA.

143. 18 U.S.C. § 2703(d).
144. *Id.*
145. 18 U.S.C. § 2705(a)(2).
146. *Id.* at (a)(4).

Specified Subset of Customer Information

The Stored Communication has general rules governing the compelled disclosure of non-content information about a customer of an ECS or RCS. In addition, there is a special rule for the following specified subset of customer information:

> (A) name;
> (B) address;
> (C) local and long distance telephone connection records, or records of session times and durations;
> (D) length of service (including start date) and types of service utilized;
> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
> (F) means and source of payment for such service (including any credit card or bank account number)…[147]

Counter-Intelligence Access

In addition to the general rules on governmental access to stored electronic communications, there are also provisions that specifically provide for counterintelligence access by federal officials.[148] The current study does not encompass access to information by federal officials, so the counter-intelligence provisions are not discussed further in this memorandum.

Preservation of Evidence

The Stored Communications Act provides two ways in which the government can require a communication service provider to secure evidence against destruction by a customer, while the government obtains the necessary authorization for access.

First, the government can simply "request" that an ECS or RCS provider "preserve records and other evidence in its possession pending the issuance of a court order or other process."[149] The provider is obliged to do so, for a period of 90 days (subject to extension for another 90-day period on the request of the government).[150]

Second, if the government is using an administrative subpoena or court order to request access to ECS data that is in electronic storage for more than 180 days

147. 18 U.S.C. § 2703(c)(2).
148. 18 U.S.C. § 2709.
149. 18 U.S.C. § 2703(f)(1).
150. *Id.* at (f)(2).

or RCS data, it may include in the authorizing instrument a requirement that the service provider create a backup copy of the requested data.[151] Ordinarily, the customer is given notice of the creation of the backup within three days *after* the backup copy is created.[152] However, that notice can be delayed if notice would lead to the sort of "adverse results" previously described in the discussion of "Delayed Notice."[153]

A customer who receives notice of the creation of a backup may move to quash or vacate the underlying subpoena or order.[154]

Cost Reimbursement

In general, the government is required to reimburse a service provider for reasonably necessary costs incurred in "searching for, assembling, reproducing, or otherwise providing" customer information that the provider is compelled to provide.[155]

Remedies for Violations

The remedies provided in the Stored Communications Act are the exclusive remedies for a violation of the Act.[156] Notably, the Stored Communications Act does *not* provide for suppression of evidence derived from a violation of the Act (suppression may be available if a violation of the Act is also a violation of the Fourth Amendment).

Criminal Penalty

A person who intentionally accesses a communication facility without sufficient authorization and obtains, alters, or prevents authorized access to a wire or electronic communication may be fined, imprisoned, or both.[157] The maximum term of imprisonment can vary between one and 10 years, depending on the circumstances.[158]

151. 18 U.S.C. § 2704(a)(1). See also *id.* at (a)(3) (retention of backup), (4) (release of backup), (5) (authority to order backup creation to avoid destruction of evidence).
152. *Id.* at (a)(2).
153. *Id.*
154. *Id.* at (b).
155. 18 U.S.C. § 2706.
156. 18 U.S.C. § 2708. See also 18 U.S.C. § 2712(d).
157. 18 U.S.C. § 2701(b).
158. *Id.*

Civil Action Generally

Any person who is aggrieved by a knowing or intentional violation of the Stored Communications Act may bring an action against the violator (other than the United States), seeking preliminary, equitable, or declaratory relief, damages, and attorneys fees and costs.[159]

The damages that may be assessed are the greater of $1,000 or the sum of actual damages and any profits made by the violator as a result of the violation. If the violation was willful or intentional, punitive damages may be awarded.[160]

Civil Action Against the United States

Any person who is aggrieved by a willful violation of the Stored Communications Act by the United States may bring a civil action against the United States for money damages.[161] Damages are assessed to be the greater of $10,000 or actual damages, plus litigation costs.[162] Special procedures for such an action are specified in the statute.[163]

Administrative Discipline

If a court or federal agency finds that an officer or agent of the United States violated the Act, the department may take disciplinary action against the violator.[164]

Defenses

There is no cause of action against a provider, in any court, if the provider acted in accordance with a court order, warrant, subpoena, statutory authorization, or certification pursuant to the Stored Communications Act.[165]

In addition, good faith reliance on any of the following is a complete defense to any civil or criminal action brought under the Stored Communications Act or any other law:

> (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);
> (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

159. 18 U.S.C. § 2707(a)-(b).
160. *Id.* at (c).
161. 18 U.S.C. § 2712(a).
162. *Id.*
163. *Id.* at (b), (e).
164. 18 U.S.C. § 2707(d).
165. 18 U.S.C. § 2703(e).

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of…[166]

VIDEO PRIVACY PROTECTION ACT

In 1988, the SCA was amended to add a section that protects the privacy of consumer video rental histories.[167] That statute (known as the "Video Privacy Protection Act") establishes civil liability if a "video tape service provider" discloses customer information that "identifies a person as having requested or obtained specific video materials or services."[168]

By its terms, this provision applies to "prerecorded video cassette tapes *or similar audio visual materials*," "video tapes or *other audio visual material*," and to both "goods *and services*."[169] That language seems designed to extend the section's protections to audio visual content regardless of medium. Thus, there is case law that seems to accept (without analysis) that the statute applies to DVDs.[170] Similarly, a district court recently held (without analysis) that the statute applies to video content streamed over the Internet.[171]

There are exceptions to the statute's prohibition on disclosure where law enforcement obtains a warrant based on probable cause, where a court orders discovery in a civil proceeding, in the ordinary course of business, and where the customer consents to disclosure.[172] Moreover, a provider can disclose a customer's identifying information to any person, so long as the disclosed information does not identify "the title, description, or subject matter of the video" provided to the customer.[173]

Disclosure to law enforcement pursuant to a warrant can only be made with prior notice to the customer.[174] There is no provision for delayed notice.

An aggrieved customer can bring a civil action for damages against a provider who makes an unlawful disclosure.[175]

Notably, illegally obtained video history information "shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any

166. 18 U.S.C. § 2707(e).
167. 18 U.S.C. § 2710.
168. *Id.*
169. *Id.* at (a)(1), (3)-(4), (b)(2)(D)(ii).
170. Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535 (7th Cir. 2012)
171. In re Hulu Privacy Litig., 2014 U.S. Dist. LEXIS 59479 (N.D. Cal. 2014)
172. 18 U.S.C. § 2710(b).
173. *Id.* at (b)(2)(D).
174. *Id.* at (b)(3).
175. *Id.* at (c).

court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State."[176]

Finally, the statute imposes a duty on providers to destroy customer history information "as soon as practicable," but in no case more than one year from the date it is no longer needed for the purpose for which it was collected.[177]

PEN REGISTERS & TRAP AND TRACE DEVICES

The Pen Register Act governs the use of "pen registers"[178] and "trap and trace devices"[179] to collect non-content "dialing, routing, addressing, or signaling information" about wire and electronic communications. A pen register tracks outgoing communications. A trap and trace device tracks incoming communications.

Prohibition

It is generally unlawful for any person to install and use a pen register or trap and trace device.[180]

That general prohibition is subject to a number of exceptions. The most germane for the purposes of this study is the exception for interception by law enforcement pursuant to a court order.[181] The law enforcement exception is discussed in detail below.

For the sake of completeness, it is worth briefly noting the other statutory exceptions:

- It is not unlawful for a communication service provider to use such devices in relation to the operation, maintenance, or testing of service, to protect the rights or property of the provider, or to protect other users of the service from abuse or unlawful use of the service.[182]
- It is not unlawful for a communication service provider to use such devices, with the consent of the customer, to record the fact that a communication was initiated or completed in order to

176. *Id.* at (d).
177. *Id.* at (e).
178. 18 U.S.C. § 3127(3).
179. *Id.* at (4).
180. 18 U.S.C. § 3121(a).
181. *Id.*
182. *Id.* at (b)(1).

protect the provider, a related provider, or the customer from fraudulent, unlawful, or abusive use of the service.[183]

- The definition of "pen register" does not include a device used by a communication service provider for the purposes of billing a customer for the use of the service. Consequently, such a device is not subject to regulation as a pen register.[184] There should probably be a similar exception in the definition of "trap and trace device," because some providers bill for incoming communications as well. The statute does not contain such an exception.

In addition, the prohibition on the use of a pen register or trap and trace device does not apply to use pursuant to the Foreign Intelligence Surveillance Act of 1978.[185]

Law Enforcement Access

The federal and state governments can apply to a court of competent jurisdiction for an order authorizing the use of a pen register or a trap and trace device.[186] A warrant is not required. Specific details about the court order and its use are discussed below.

Application for Order

The government must apply, in writing and under oath or affirmation, for an order authorizing use of a pen register or a trap and trace device, or for the extension of such an order.[187]

The application must identify the government attorney applying for the order and the agency conducting the criminal investigation at issue.[188] The application must also certify that the "information likely to be obtained" pursuant to the order is "relevant to an ongoing criminal investigation being conducted by that agency."[189]

Legal Standard for Granting Authority

If the court finds that the officer submitting the application "has certified" that the information likely to be obtained by use of the pen register or trap and trace device is relevant to an ongoing criminal investigation, the court *shall* issue

183. *Id.* at (b)(2).
184. 18 U.S.C. § 3127(3).
185. 18 U.S.C. § 3121(a).
186. *Id.*
187. 18 U.S.C. § 3122(a).
188. *Id.* at (b)(1).
189. *Id.* at (b)(2).

the order.[190] Consequently, "judicial review is ministerial, and the issuing judge does not conduct an independent inquiry into the facts attested to by the applicant."[191]

Content of Order

An authorizing court order must contain all of the following information:[192]

- The identity, if known, of the person whose facilities will be monitored.
- The identity, if known, of the person who is the subject of the criminal investigation.
- A description of the communications to be monitored.
- A statement of the offense being investigated.
- If requested by the applicant, language directing the assistance of service providers.

Duration and Extension

A court order authorizing the use of a pen register or a trap and trace device is limited to 60 days, unless that period is extended. Additional 60-day extensions may be granted, under the rules described above.[193]

Nondisclosure

The statute protects the secrecy of the use of a pen register or a trap and trace device, in two ways:[194]

- The court order authorizing use is sealed.
- The court order prohibits any service provider from disclosing the use of the pen register or trap and trace device to any person.

Minimization

A government agency that is authorized to use a pen register or a trap and trace device must use reasonably available technology to prevent the acquisition of communication *content*.[195]

190. 18 U.S.C. § 3123(a)(1)-(2).
191. *Electronic Surveillance, supra* note 9, at 4:84 (footnotes omitted).
192. 18 U.S.C. § 3123(b).
193. *Id.* at (c).
194. *Id.* at (d).
195. 18 U.S.C. § 3121(c).

Reporting

If a government agency uses its own device on a packet-switched network[196] of an electronic communication service provider, the agency is required to keep certain records and provide them to the court.[197] The record must include the names of officers accessing the device, the date and time the device was installed and uninstalled, the date and duration of each use of the device, the configuration of the device, and any information collected by the device.[198] The record must be provided under seal to the court, ex parte, within 30 days after termination of the order (including any extensions).[199] It is not clear to the staff why this record-keeping requirement only applies to devices owned by law enforcement that are attached to a packet-switched network.

Required Assistance and Compensation

If a government agency is authorized to use a pen register or a trap and trace device and the agency requests (and the court orders) assistance from a communication service provider, landlord, custodian, or other person, that person is required to provide any information, facilities, and technical assistance necessary to accomplish the installation of the device unobtrusively and with a minimum of service disruption.[200]

Persons who are required to provide assistance are entitled to compensation of their reasonable expenses.[201]

Emergency Exception

A government agency is not required to obtain an authorizing court order before using a pen register or trap and trace device if (1) there is an emergency situation that requires such use before an order could, with due diligence, be obtained, and (2) there are grounds for issuance of such an order.[202] For the purposes of this exception, an emergency situation is one that involves any of the following:

196. Packet-switching is a protocal for transmitting data over a shared network (e.g., the Internet), by dividing content into small units ("packets") for transmission by varying routes. It is contrasted with "circuit switching," which involves transmission over dedicated circuits. See generally http://en.wikipedia.org/wiki/Packet_switching.
197. 18 U.S.C. § 3123(a)(3).
198. *Id.*
199. *Id.*
200. 18 U.S.C. § 3124(a)-(b).
201. *Id.* at (c). See also 18 U.S.C. § 3125(d).
202. 18 U.S.C. § 3125(a).

(A) immediate danger of death or serious bodily injury to any person;

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year ….[203]

If an agency proceeds under this exception, it is required to obtain a court order within 48 hours after the installation of the device.[204] In the absence of such an order, use of the device must end at the earliest of the 48-hour period, the refusal of the court to grant the order, or the acquisition of the information sought.[205]

The knowing failure to apply for an order authorizing emergency use within the 48-hour period specified above is a violation of the statute.[206]

Remedy for Violation

A person who knowingly violates the prohibition on installation and use of a pen register or a trap and trace device may be fined, imprisoned for not more than one year, or both.[207] There does not appear to be any civil remedy.

Moreover, if an investigative or law enforcement officer willfully discloses a record obtained with a pen register or a trap and trace device, other than in the official performance of duties, the disclosure is deemed to be a violation of the Stored Communications Act.[208] The remedies for a violation of the Stored Communication Act are discussed earlier in this memorandum.

Defense from Liability

There is no cause of action in any court against a communication provider (or its personnel) for providing assistance in accordance with a court order or request pursuant to the statute.[209] Good faith reliance on a court order or request under The Pen Register Act is a complete defense against any civil or criminal action brought under any law.[210]

---

203. *Id.* at (a)(1).
204. *Id.* at (a).
205. *Id.* at (b).
206. *Id.* at (c).
207. 18 U.S.C. § 3121(d).
208. 18 U.S.C. § 2707(g). This rule does not apply to records that were previously lawfully disclosed by the government or by the plaintiff in a civil suit. *Id.*
209. 18 U.S.C. § 3124(d).
210. *Id.* at (e).

Statistical Reporting

The United States Attorney General is required to submit annual reports to Congress providing specified statistics on the use of pen registers and trap and trace devices by the Department of Justice.[211]

Communications Assistance for Law Enforcement Act

A provision of the Stored Communications Act authorizes a court order to enforce the requirements of CALEA.[212] That provision also applies in the context of pen registers and trap and trace devices.

LOCATION DATA

Can the statutes discussed above be used by the government to access customer location data? The answer is complicated and somewhat uncertain.

First, a distinction must be drawn between *historical* location data and data that is *real-time or prospective*. Most of the reported cases focus on the latter, but there are cases holding that *historical* data can be accessed under the Stored Communication Act.[213] The argument seems to be that cell phone location data is "a record or other information pertaining to a subscriber to or customer of" an ECS or RCS provider.[214] As discussed earlier, the government can compel the disclosure of such records with less than a showing of probable cause. That said, the general purpose of the Stored Communications Act is to obtain *existing* records, not to gather future records and convey them to the government.[215]

In most cases, the government would use a pen register or a trap and trace device to gather real-time or prospective non-content data about customer communications. The statute governing such devices specifically provides for the collection of "signaling information,"[216] which appears to encompass cell site

211. 18 U.S.C. § 3126.
212. 18 U.S.C. § 2522.
213. See, e.g., In re Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
214. 18 U.S.C. § 2703(c).
215. See, e.g., In re Application for Pen Register and Trap/Trace Device With Cell Site Location and Auth., 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) ("[T]he entire focus of the [Stored Communications Act] is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service providers. Nothing in the [Stored Communications Act] contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities.").
216. 18 U.S.C. § 3127(3)-(4).

location data.[217] On its face, that language suggests that a pen register could be used to track real-time and prospective cell site location data.

However, the Communications Assistance for Law Enforcement Act (discussed earlier) includes language that presents an obstacle to such use of a pen register. That Act, which requires telecommunication providers to make their systems technically accessible to government surveillance, provides in part:

> (a) Capability requirements . . . [A] telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of -
>
> . . .
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier -
>
> (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
>
> (B) in a manner that allows it to be associated with the communication to which it pertains,
>
> *except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)*.[218]

In response to that apparent restriction on the use of a pen register to gather location information, the government has emphasized the use of the word "solely" in the phrase "information acquired *solely* pursuant to the authority for pen registers and trap and trace devices." The government has argued that use of a pen register to acquire such information is permissible if coupled with some other source of authority. Specifically, it has been argued that a pen register can be used to gather location information if the applicant obtains an order to obtain non-content information under the Stored Communications Act. This requires a higher evidentiary showing than under the pen register statute, but does not require a warrant based on probable cause. The federal courts have split on whether the government's "hybrid" or "converged" authority argument is

217. See, e.g., In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) ("cell site location data is encompassed by the term 'signaling information.'").

218. 47 U.S.C. § 1002 (emphasis added).

plausible. Most courts have rejected it, holding that there is no authority under ECPA to gather prospective location data.[219] But a few courts have accepted the argument and have issued orders accordingly.[220]

Moreover, the statutory arguments discussed above may have partially been superseded by the United States Supreme Court. In the fairly recent case of *United States v. Jones*,[221] the Court held that the use of a GPS tracking device without a warrant violated the Fourth Amendment of the United States Constitution. Although the Court did not decide how the Fourth Amendment would apply to location tracking using cell site or GPS location data that is obtained from a communication service provider, the five concurring Justices indicated that such tracking could be a Fourth Amendment search.[222] The Fourth Amendment status of such a search would depend on the duration of tracking and the severity of the crime.[223] The concurring Justices did not offer a bright line standard, but did state that such a search conducted on the facts before it (four weeks of tracking in a routine drug trafficking case) would have violated the Fourth Amendment.[224]

This strongly suggests that location tracking without probable cause and a warrant, under the "hybrid" statutory authority discussed above, would violate the Fourth Amendment in some scenarios.

PREEMPTION OF STATE LAW

When the Commission reaches the stage of drafting proposed legislation on government access to customer information of communication service providers in California, it will be necessary to know the extent to which ECPA preempts state law. In addressing that issue, this memorandum begins by discussing the general principles of federal preemption. It then applies those principles to the four elements of ECPA that are discussed above (i.e., interception of communications, access to stored communications, videotape privacy, and the use of pen registers and trap and trace devices).

---

219. See generally Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use, 15 A.L.R. Fed. 2d 537 (2014).
220. *Id.*
221. 132 S. Ct. 945 (2012).
222. See generally Memorandum 2014-13, pp. 35-39.
223. *Id.*
224. *Id.*

Federal Preemption Generally

Clause 2 of Article VI of the United States Constitution (the "Supremacy Clause") provides as follows:

> This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.

Under the Supremacy Clause, a valid federal law that is applicable to the states is superior to and will control over a state law. That does not mean that state law will always displaced. The preemption of state law by a federal statute depends on congressional intent.

In some cases, Congress intends to preempt an entire field of regulation, precluding any state regulation in the area. Field preemption may be based on express statutory language or evidence of congressional intent. Or it may be implied where there is a clear need for national uniformity or where the statutory scheme is so comprehensive that it leaves no room for state regulation.

Out of respect for the police powers of the states, the Supreme Court generally presumes against finding field preemption:

> The principle to be derived from our decisions is that federal regulation of a field of commerce should not be deemed preemptive of state regulatory power in the absence of persuasive reasons — either that the nature of the regulated subject matter permits no other conclusion, or that the Congress has unmistakably so ordained.
>
> …
>
> The settled mandate governing this inquiry, in deference to the fact that a state regulation of this kind is an exercise of the "historic police powers of the States," is not to decree such a federal displacement "unless that was the clear and manifest purpose of Congress[.] … In other words, we are not to conclude that Congress legislated the ouster of this California statute … in the absence of an unambiguous congressional mandate to that effect."[225]

As will be seen below, this general presumption against finding field preemption is important in analyzing the preemptive effect of ECPA.

In the absence of field preemption, a federal statute will still preempt federal laws that are in conflict with the federal law:

---

225. Florida Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142, 146 (1963).

> In areas of the law not inherently requiring national uniformity, our decisions are clear in requiring that state statutes, otherwise valid, must be upheld unless there is found "such actual conflict between the two schemes of regulation that both cannot stand in the same area…."[226]

An irreconcilable conflict between federal and state law can arise where the state law requires something that the federal law forbids. In such a case, it would be impossible to comply with both laws. The inconsistent state requirement would be preempted:

> A holding of federal exclusion of state law is inescapable and requires no inquiry into congressional design where compliance with both federal and state regulation is a physical impossibility….[227]

There may also be a conflict between federal and state law where compliance with the state rule would frustrate the federal regulatory goals (i.e., the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[228]

To summarize, in analyzing the extent to which the various parts of ECPA preempt state regulation of the same topics, we must consider all of the following issues:

- Whether there is an "unmistakable" and "unambiguous" Congressional mandate to preempt the entire field of regulation.
- Whether the nature of the regulated subject matter "permits no other conclusion" than that Congress intended to preempt the field.
- Whether a California statute would be "an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."
- Whether a California statute would create an irreconcilable conflict with the federal law, making it impossible to comply with both.

Wiretap Act

Express Statutory Language

The Wiretap Act does not contain language that expressly preempts state law. To the contrary, the Act expressly provides that states will enact statutes

226. Head v. New Mexico Board, 374 U.S. 424, 430 (1963) (citation omitted).
227. *Florida Lime & Avocado Growers*, 373 U.S. at 142-43.
228. Hines v. Davidowitz, 312 U.S. 52, 67 (1941).

addressing major substantive issues relating to state government interception of communications:

> The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, *if such attorney is authorized by a statute of that State* to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter *and with the applicable State statute* an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, *designated in any applicable State statute authorizing such interception*, or any conspiracy to commit any of the foregoing offenses.[229]

Under that provision, a state statute can determine which state or local government attorneys have authority to obtain a court order authorizing interception and the specific crimes that must serve as the necessary predicate for issuance of an order. The provision also states that a state interception warrant must be issued in conformity with *both* Section 2518 *and* the applicable state statute. This seems to mean that a state law can impose requirements beyond what is required by the federal statute. Otherwise, there would be no purpose in stating that both federal and state statutes must be satisfied.

Despite that express grant of state legislative discretion to regulate some of the most important substantive elements in the regulated field, one federal trial court has held, in *Bunnell v. MPAA*,[230] that the Wiretap Act preempts the entire field, precluding any state regulation of the interception of wire, oral, or electronic communications. That conclusion was based in part on the express language of a provision limiting the remedies available for a violation of the Wiretap Act:[231]

> The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the

229. 18 U.S.C. § 2516(2) (emphasis added).
230. Bunnell v. Motion Picture Ass'n of Am., 567 F. Supp. 2d 1148 (C.D. Cal. 2007).
231. *Id.* at 1154.

> only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.[232]

The Court in *Bunnell* did not explain why it viewed that provision as a statement of express field preemption. In the staff's view, that is strained reading of the provision, which can be read to serve a much more modest purpose.

Other federal trial courts have expressed the same view as the staff, holding that the exclusive remedies provision was not intended to establish field preemption:

> In this Court's view, that provision does not even impact the question of preemption, but rather focuses on the scope of available federal remedies when a violation of the statute has been established. Other courts agree and have persuasively argued that this provision, which appears as a subsection of a provision addressing suppression of wiretap evidence obtained in violation of the Act, neither (1) explicitly provides for the preemption of state law; nor (2) applies outside the suppression context. See In re Google Street View Electronic Comm'ns Litig., 794 F. Supp. 2d at 1085 n.12 ("The legislative history supports the proposition that the provision was appended to the ECPA solely to address suppression of evidence by criminal defendants."); Valentine [v. NebuAd, Inc, 804 F Supp. 2d 1022, 1029 (2011)]; In re National Security Agency Telecomm'ns Records Litig., 483 F. Supp. 2d 934, 939 (N.D. Cal. 2007) (this provision was "added to the ECPA for a limited purpose: to prevent criminal defendants from suppressing evidence based on electronic communications or customer records obtained in violation of ECPA's provisions").[233]

On balance, the staff does not think that the statutory language of the Wiretap Act contains an unmistakable and unambiguous congressional mandate to preempt state regulation in the field. To the contrary, the statute expressly calls for state regulation of major issues relating to state court approval of law enforcement interception of communications. Those provisions seem incompatible with any Congressional intent to entirely preempt the field.

Legislative History

A number of courts have examined the legislative history relating to the enactment of the Wiretap Act and have found that Congress intended to establish a uniform regulatory *floor*, so that all interceptions would be in

232. 18 U.S.C. § 2518(10)(c).

233. Leong v. CarrierIQ, Inc., 2012 U.S. Dist. LEXIS 59480, *11-12. See also Valentine v. NebuAd, Inc., 804 F. Supp. 2d 1022 (N.D. Cal. 2011).

compliance with the minimum requirements of the Fourth Amendment as articulated in *Berger v. New York*[234] and *Katz v. United States*.[235] For example, in *People v. Conklin*,[236] the California Supreme Court held that the Wiretap Act did not preempt the California statute on the interception of wire and oral communications:

> [T]he Senate Report indicates that Congress anticipated state regulation of electronic surveillance. As we discussed in *Halpin*[237] … the report refers to numerous areas touching upon the field of electronic surveillance which state law may control. Thus, in referring to a need for uniform nationwide standards, it appears that Congress was not expressing an intent to preempt the entire field; rather, it was emphasizing the need to ensure nationwide compliance with the newly declared standards in *Berger* and *Katz*. Accordingly, we conclude that Congress did not intend to occupy the entire field of electronic surveillance to the exclusion of state regulation.[238]

In 2006, the California Supreme Court reaffirmed its holding in *Conklin*:

> In People v. Conklin (1974) 12 Cal.3d 259, 270–273 [114 Cal. Rptr. 241, 522 P.2d 1049], this court specifically addressed the question whether the provisions of title III of the federal Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§ 2510–2520, hereafter title III) — relating to the wiretapping or recording of telephone conversations — preempted the application of the more stringent provisions embodied in California's invasion-of-privacy law. Reviewing the legislative history of title III, the court in Conklin determined that "Congress intended that the states be allowed to enact more restrictive laws designed to protect the right of privacy" (12 Cal.3d at p. 271), pointing out that a legislative committee report prepared in conjunction with the consideration of title III specifically observed that "'[t]he proposed provision envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation.'" (12 Cal.3d at p. 272.) Accordingly, the court in Conklin rejected the preemption claim.

234. 388 U.S. 41 (1967).
235. 389 U.S. 347 (1967).
236. People v. Conklin, 12 Cal. 3d 259 (1974).
237. Halpin v. Superior Court, 6 Cal. 3d 885, 899 n.17 (1972) ("The Senate Report specifically indicates areas in which the Congress did not intend to preempt state legislation; for example: the degree of disclosure and scope of knowledge required to violate section 2511 (Sen. Rep., supra, at p. 93); the provisions of section 2512 banning the manufacture, distribution, possession and advertisement of interception devices (Sen. Rep., supra, at p. 94); rules in section 2516 governing the authorization of intercepting communications (Sen. Rep., supra, at p. 98); and provisions in section 2520 authorizing the recovery of civil damages (Sen. Rep., supra, at p. 107).").
238. *Conklin,* 12 Cal. 3d at 269.

> Although an amicus curiae brief in the present case urges that the decision in Conklin be reconsidered (see amicus curiae brief of U.S. Chamber of Commerce, pp. 20–23), the brief fails to point to any developments in the almost four decades since Conklin that would warrant such reconsideration, and omits reference to the numerous sister-state and federal decisions that have reached the same conclusion as Conklin with regard to the preemption issue. (See, e.g., Roberts v. Americable Intern. Inc. (E.D.Cal. 1995) 883 F. Supp. 499, 503, fn. 6; United States v. Curreri (D.Md. 1974) 388 F. Supp. 607, 613; Bishop v. State (1999) 241 Ga. App. 517 [526 S.E.2d 917, 920]; People v. Pascarella (1981) 92 Ill. App. 3d 413 [415 N.E.2d 1285, 1287, 48 Ill. Dec. 1]; see also Warden v. Kahn (1979) 99 Cal. App. 3d 805, 810 [160 Cal. Rptr. 471].) … Accordingly, there is no basis for concluding that application of California law is preempted by federal law.[239]

Implied Field Preemption

The *Bunnell* court also finds implied field preemption, on the grounds that ECPA is "so comprehensive" that it "'left no room' for supplementary state regulation."[240] The staff sees no way to square that argument with the fact that the Wiretap Act expressly provides for supplementary state regulation, as discussed above. Plainly, the statute leaves room for supplementary state regulation.

Nor can the argument for implied preemption be reconciled with the analysis of congressional intent in *Conklin* and other cases.

Conflict Preemption

As discussed above, it appears that the Wiretap Act was intended to establish a uniform regulatory floor, ensuring that state interception of communications would be consistent with the minimum requirements of the Fourth Amendment.

Thus, a state statute that is less protective of communication privacy would seem to be in irreconcilable conflict with the federal statute. For example, if California law were to permit the interception of electronic communications without a warrant it would be in direct conflict with the federal prohibition on

239. Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95, 105-06 (2006). See also Lane v. CBS Broad., Inc., 612 F. Supp. 2d 623 (E.D. Pa. 2009) ("Congress expressly authorized states to legislate in this field. Congress apparently wanted to ensure that states meet base-line standards, however, and thus federal law supersedes to the extent that state laws offer less protection than their federal counterparts. In the absence of any other indication that Congress intended to preempt the entire field at issue in this case, and keeping in mind the rarity with which complete preemption applies, we decline to find that complete preemption applies in this matter.").

240. *Bunnell*, 567 F. Supp. 2d at 1154.

such interception. Moreover, it would be an impediment to the overall purpose of the Wiretap Act, ensuring nationwide uniformity as to the minimum protection of communication privacy.

Conclusion

The staff is persuaded that the Wiretap Act does not wholly preempt state regulation of the interception of wire, oral, and electronic communications. However, the Act does establish minimum requirements for the protection of the privacy of such communications. Any California statute must be at least as protective of privacy as the federal statute.

It is not entirely clear whether the provision expressly limiting the remedies available for a violation of the Wiretap Act has any preemptive effect on state law remedies for similar conduct. It might be prudent to fashion any state law remedies so that they mirror the remedies available under the federal act.

Stored Communications Act

Express Statutory Language

The Stored Communications Act does not contain language that expressly preempts state law regulation of the entire field that it regulates.

However, the SCA does contain language that specifically allows a state to bar its own officials from using a court order pursuant to Section 2703(d) (rather than a warrant or subpoena) to obtain stored electronic information:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. *In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.*[241]

One could perhaps argue that the provision allowing states to opt out of the use of a court order to obtain stored electronic information creates a negative inference that states are not permitted to modify *other* elements of the SCA. That inference seems reasonable, but it probably falls short of the "unmistakable" and

241. 18 U.S.C. § 2703(d) (emphasis added).

"unambiguous" congressional mandate that is required in order to find field preemption.

There is one provision that might have some limited preemptive effect — the SCA's exclusive remedies provision:

> The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.[242]

As discussed above, in connection with the Wiretap Act, it is possible that such a provision is intended to preempt the creation of additional state remedies for conduct that would also violate the federal statute. In fact, a published federal trial court opinion (*Quon v. Arch Wireless Operating Co., Inc.*[243]) construes the exclusive remedies provision that way:

> Section 2708 in the SCA provides that, other than pursuit of federal constitutional violations, the remedies outlined in the SCA are the exclusive ones a party may pursue in court for conduct covered by the statute: "The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." Congress' command in enacting section 2708 is clear[.] Only those remedies outlined in the SCA are the ones, save for constitutional violations, that a party may seek for conduct prohibited by the SCA. The SCA thus displaces state law claims for conduct that is touched upon by the statute, such as in divulging stored electronic communications to third parties.[244]

However, as discussed above in connection with the Wiretap Act, there are other possible purposes served by an exclusive remedies provision. As other federal courts have noted, the provision may have been enacted solely to clarify the federal remedies available for a violation of the federal statute.[245]

Legislative History

The staff did not find any case discussing the legislative history of the SCA with regard to preemption.

242. 18 U.S.C. § 2708.
243. 445 F. Supp. 2d 1115 (C.D. Cal. 2006).
244. *Id.* at 1138.
245. See *supra* note 233 and accompanying text.

Implied Field Preemption

In *Quon* (previously mentioned in connection with the exclusive remedy provision), the court seems to agree with an unpublished federal trial court decision, which held that the SCA is so comprehensive that it leaves no room for state regulation:

> On that point the Court agrees with [Muskovich v. Crowell, 1995 U.S. Dist. LEXIS 5899, 1995 WL 905403, at *1 (S.D. Iowa March 21, 1995)] that, in enacting the SCA, Congress left no room for supplementary state regulation for conduct covered by the statute. There are other indicia in the statute itself that evinces Congress' effort to make suits to enforce or seek redress for the statute's prohibitions the exclusive ones for parties to pursue. The intricacies of the regulatory scheme crafted by the ECPA (and the SCA) are fairly comprehensive: Regulating private parties conduct, law enforcement efforts to uncover stored electronic communications, and devising a fairly complicated scheme to accomplish both, including a private right of action for violations of the statute's provisions. In light of the breadth of the SCA regulatory scheme and the clear command concerning the exclusivity of remedies (aside from federal constitutional claims) contained in section 2708 for conduct covered by the statute, it stands to reason "that Congress 'left no room' for supplementary state regulation." Cybernetic, 252 F.3d at 1045.

Other federal trial court decisions have found, without much explanation, that the SCA does not preempt the field that it regulates.[246]

In the staff's opinion, the fact that Congress "left room" for state regulation of *wiretapping* suggests that there is also likely to be room for state regulation of access to *stored communications*. The Wiretap Act and the SCA seem to be equally "intricate" and "comprehensive." They both provide general prohibitions protecting privacy, a complex set of exceptions (including exceptions for law enforcement access pursuant to lawful process), and civil and criminal remedies for statutory violations. If the Wiretap Act leaves room for state regulation, it seems probable that the SCA does the same.

The two statutes are also very similar in terms of their legal and policy effects. If the important policies effectuated in the Wiretap Act are not uniquely federal in character and do not require national uniformity so as to warrant field

246. See Lane v. CBS Broad., Inc., 612 F. Supp. 2d 623 (E.D. Penn. 2009); White v. Baker, 696 F. Supp. 2d 1289 (N.D. Ga. 2010).

preemption, then the same conclusion would seem to apply to the policies underlying the SCA.

If anything, there may be a stronger argument for uniformity for the Wiretap law, because it was intended to ensure that the states meet minimum standards consistent with the Fourth Amendment. By contrast, much of the data that is protected by the SCA is probably not governed by the Fourth Amendment under the third party doctrine. Thus, there is less of a federal interest in establishing uniform minimum standards with respect to access to such data.

For those reasons, with respect to the SCA, the staff does not believe that the argument for implied field preemption is strong enough to overcome the presumption against finding field preemption (i.e., that "the nature of the regulated subject matter permits no other conclusion.").

Conclusion

It is clear that a state may enact a statute forbidding the use of a Section 2703(d) order to obtain stored electronic communications. The SCA expressly permits such legislation.

Despite the absence of appellate authority, and the existence of conflicting federal trial court decisions, it seems probable that the SCA does not entirely preempt state regulation within the field that is covered by the Act. The staff simply does not see the kind of "unmistakable" and "unambiguous" congressional mandate that is required to overcome the presumption against field preemption. Nor is there anything about the intricacy or comprehensiveness of the SCA that clearly compels field preemption. The Wiretap Act is just as intricate and complex and it does not preempt all state regulation in its field.

As discussed in connection with the Wiretap Act, it is not entirely clear whether the provision expressly limiting the remedies available for a violation of the Wiretap Act has any preemptive effect on state law remedies for similar conduct. It might be prudent to fashion any state law remedies so that they mirror the remedies available under the federal act.

Video Privacy Protection Act

The Video Privacy Protection Act contains an express preemption provision:

> The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.[247]

In other words, there is no field preemption. The statute preempts state law only to the extent of any direct conflict with its prohibition on disclosure of protected information.

Pen Register Act

Express Statutory Language

The Pen Register Act does not contain language that expressly preempts state law regulation of the entire field that it regulates.

However, the SCA does contain language that specifically allows a state to regulate important aspects of the law governing use of pen registers and trap and trace devices. For example, a state may enact a statute that bars its own officials from using a pen register or trap and trace device:

> *Unless prohibited by State law*, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.[248]

There is also language that seems to recognize a state's authority to specify *which* state government agencies are authorized to use a pen register or trap and trace device:

> A government agency authorized to install and use a pen register or trap and trace device under this chapter *or under State law*…[249]

In addition, the provision authorizing the emergency use of a pen register or trap and trace device only applies to a state agency that is acting pursuant to an authorizing state statute:

> Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by

247. 18 U.S.C. § 2710(f).
248. 18 U.S.C. § 3122(a)(2) (emphasis added).
249. 18 U.S.C. § 3121(c).

> the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof *acting pursuant to a statute of that State*, …[250]

Finally, the definition of "court of competent jurisdiction," as applied to a state, only includes a criminal court that is authorized by a state statute to issue orders permitting the use of a pen register or trap and trace device:

> … a court of general criminal jurisdiction of a State *authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device* ….[251]

Those provisions, expressly recognizing state regulatory authority on a number of important substantive points, seem incompatible with any congressional intent to wholly preempt the field.

Legislative History

The staff did not find any case discussing the legislative history of the Pen Register Act with regard to preemption.

Implied Field Preemption

The staff did not find any case discussing whether the Pen Register Act impliedly preempts state regulation in the field that it occupies. Nor does there seem to be any good argument to find field preemption. Congress has not comprehensively regulated the subject so as to leave no room for state regulation. Instead, the statute expressly recognizes scope for significant state regulation.

Conclusion

The staff sees no compelling evidence that the Pen Register Act was intended to preempt the field that it regulates. There is no clear congressional mandate for field preemption and the statute itself expressly invites state regulation.

Summary of Preemption Conclusions

The conclusions from the above analysis can be summarized as follows:

250. 18 U.S.C. § 3125(a).
251. 18 U.S.C. § 3127(2)(B).

- The Wiretap Act preempts state laws that are less protective of conversational privacy, to ensure compliance with the minimum requirements of the Fourth Amendment.
- The Wiretap Act generally allows states to enact more stringent privacy protections.
- The Wiretap Act expressly provides for state regulation of certain elements of the warrant application and issuance process.
- The SCA does not appear to preempt state regulation generally.
- The SCA expressly allows states to opt out of using Section 2703(d) orders.
- It is possible that the exclusive remedy provisions in the Wiretap Act and the SCA were intended to preempt state remedies for conduct that violates the federal laws.
- The Video Privacy Protection Act does not preempt state law, except to the extent that a state law would require a disclosure that the federal law prohibits.
- The Pen Register Act does not appear to preempt the field that it regulates. It expressly recognizes scope for state regulation on a number of important issues addressed by the Act. This includes the right of a state to opt out of authorizing the use of pen registers and trap and trace devices.
- Any provision of state law could be preempted if it conflicts with the federal statutes described in this memorandum.

Respectfully submitted,

Brian Hebert
Executive Director