Study G-300 February 6, 2014

First Supplement to Memorandum 2014-5

State and Local Agency Access to Customer Information from Communication Service Providers (Material Received at Meeting)

The following material was received by the Commission[1] at the meeting on February 6, 2014, in connection with Study G-300 on State and Local Agency Access to Customer Information from Communication Service Providers , and is attached as an Exhibit:

Respectfully submitted,

Brian Hebert
Executive Director

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.

F. Quick Reference Guide

	Voluntary Disclosure Allowed?		How to Compel Disclosure	
	Public Provider	**Non-Public**	**Public Provider**	**Non-Public**
Basic subscriber, session, and billing information•	No, unless §2702(c) exception applies *§ 2702(a)(3)*	Yes *§ 2702(a)(3)*	Subpoena; 2703(d) order; or search warrant *§ 2703(c)(2)*	Subpoena; 2703(d) order; or search warrant *§ 2703(c)(2)*
Other transactional and account records	No, unless §2702(c) exception applies *§ 2702(a)(3)*	Yes *§ 2702(a)(3)*	2703(d) order or search warrant *§ 2703(c)(1)*	2703(d) order or search warrant *§ 2703(c)(1)*
Retrieved communications and the content of other stored files#	No, unless § 2702(b) exception applies *§ 2702(a)(2)*	Yes *§ 2702(a)(2)*	Subpoena with notice; 2703(d) order with notice; or search warrant* *§ 2703(b)*	Subpoena; SCA does not apply* *§ 2711(2)*
Unretrieved communications, including email and voice mail (in electronic storage more than 180 days)†	No, unless § 2702(b) exception applies *§ 2702(a)(1)*	Yes *§ 2702(a)(1)*	Subpoena with notice; 2703(d) order with notice; or search warrant *§ 2703(a), (b)*	Subpoena with notice; 2703(d) order with notice; or search warrant *§ 2703(a), (b)*
Unretrieved communications, including email and voice mail (in electronic storage 180 days or less)†	No, unless § 2702(b) exception applies *§ 2702(a)(1)*	Yes *§ 2702(a)(1)*	Search warrant *§ 2703(a)*	Search warrant *§ 2703(a)*

• See 18 U.S.C. § 2703(c)(2) for listing of information covered. This information includes local and long distance telephone connection records and records of session times and durations as well as IP addresses assigned to the user during the Internet connections.

† Includes the content of voice communications.

* For investigations occurring in the Ninth Circuit, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), requires use of a search warrant unless the communications have been in storage for more than 180 days. Some providers follow *Theofel* even outside the Ninth Circuit; contact CCIPS at (202) 514-1026 if you have an appropriate case to litigate this issue.

EX 1

Susan S. Kreston[i] and Robert M. Morgester[ii]

Computer are increasingly becoming a common element of the domestic violence crime scene. Used as either a tool to facilitate the commission of the crime or as a repository of information, the use of a computer by both victims and suspects is forcing prosecutors to become experts in a area of law that is evolving at unsettled pace. In dealing with computer related evidence prosecutors must become aware of some of the lessor-known federal and state privacy issues that may come into play.[iii]

Title III of the Ominbus Crime Control and Safe Street Act of 1968 (Title III), Pen Registers and Trap and Trace Device chapter of Title 18 (Pen/Trap), Electronic Communication Privacy Act (ECPA) and the Privacy Protection Act (PPA) are four such statutes and a basic awareness of their principles and the rights they may afford to suspects and third parties is essential to avoiding unnecessary legal difficulties which might lead to financial liability. It also must be remembered that although the ECPA sets the minimum level of privacy protection, the California Constitution, state statutes, and state court decisions provide additional levels of privacy protection.

Title III - Title III protects electronic communication from interception during transmission (e.g. wiretap) by a third party who is not a participating member of the communication.[iv] A human voice and most Internet communications (including e-mail) are electronic communication.[v] Title III applies to all parties, private and law enforcement alike. California's more restrictive version of Title III is codified in Chapter 1.3 of the Penal Code.[vi] California additionally prohibits interception or recording of a confidential communication[vii] during transmission (e.g. recording) by a party to the communication.[viii]

A public or private party is generally prohibited from voluntarily disclosing the content of wire and electronic communication intercepted during transmission. In California state court the eight exceptions to this rule are: (1) wire tap order;[ix] (2) where the addressee / sender consents to the interception;[x] (3) when the interception is necessary to protect the rights or property of the communication service provider;[xi] (4) when the interception is made by a law enforcement officer or designee who is a party to the communication;[xii] (5) when the interception is made by a victim of a specified crime (including harassing phone calls) who is a party to the communication;[xiii] (6) upon order by a judge following the request of victim of domestic

violence who is seeking a domestic violence restraining order;[xiv] (7) where the communication provider inadvertently obtains information that pertains to the commission of a crime;[xv] and (8) when the communication is made through a system that is configured so that the communication is readily accessible to the general public.[xvi] A confidential communication that is obtained in violation of these provisions cannot be used for any purpose.[xvii]

Pen/Trap - Pen Trap statute regulates the collection of addressing information for wire and electronic communication.[xviii] The addressing information for a telephone call is either the outgoing call's telephone number or the incoming call's origination number (caller ID).[xix] This also applies to internet communication. Every computer communication contains a "header" which contains address information.

An Electronic Service (ECS) provider[xx] may use a pen / trap device without a court order where: (1) the user consents to the interception;[xxi] (2) when the interception is necessary to protect the rights or property of the communication service provider;[xxii] (3) when the interception is necessary to protect the communication service provider or a user of that service (customer or other provider) from fraudulent, unlawful, or abuse of service;[xxiii] and (4) when there is an emergency involving an immediate risk of death or serious physical injury to a person.[xxiv]

Law enforcement can obtain this address information via a pen register or trap and trace order. This investigative tool is helpful in identifying the address of where the suspect is coming from when they access information in a Hotmail or Yahoo account. In California a judicial review of the order is required to authorize the installation of a pen register or trap and trace device.[xxv] The applicant is required to justify that the information likely to be obtained is relevant to an on going criminal investigation.[xxvi] The order is only good for 60 days, however upon application extensions may be granted.[xxvii] The order shall be sealed until otherwise directed by the court and the ECS shall be directed not to information relating to the pen / trap device until further ordered by the court.[xxviii]

Although federal law grants the authority to state courts to issue these orders, it is unclear if a state court can issue such an order upon an out-of-state ECS. Use of a search warrant to authorize the use of a pen / trap device remedies this issue. The order is only good for ten days and must be issued by a Superior Court Judge.[xxix] Penal Code section 1524.2 allows the out of state service of a California search warrant on an ECS who is qualified to do business in California pursuant to section 2105 of the Corporations Code.

ECPA - ECPA protects communication based upon its form. It protects wire and electronic communication content in storage by the provider (e.g. e-mail records held by an Internet Service Provider).[xxx] The ECPA applies to all parties, private and law enforcement alike. However, for law enforcement , there are mechanisms for requiring disclosure to the government by public ECS providers of information regarding an electronic communication. The most well known example of an ECS would be an Internet Service Provider (ISP), such as America On Line, Hotmail, or Yahoo.

A public or private ECS is generally prohibited from voluntarily disclosing the content of wire and electronic communication intercepted during transmission[xxxi]. The four exceptions to this rule are: (1) where the addressee / sender consents to the disclosure;[xxxii] (2) where the communication provider is permitted to disclose customer communications in emergencies involving an immediate risk of death or serious physical injury to a person;[xxxiii] (3) when the disclosure is necessary to protect the rights or property of the communication service provider;[xxxiv] and (4) where the communication provider inadvertently obtains information that pertains to the commission of a crime.[xxxv] The appropriate mechanisms available to California law enforcement to law enforcement to compel disclosure of information is a search warrant.[xxxvi]

Pursuant to the ECPA a subpoena can be used to obtain basic subscriber information.[xxxvii] Basic subscriber information includes customer's name, address, length of service, means and source of payment including any credit card or bank account number, local and long distance telephone toll billing records, records of session times and durations, as well as any temporarily assigned network address[xxxviii]. However, in that this information would be considered a "virtual current biography" of a person, the California Constitution requires a subpoena duces tecum[xxxix] or other judicially reviewed process, to obtain this information.[xl] Failure to obtain a subpoena duces tecum or other process authorized by a state judge for this information will not result in suppression but may have civil consequences.[xli]

Pursuant to the ECPA a subpoena can be used to obtain opened e-mail from a provider if the "customer" or "subscriber" is given prior notice of the disclosure by the government.[xlii] This disclosure may be delayed for up to 90 days when notice would jeopardize a pending investigation or endanger the physical safety of a person.[xliii] An extension of an additional 90 days may be considered by the issuing court.[xliv] Following the delay notification period the government must give notice.[xlv]

Pursuant to the ECPA a court order, sometimes referred as to an "articulable facts order" or "§ 2703 (d) court order" may be sought to obtain all other subscriber information except the content of an unopened e-mail that has been stored for 180 days or less.[xlvi] To obtain a "§ 2703 (d) court order," there must be specific and articulable facts showing that there are reasonable grounds to believe that the specified records are relevant and material to an ongoing criminal investigation.[xlvii] These records would include complete audit trails/logs, web sites visited, identities of e-mail correspondents, cell site data from cellular / PCS carriers, and opened e-mail. As a practical matter a "§ 2703 (d) court order" can also be used to obtain basic subscriber information. Notice to the subscriber is only required when opened e-mail is requested from the provider (see supra using a subpoena to obtain opened e-mail).

A search warrant is necessary for obtaining unopened electronic communication in storage for less then 180 days or voice mail.[xlviii] As the level of governmental process escalates from subpoena to court order to search warrant , it must be remembered that the information available under the less exacting standard is included at the higher level (i.e. a search warrant will get you basic subscriber information, transactional information, and content of the stored communication). The use of a search warrant removes the need for the government to comply with the notice requirements previously mentioned.[xlix] Additionally, law enforcement is allowed to request from the court an order commanding the communication provider not to disclose the existence of any issued court order, for such a period as the court deems appropriate, where notification would lead to: (1) endangering the physical safety of an individual; (2) flight from prosecution; (3) tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.[l]

Law enforcement can and should talk to ISP in advance about what types of information are sought and what the ISP may have. 18 U.S.C. § 2703(f) authorizes law enforcement to request the provider to take all steps necessary to preserve records and other information in its possession while law enforcement begins to obtain the necessary legal process to obtain the records.. This 2703(f) order or preservation request only applies to information in possession of the provider at the time the request is made.

There is no suppression remedy for a violation of the ECPA except in those cases where the defendant's constitutional rights have been violated.[li] Civil damages are the exclusive remedy for violation of the ECPA.[lii] These include a minimum damage amount of $1,000, plus

costs, punitive damages and attorney fees. Negligent breaking or destroying of equipment is also actionable. Additionally, loss of business opportunity may be actionable, particularly if it is brought by innocent third parties. Employees of the United States may be subject to disciplinary action if the violation was willful or intentional. Good faith defense is complete.[liii]

PPA - The PPA[liv] protects persons who may broadly, but reasonably claim to be publishers. The PPA establishes safeguards for these "publishers" from governmental search and seizure of the materials in their possession. These materials may be either "work product" (materials created by the author / publisher) or "documentary materials" (any materials that document or support the work product). Unlike the ECPA, the PPA applies only to law enforcement. If the material is covered by the PPA, law enforcement must serve the target with a subpoena, allowing the target to challenge the subpoena by a motion to quash before complying with it. Article I, section 2(b) of the California State Constitution "additionally protects a newsperson from being adjudged in contempt for refusing to disclose either (1) unpublished information, or (2) the source of the information, whether published or unpublished."[lv]

Exception to the PPA requirements of a subpoena generally include: (1) materials searched for or seized are contraband, instrumentalities, or fruits of the crime; (2) materials searched for are evidence of a crime; or (3) the seizure of materials is necessary to prevent death or serious bodily injury.[lvi] The PPA does not require investigators to give the publisher notice when doing so would reasonably result in the destruction, alteration, or concealment of the materials.[lvii]

The importance of this act to prosecutors and investigators lies more in the area of commingled materials. Where there is evidence relating to the crime located on a computer which also contains protected material ("work product" or "documentary materials"), issues concerning proper scope and execution of a search warrant will arise. It is recommended that a protocol be in place to address how to attempt to separate these types of material.[lviii] Recent court cases appear to indicate that the courts are limiting the scope of PPA protection to the press and certain other people not suspected of committing a crime (i.e. PPA does not apply to criminal suspects).[lix] However until this issue is more firmly settled, the best practice would be to minimize the taking of potentially protected materials and to return potentially protected materials that are taken as soon as possible.[lx]

There is no suppression remedy for a violation of the PPA.[lxi] Civil damages are the exclusive remedy for violation of the PPA. These include actions for damages, including attorney fees and costs, with a statute of limitations of two years.[lxii] The "good faith" defense is available to law enforcement investigators under this statute.[lxiii] The good faith defense does not extend to government entities, except in limited circumstances.[lxiv] Nothing in the PPA prevents the government from seeking forfeiture of computers or related media containing commingled materials.[lxv]

Conclusion

Computers and electronic communication are an intrinsic part of the new crime scene. Knowing the laws that protect the privacy of information must be a priority for the investigators and prosecutors who seek to utilize the best practices in search and seizure of computer evidence, and to minimize the potential personal and departmental liability of the parties involved.

---

i. Deputy Director, National Center for Prosecution of Child Abuse.

ii. Deputy Attorney General, State of California Department of Justice.

iii. An excellent resource on federal issues is the United States Department of Justice manual entitled *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. The manual may be downloaded at http://www.cybercrime.gov.

iv. *See* 18 U.S.C. §§ 2510-2522; Pen. Code, §§ 631(wiretap), 632 (cellular radio), 632.6 (cordless or cellular telephones).

v. 18 U.S.C. § 2510.

vi. *See generally* Pen. Code, §§ 629.50-629.98

vii. The term "confidential communication" includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded. (Pen. Code, § 632 (c).)

viii. Pen. Code, § 632. Federal law is less restrictive. (See 18 U.S.C. § 2510(5)(a).)

ix. *See* 18 U.S.C. §§ 2510-2522; Pen. Code, §§ 629.50-629.98. A resources for sample wiretap orders and other pertinent legal authority is Robert Schirn, Barbara E. Turner, *WIRETAP MANUAL Los Angeles County District Attorney's Office* (2001).

x. 18 U.S.C. § 2511(2)(c)-(d).

xi. 18 U.S.C. § 2511(2)(a)(i); Pen. Code, §§ 632 (e), 632.5 (b), 632.7 (b).

xii. Pen. Code, § 633.

xiii. One party to a confidential communication may record the communication for the purpose of obtaining evidence reasonably believed to relate to the commission by another party to the communication of the crime of extortion, kidnapping, bribery, any felony involving violence against the person, or a violation of Section 653m. (Pen. Code, § 633.5.)

xiv. Pen. Code, § 633.6.

xv. 18 U.S.C. § 2511(3)(b)(iv).

xvi. 18 U.S.C. § 2511(2)(g)(i).

xvii. Pen. Code, § 632 (d).

xviii. *See* 18 U.S.C. §§ 3121-3127. A resources for sample pen / trap device orders and other pertinent legal authority is Robert Schirn, Barbara E. Turner, *WIRETAP MANUAL Los Angeles County District Attorney's Office* (2001).

xix. *See* 18 U.S.C. § 3127 (3)-(4).

xx. An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. 2510 (15).

xxi. 18 U.S.C. § 3121(b).

xxii. *Id.*; 18 U.S.C. § 2702(c)(3); See also Pen. Code, §§ 632 (e), 632.5 (b), 632.7 (b); although not directly addressed under California law, the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. *Cf. United States v. Auler* (7th Cir. 1976) 539 F.2d 642, 646 n.9 (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device).

xxiii. *Id.*

xxiv. 18 U.S.C. § 2702(b)(6). ***Warning***, this information may be considered protected under the California Constitution. (*See* Cal. Const., art. 1, §§ 13; *People v. Larkin* (1987) 194 Cal.App.3d 650; *People v. Chapman* (1984) 36 Cal.3d 98, 105-106, 110; *People v. Blair* (1979) 25 Cal.3d 640, 748-755; *Carlson v. Superior Court* (1976) 58 Cal.App.3d 13, 21-23.) There is currently an absence of statutory rules addressing this type of disclosure (*cf.* Pen. Code, §§ 632 (e), 632.5 (b), 632.7 (b)). Disclosure will not result in suppression but may have civil consequences. (*People v. McKay* (2002) 27 Cal.4th 601; *People v. Larkin, supra,* 194 Cal.App.3d 650.)

xxv. *People v. Larkin, supra,* 194 Cal.App.3d 650.

xxvi. 18 U.S.C. § 3123.

xxvii. 18 U.S.C. § 3123 (c).

xxviii. 18 U.S.C. § 3123 (d).

xxix. *People v. Larkin, supra,* 194 Cal.App.3d 650.

xxx. *See* 18 U.S.C. § 2701 et seq.

xxxi. *See* 18 U.S.C. § 2701 (a).

xxxii. *See* 18 U.S.C. § 2701 (c).

xxxiii. *See* 18 U.S.C. § 2702 (b)(6). ***Warning***, this information may be considered protected under the California Constitution. (*See* Cal. Const., art. 1, §§ 13; *People v. Larkin, supra,* 194 Cal.App.3d 650; *People v. Chapman, supra,* 36 Cal.3d 98, 105-106, 110; *People v. Blair, supra,* 25 Cal.3d 640, 748-755; *Carlson v. Superior Court, supra,* 58 Cal.App.3d 13, 21-23.) There is currently an absence of statutory rules addressing this type of disclosure (*cf.* Pen. Code, §§ 632 (e), 632.5 (b), 632.7 (b)). Disclosure will not result in suppression but may have civil consequences. (*People v. McKay, supra.* 27 Cal.4th 601; *People v. Larkin, supra,* 194 Cal.App.3d 650.)

xxxiv. *See* 18 U.S.C. § 2702 (c); Pen. Code, §§ 632 (e), 632.5 (b), 632.7 (b).

xxxv. *See* 18 U.S.C. § 2702 (c).

xxxvi. As a practical matter the search warrant allows access to basic subscriber information, transactional information, and content of the stored communication and pursuant to Penal Code section 1524.2 can be served on an out-of-state ECS who does business with California.

xxxvii. *See* 18 U.S.C. § 2702 (c).

xxxviii. *See* 18 U.S.C. § 2703 (c).

xxxix. "The issuance of a subpoena duces tecum ... is purely a ministerial act and does not constitute legal process in the sense that it entitles the person on whose behalf it is issued to obtain access to the records described therein until a judicial determination has been made that the person is legally entitled to receive them." (*People v. Blair, supra,* 25 Cal.3d 640, 651.)

xl. Cal. Const., art. I, § 13; *People v. Chapman, supra,* 36 Cal.3d 98, 105-106, 110 [the government is seeking the name and address of a person in order to provide an essential link to establish a "virtual current biography." Thus, protection of the individual's name and address is the only way to protect the 'virtual current biography]; *People v. Blair, supra,* 25 Cal.3d 640, 748-755; *Carlson v. Superior Court* (1976) 58 Cal.App.3d 13, 21-23; *See also* California Public Utilities Rule 35.

xli. Because use of a subpoena does not violate the Fourth Amendment, the exclusionary rule is not applicable. (*People v. Bencomo* (1985) 171 Cal.App.3d 1005, 1014-1015 [federal exclusionary rules do not require suppression of unlisted telephone subscriber information obtained without warrant]. Nevertheless, California law still governs the scope of lawful searches and seizures in this state and law enforcement officials are still required to follow that law. (*People v. McKay, supra*, 27 Cal.4th 601; *People v. Larkin, supra*, 194 Cal.App.3d 650, 654; *cf. United States v. Leon* (1984) 468 U.S. 897, 104 S.Ct. 3405, 3411-3412, 82 L.Ed.2d 677 [constitutional invasion of rights is fully accomplished by unlawful search or seizure itself, not by subsequent admission of evidence].)

xlii. *See* 18 U.S.C. §§ 2703(b)(1)(B), 2705.

xliii. *See* 18 U.S.C. §§ 2703(b)(1)(B), 2705 (a)(4).

xliv. *Id.*

xlv. The government must send a copy of the request or process used as well as notifying the subscriber why the notice was delayed. *See* 18 U.S.C. § 2703(a)(5).

xlvi. 18 U.S.C. §§ 2703(d).

xlvii. *Id.*

xlviii. 18 U.S.C. §§ 2703(a).

xlix. *See* 18 U.S.C. § 2703(b)(1)(A).

l. *See* 18 U.S.C. §§ 2703(b)(1)(A), 2705(a).

li. *See United States v. Kennedy* (2000) 81 F.Supp. 2d 1103.

lii. *See* 18 U.S.C. §§ 2707, 2708.

liii. *See* 18 U.S.C. § 2707(e) - *Defense. A good faith reliance on -(1) a court warrant or order, a grand jury subpoena, legislative authorization, or a statutory question; . . . is a complete defense to any civil or criminal action brought under this chapter or any other law.*

liv. *See* 42 U.S.C. §§ 2000aa et seq. For a succinct summary of the history of the PPA, see *Depugh v. Sutton* (1996) 917 F.Supp. 690. For an overview of both the PPA and state law, see Jerry P. Coleman, *The Prosecution Versus the Press: A Historical and Personal Perspective*, The Califonia District Attorney's Association's Quarterly Journal, Vol. XXI, No. 3 (1999).

lv. *Delaney v. Superior Court* (1990) 50 Cal.3d 785, 796-797.

lvi. *See* 42 U.S.C. §§ 2000aa et seq

lvii. 42 U.S.C. §§ 2000aa (b). This applies to "documentary materials" as defined by 42 U.S.C. §§ 2000aa-7(a).

lviii. *See United States v. Hunter* (D. Vt. 1998) 13 F.Supp. 2d 574.

lix. *U.S. v Hunter* (D. Vt. 1998) 13 F. Supp.2d 574, 582; See also *Capra v. Smith* (9th Cir. 2000 - unpublished) 208 F.3d 220

lx. *See Steve Jackson Games, Inc. v. United States Secret Service* (1994) 816 F.Supp. 432.

lxi. *See* 42 U.S.C. §§ 2000aa-6(a),(d),(e); *Davis v. Gracey* (10th Cir. 1997) 11 F.3d 1472, 1482.

lxii. *See* 42 U.S.C. §§ 2000aa-6(f).

lxiii. *See* 42 U.S.C. §§ 2000aa-6(b).

lxiv. *See* 42 U.S.C. §§ 2000aa-6(c).

lxv. *See State v. One (1) Pioneer CD_ROM Changer* (1994) 891 P.2d 600, 607, cited in Stephen K. Bayens, *The Search and Siezure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 Drake L.Rev. 239 (2000).