

**OFFICE OF THE DISTRICT ATTORNEY
COUNTY OF VENTURA**

MCLE AGENDA

Admitting Digital Evidence and Cal ECPA Update

February 13, 2017

HOA: Lower Assembly Room

Instructor: Senior Deputy District Attorney Howard Wise
Senior Deputy District Attorney Marc Leventhal

- | | |
|-----------------|--|
| (10:00– 10:20) | Cal ECPA Update- Leventhal |
| (10:20 – 11:30) | Admitting Digital Evidence in Court-Wise |

Introducing Digital Evidence in California State Courtsⁱ

Introducing Documentary and Electronic Evidence

In order to introduce documentary and electronic evidence obtained in compliance with California Electronic Communication Privacy Act (Penal Code §§ 1546.1 and 1546.2) in court, it must have four components: 1) it must be relevant. 2) it must be authenticated. 3) its contents must not be inadmissible hearsay; and 4) it must withstand a "best evidence" objection.

If the digital evidence contains "metadata" (data about the data such as when the document was created or last accessed, or when and where a photo was taken) proponents will need to address the metadata separately, and prepare an additional foundation for it.

I. Relevance

Only relevant evidence is admissible. (Evid. Code, § 350.) To be "relevant," evidence must have a tendency to prove or disprove any disputed fact, including credibility. (Evid. Code, § 210.) All relevant evidence is admissible, except as provided by statute. (Evid. Code, § 351.)

For digital evidence to be relevant, the defendant typically must be tied to the evidence, usually as the sender or receiver. With a text message, for example, the proponent must tie the defendant to either the phone number that sent, or the phone number that received, the text. If the defendant did not send or receive/read the text, the text-as-evidence might lack relevance. In addition, evidence that the defendant is tied to the number can be circumstantial. And evidence that the defendant received and read a text also can be circumstantial.

Theories of admissibility include:

- Direct evidence of a crime
- Circumstantial evidence of a crime
- Identity of perpetrator
- Intent of perpetrator
- Motive
- Credibility of witnesses
- Impeachment
- Negates or forecloses a defense
- Basis of expert opinion
- Lack of mistake

II. Authentication

To "authenticate" evidence, you must introduce sufficient evidence to sustain a finding that the writing is what you say it is. (Evid. Code, § 1400 (a).) You need not prove the genuineness of the evidence, but to authenticate it, you must have a witness lay basic foundations for it. In most cases you do this by showing the writing to the witness and asking, "what is this?" and "how do you know that?" It is important to note that the originator of the document is not required to testify. (Evid. Code, § 1411.)

The proponent should present evidence of as many of the grounds below as possible. However, no one basis is required. Additionally, authentication does not involve the truth of the document's content, rather only whether the document is what it is claimed to be. (*City of Vista v. Sutro & Co.* (1997) 52

Cal.App.4th 401, 411-412.) Digital evidence does not require a greater showing of admissibility merely because, in theory, it can be manipulated. Conflicting inferences go to the weight not the admissibility of the evidence. (*People v. Goldsmith* (2014) 59 Cal. App.258, 267) *In Re KB* (2015) 238 Cal.App.4th 989, 291-292 [upholding red light camera evidence].) *Goldsmith* superseded *People v. Beckley* (2010) 185 Cal. App.4th 509, which required the proponent to produce evidence from the person who took a digital photo or expert testimony to prove authentication. Documents and data printed from a computer are considered to be an "original." (Evid. Code 255.)

Printouts of digital data are presumed to be accurate representation of the data. (Evid Code §§ 1552, 1553.) However, that presumption can be overcome by evidence presented by the opposing party. If that happens, the proponent must present evidence showing that by a preponderance, the printouts are accurate and reliable. (*People v. Retke* (2015), 232 Cal. App. 4th 1237 [successfully challenging red light camera data].)

A. You can authenticate documents by:

- Calling a witness who saw the document prepared. (Evid. Code, § 1413.)
- Introducing an expert handwriting comparison. (Evid. Code, § 1415.)
- Asking a lay witness who is familiar with the writer's handwriting to identify the handwriting. (Evid. Code, § 1516.)
- Asking the finder of fact (i.e. the jury) to compare the handwriting on the document to a known exemplar. (Evid. Code, § 1470.)
- Showing that the writing refers to matters that only the writer would have been aware. (Evid. Code, § 1421.)
- Using various presumptions to authenticate official records with an official seal or signature. (Evid. Code, § 1450-1454.) Official records would include state prison records, Department of Motor Vehicle documents or documents filed with the Secretary of State. There is a presumption that official signatures are genuine. (Evid. Code, § 1530, 1453.)
- Any other way that will sustain a finding that the writing is what you say it is. The Evidence Code specifically does not limit the means by which a writing may be authenticated and proved. (Evid. Code, § 1410; See also *People v. Olguin* (1994) 31 Cal.App.4th 1355, 1372-1373 [rap lyrics authenticated in gang case even though method of authentication not listed in Evidence Code].)

B. Common ways to authenticate email include:

- Chain of custody following the route of the message, coupled with testimony that the alleged sender had primary access to the computer where the message originated.
- Security measures such as password-protections for showing control of the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- The content of the email writing refers to matters that only the writer would have been aware.

- Recipient used the reply function to respond to the email; the new message may include the sender's original message.
- After receipt of the email, the sender takes action consistent with the content of the email.
- Comparison of the e-mail with other known samples, such as other admitted e-mails.
- E-mails obtained from a phone, tablet or computer taken directly from the sender/receiver, or in the sender/receiver's possession.

In the majority of cases a variety of circumstantial evidence establishes the authorship and authenticity of a computer record. For further information, please consult *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <<http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>> (accessed Aug. 18, 2016). See also, *Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241F.R.D. 534, 546 [seminal case law on authenticating digital evidence under F.R.E.].)

C. Common ways to authenticate chat room or Internet relay chat (IRC) communication include:

- Evidence that the sender used the screen name when participating in a chat room discussion. For example, evidence obtained from the Internet Service Provider that the screen name, and/or associated internet protocol (IP address) is assigned to the defendant or evidence circumstantially tying the defendant to a screen name or IP address.
- Security measures such as password-protections for showing control of the account of the sender and excluding others from being able to use the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- The sender takes action consistent with the content of the communication.
- The content of the communication identifies the sender or refers to matters that only the writer would have been aware.
- The alleged sender possesses information given to the user of the screen name (contact information or other communications given to the user of the screen name).
- Evidence discovered on the alleged sender's computer reflects that the user of the computer used the screen name. (See *U.S. v. Tank* (9th Cir. 2000) 200 F.3d 627.)
- Defendant testified that he owned account on which search warrant had been executed, that he had conversed with several victims online, and that he owned cellphone containing photographs of victims, personal information that defendant confirmed on stand was consistent with personal details interspersed throughout online conversations, and third-party service provider (Facebook) provided certificate attesting to chat logs' maintenance by its automated system. (*U.S. v. Browne* (3d Cir. Aug.25, 2016) 2016 WL 4473226, at 6.)

In the majority of cases it is a variety of circumstantial evidence that provides the key to establishing the authorship and authenticity of a computer record. For further information, please consult *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009)

<<http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>> (accessed Aug. 18, 2016.)

D. Common ways to authenticate social media postings include:

- Testimony from a witness, including a police officer, with training and experience regarding the specific social media outlet used testified about what s/he observed. (*In re K.B.* (2015) 238 Cal.App.4th 989.) What is on the website or app, at the time the witness views it, should be preserved in a form that can be presented in court.
- Evidence of social media postings obtained from a phone, tablet or computer taken directly from the sender/receiver, or in the sender/receiver's possession.
- Testimony from the person who posted the message.
- Chain of custody following the route of the message or post, coupled with testimony that the alleged sender had primary access to the computer where the message originated.
- The content of the post refers to matters that only the writer would have been aware.
- After the post on social media, the writer takes action consistent with the content of the post.
- The content of the post displays an image of the writer. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- Other circumstantial evidence including that the observed posted images were later recovered from suspect's cell phone and the suspect was wearing the same clothes and was in the same location that was depicted in the images. (*In re K.B.* (2015) 238 Cal.App.4th 989.)
- Security measures for the social media site such as passwords-protections for posting and deleting content suggest the owner of the page controls the posted material. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.)

In the majority of cases it is a variety of circumstantial evidence that provides the key to establishing the authorship and authenticity of a computer record. "Mutually reinforcing content" as well as "pervasive consistency of the content of the page" can assist in authenticating photographs and writings. (*People v. Valdez* (2011) 201 Cal.App.4th 1429, 1436.) For further information, please consult *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009)

<<http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>> (accessed Aug. 18, 2016.) For examples of sufficient circumstantial evidence authenticated social media posts see, *Tienda v. State* (Tex. Crim. App. 2012) 358 S.W.3d 633, 642; *Parker v. State* (Del. 2014) 85 A.3d 682, 687. Contrast, *Griffin v. State* (2011) 419 Md. 343, 356–359.

E. Common ways to authenticate web sites include:

- Testimony from a witness, including a police officer about what s/he observed. (See *In re K.B.* (2015) 238 Cal.App.4th 989.) What is on the website or app, at the time the witness views it, should be preserved in a form that can be presented in court.
- Testimony from the person who created the site.
- Website ownership/registration. This is a legal contract between the registering authority (e.g. Network Solutions, PDR Ltd, D/B/A PublicDomainRegistry.com, etc.) and the website owner, allowing the registered owner to have total dominion and control of the use of a website name (domain) and its content. (See *People v. Valdez* (2011) 201 Cal.App.4th 1429 [password protection suggest the owner of the page controls the posted material].) It may be possible to admit archived versions of web site content, stored and available at a third party web site (See <https://archive.org/web/> [Wayback Machine].) First, it may be authenticated by a percipient witness who previously saw or used the site. It may also be possible to obtain a declaration or witness to testify to the archive. (See e.g. *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740, at 16 (N.D.Ill. Oct. 15, 2004) [analyzing admissibility of the content of an archived website].)

The underlying challenge for web sites is not the authentication of the site; rather the content or hearsay material contained therein. In *St. Clair v. Johnny's Oyster & Shrimp, Inc.* (S.D.Tex.1999) 76 F.Supp.2d 773, 774-75 the court noted that "voodoo information taken from the Internet" was insufficient to withstand motion to dismiss because "[n]o web-site is monitored for accuracy" and "this so-called Web provides no way of verifying the authenticity" of information plaintiff wished to rely on. (See also *Badasa v. Mukasey* (8th Cir. 2008) 540 F.3d 909 [Nature of Wikipedia makes information from the website unreliable].) However, as noted in *Section III Hearsay*, the contents of the web site could be admitted as an operative fact or under a number of exceptions including an admission of a party opponent.

F. Authenticating Texts:

A text message is a writing within the meaning of Evidence Code section 250, which may not be admitted in evidence without being authenticated. (*Stockinger v. Feather River Community College* (2003) 111 Cal.App.4th 1014, 1027–1028.) A text message may be authenticated "by evidence that the writing refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the proponent of the evidence to be the author of the writing" (Evid.Code, § 1421), or by any other circumstantial proof of authenticity (*Id.*, § 1410).

As of August 2016, there are no published California cases that specifically discuss what is required for authenticating a text message. Unpublished California opinions are consistent with the rule set forth above for authenticating e-mails and chats through a combination of direct and circumstantial evidence based on the facts of the case. Because of the mobile nature of smart phones, the proponent must take care to tie the declarant to the phone from which texts were seized or to the phone number listed in records obtained from the phone company. Often this is done through cell phone records or the phone being seized from the defendant, his home or car or other witnesses testifying that this was how they communicated with the defendant.

Published opinions from other jurisdictions and unpublished opinions from California provide some guidance:

- Victim testified he knew the number from which text was sent because Defendant told him the number. The contents of the texts referred to victim as a snitch. The defendant called the victim during the course of the text message conversation. [(*Butler v. State*, 459 S.W. 3d 595 (Crim. Ct App. Tx. April 22, 2015).)]
- Testimony of records custodian from telecommunications company, explaining how company kept records of actual content of text messages, the date and time text messages were sent or received, and the phone number of the individuals who sent or received the messages, provided proper foundation for, and sufficiently authenticated, text messages admitted into evidence in trial on armed robbery charges. (Fed.Rules Evid.Rule 901(a), *U.S. v. Carr* (11th Cir. 2015) 607 Fed.Appx. 869.)
- Ten of 12 text messages sent to victim's boyfriend from victim's cellular telephone following sexual assault were *not* properly authenticated to extent that State's evidence did not demonstrate that defendant was author of text messages. (*Rodriguez v. State* (2012) 128 Nev. Adv. Op. 14, [273 P.3d 845].)
- Murder victim's cell phone recovered from scene of crime. Forensic tools used on phone recovered texts back and forth between victim and defendant. (*People v. Lehmann* (Cal. Ct. App., Sept. 17, 2014, No. G047629) 2014 WL 4634272 [Unpublished].)
- Defendant laid an inadequate foundation of authenticity to admit, in prosecution for assault with a deadly weapon, hard copy of e-mail messages (Instant Messages) between one of his friends and the victim's companion, as there was no direct proof connecting victim's companion to the screen name on the e-mail messages. (*People v. Von Gunten* (2002 Cal.App.3d Dist.) 2002 WL 501612. [Unpublished].)

G. Authenticating Metadata:

Another way in which electronic evidence may be authenticated is by examining the metadata for the evidence. Metadata, "commonly described as 'data about data,' is defined as 'information describing the history, tracking, or management of an electronic document.' Metadata is 'information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information).' Some examples of metadata for electronic documents include: a file's name, a file's location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept." Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Federal Rule 901(b)(4).

Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because, "[a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide authorization for selected network administrators to override an individual password identification number to gain access when necessary. Metadata markers can reflect that a document was modified when in fact it simply was saved to a different location. Despite its lack of conclusiveness, however, metadata certainly is a

useful tool for authenticating electronic records by use of distinctive characteristics.” (*Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 547–48 [citations omitted].)

F. Challenges to Authenticity

Challenges to the authenticity of computer records often take on one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created.

Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. California state courts have refused to require, as a prerequisite to admission of computer records, testimony on the “acceptability, accuracy, maintenance, and reliability of ... computer hardware and software.” (*People v. Lugashi* (1988) 205 Cal.App.3d 632, 642.) As *Lugashi* explains, although mistakes can occur, “ ‘such matters may be developed on cross-examination and should not affect the admissibility of the [record] itself.’ ” (*People v. Martinez* (2000) 22 Cal.4th 106, 132.)

Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author. For further information, please consult “Defeating Spurious Objections to Electronic Evidence,” by Frank Dudley Berry, Jr., [\[click here\]](#) or *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <<http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>> (accessed Aug. 18, 2016).

III. Hearsay Rule

The first question to ask is whether or not the information within the document is hearsay. If it is hearsay, then you need an applicable exception, such as business and government records or statement by party opponent. Examples of things that are *not* hearsay include; 1) operative facts and 2) data that is generated by a mechanized process and not a human declarant and, 3) A statement being used to show its falsity not its truth.

A. Operative Facts

Where “ ‘the very fact in controversy is whether certain things were said or done and not ... whether these things were true or false, ... in these cases the words or acts are admissible not as hearsay[,] but as original evidence.’ ” (1 Witkin, *Cal. Evidence* (4th ed. 2000) Hearsay, § 31, p. 714.) For example, in an identity theft prosecution, there will be no hearsay issue for the majority of your documents. The documents are not being offered for the truth of the matter asserted; they are operative facts. In *Remington Investments, Inc v. Hamedani* (1997) 55 Cal.App.4th 1033, the court distinguished between the concept of authentication and hearsay. The issue was whether a promissory note was admissible. The court observed that: ‘The Promissory Note document itself is not a business record as that term is used in the law of hearsay, but rather an operative contractual document admissible merely upon adequate evidence of authenticity. (*Id.* At 1043.)

Under *Remington*, promissory notes, checks and other contracts are not hearsay, but operative facts. Moreover, forged checks, false applications for credit, and forged documents are not hearsay. They

are not being introduced because they are true. They are being introduced because they are false. Since they are not being introduced for the truth of the matter asserted there is no hearsay issue.

Other examples of non-hearsay documents would include:

- The words forming an agreement are not hearsay (*Jazayeri v. Mao* (2009) 174 Cal.App.4th 301, 316 as cited by *People v. Mota* (Cal. Ct. App., Oct. 8, 2015, No. B252938) 2015 WL 5883710 (Unpublished))
- A deposit slip and victim's identification in a burglary case introduced to circumstantially connect the defendant to the crime. (*In re Richard* (1979) 91 Cal.App.3d 960, 971-979.)
- Pay and owes in a drug case. (*People v. Harvey* (1991) 233 Cal.App.3d 1206, 1222-1226.)
- Items in a search to circumstantially connect the defendant to the location. (*People v. Williams* (1992) 3 Cal.App.4th 1535, 1540-1543.)
- Invoices, bills, and receipts are generally hearsay unless they are introduced for the purpose of corroborating the victim's damages. (*Jones v. Dumrichob* (1998) 63 Cal.App.4th 1258, 1267.)
- Defendant's social media page as circumstantial evidence of gang involvement. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- Logs of chat that was attributable to Defendant were properly admitted as admissions by party opponent, and the portions of the transcripts attributable to another person were properly classified as "non hearsay", as they were not "offered for the truth of the matter asserted." Replacing screen names with actual names appropriate demonstrative evidence. (*U.S. v. Burt* (7th Cir., 2007) 495 F.3d 733.)
- "To the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all—and thus fall outside the ambit of the hearsay rule." (*Perfect 10, Inc. v. Cybernet Ventures, Inc.* (C.D.Cal.2002) 213 F.Supp.2d 1146, 1155.)
- Generally, photographs, video, and instrument read outs are not statements of a person as defined by the Evidence Code. (Evid.Code §§ 175, 225; *People v. Goldsmith* (2014) 59 Cal.4th 258, 274; *People v. Lopez* (2012) 55 Cal.4th 569, 583.)

Although the check itself is not hearsay, the bank's notations placed on the back of the check showing that it was cashed is hearsay. The bank's notations would be introduced for the truth of the matter asserted – that the check was cashed. Evidence Code sections 1270 and 1271 solve this problem by allowing the admission of these notations as a business record.

Two helpful rules that apply to business records. First, it may be permissible to infer the elements of the business record exception. In *People v. Dorsey* (1974) 43 Cal.App.3d 953, the court was willing to find that it was common knowledge that bank statements on checking accounts are prepared daily on the basis of deposits received, checks written and service charges made even though the witness failed to testify as to the mode and time of preparation of bank statements. The second rule is that

"lack of foundation" is not a sufficient objection to a business record. The defense must specify which element of the business record exception is lacking. (*People v. Fowzer* (1954) 127 Cal.App.2d 742.)

B. Computer Records Generated by a Mechanized Process

The first rule is that a printout of the results of the computer's internal operations is not hearsay evidence because hearsay requires a human declarant. (Evid.Code §§ 175, 225.) The Evidence Code does not contemplate that a machine can make a statement. (*People v. Goldsmith* (2014) 59 Cal.4th at 258, 274 [rejecting hearsay claims related to red light cameras]; *People v. Hawkins* (2002) 98 Cal.App.4th 1428; *People v. Lopez* (2012) 55 Cal. 4th 569). These log files are computer-generated records that do not involve the same risk of observation or recall as human declarants. Thus, email header information and log files associated with an email's movement through the Internet are not hearsay. The usual analogy is that the clock on the wall and a dog barking are not hearsay. An excellent discussion on this issue can be found in *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <<http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>> (accessed Aug. 18, 2016) Metadata such as date/time stamps are not hearsay nor do they violate the confrontation clause because they are not testimonial. (See, *People v. Goldsmith* 59 Cal.4th at 258, 274-275; *People v. Lopez* (2012) 55 Cal. 4th 569, 583.)

C. Business Records

Log files and other computer-generated records from Internet Service Providers may also easily qualify under the business records exception to the hearsay rule. (Evid.Code §§1270, 1271, 1560, 1561.) Remember, you do not need to show the reliability of the hardware or software. (*People v. Lugashi* (1988) 205 Cal.App.3d 632.) Nor does the custodian of records need to completely understand the computer. (*Id.*) Additionally, the printout (as opposed to the entry) need not be made "at or near the time of the event." (*Aguimatang v. California State Lottery* (1991) 234 Cal.App.3d 769.) Finally, a cautionary note from the Appellate Court in *People v. Hawkins* (2002) 98 Cal.App.4th 1428: "the true test for admissibility of a printout reflecting a computer's internal operations is not whether the printout was made in the regular course of business, but whether the computer was operating properly at the time of the printout."

If the computer is used merely to store, analyze, or summarize material that is hearsay in nature, it will not change its hearsay nature and you will need an applicable exception for introduction. Common exceptions for the contents of email include: statement of the party, adoptive admission, statement in furtherance of a conspiracy, declaration against interest, prior inconsistent statement, past recollection recorded, business record, writing as a record of the act, or state of mind.

Note also that records obtained by search warrant, and accompanied by a complying custodian affidavit, are admissible as if they were subpoenaed into court (Evid. Code §§ 1560-1561, effective January 1, 2017) and records obtained from an Electronic Communication Service provider that is a foreign corporation, and are accompanied by a complying custodian affidavit, are currently admissible pursuant to Penal Code § 1524.2(b)(4). (See also Pen. Code § 1546.1(d)(3).)

D. Government Records

An official record is very similar to a business record, even if it is obtained from a government website. The chief difference is that it may be possible to introduce an official record without calling the custodian or another witness to authenticate it. (Evid. Code, § 1280; See *Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 548-49; *EEOC v. E.I duPont de Nemours & Co.* (2004) 65 Fed. R. Evid. Serv. 706 [Printout from Census Bureau web site containing domain address from which

image was printed and date on which it was printed was admissible in evidence].) The foundation can be established through other means such as judicial notice or presumptions. (*People v. George* (1994) 30 Cal.App.4th 262,274.)

E. Published Tabulations

Prosecutors are often plagued with how to introduce evidence that was found using Internet-based investigative tools. For example, if your investigator used the American Registry For Internet Numbers (ARIN) programs (WHOIS, RWhois or Routing Registry Information), how is this admissible without calling the creator of these Internet databases? Evidence Code Section 1340 allows an exception to the hearsay rule, which allows the introduction of published tabulations, lists, directories, or registers. The only requirement is that the evidence contained in the compilation is generally used and relied upon as accurate in the course of business.

Note that not all data aggregation sites may have the proper characteristics for this exception. In *People v. Franzen* (2012) 210 Cal.App.4th 1193, 1209–13, the court found that a subscription based service did not possess the characteristics that would justify treating its contents as a published compilation for purposes of section 1340

IV. Former Best Evidence Rule

Reminder: The Best Evidence Rule has been replaced in California with the Secondary Evidence Rule. The Secondary Evidence Rule allows the admissibility of copies of an original document. (Evid. Code, § 1521.) They are not admissible, however, if "a genuine dispute exists concerning material terms of the writing and justice requires the exclusion," or if admitting the evidence would be "unfair." (Evid. Code, § 1521.)

In a criminal action it is also necessary for the proponent of the evidence to make the original available for inspection at or before trial. (Evid. Code, § 1522.) For email or any electronic document, this is especially important, given the wealth of information contained in its electronic format, as opposed to its paper image.

Of interest, Evidence Code Section 1522 requires that the "original" be made available for inspection. Evidence Code Section 255 defines an email "original" as any printout shown to reflect the data accurately. Thus, the protections offered by Evidence Code Section 1522 are stripped away by Evidence Code Section 255. This is where the protections of Evidence Code Section 1521 are invoked: "It's unfair, your Honor, not be able to inspect the email in its original format."


Also, remember that Evidence Code Section 1552 states that the printed representation of computer information or a computer program is presumed to be an accurate representation of that information. Thus, a printout of information will not present any "best evidence rule" issues absent a showing that the information is inaccurate or unreliable.

Oral testimony regarding the content of an email [writing] is still inadmissible absent an exception. (Evid. Code, § 1523.) Exceptions include where the original and all the copies of the document were accidentally destroyed.

Of course, none of the above rules applies at a preliminary hearing. (See Pen. Code § 872.5 [permits otherwise admissible secondary evidence at the preliminary hearing]; B. Witkin, 2 California Evidence (3rd ed., 1986) § 932, p. 897 ["secondary evidence" includes both copies and oral testimony].)

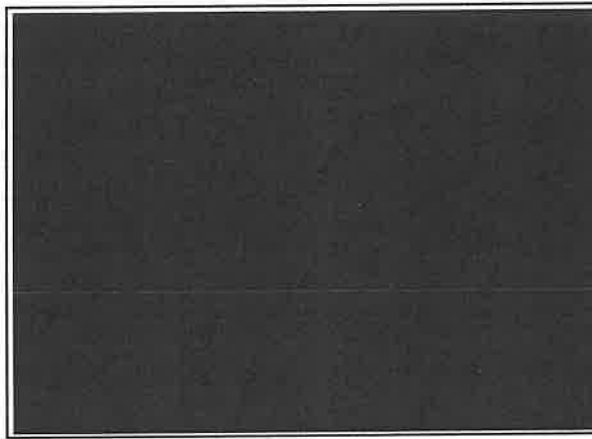
¹ This material was prepared by Robert M. Morgester, Senior Assistant Attorney General, California Department of Justice in 2003 for the *High-Technology Crime: Email and Internet Chat Resource CD-ROM*, and draws heavily upon *Documentary Evidence Primer*, by Hank M. Goldberg, Deputy District Attorney, Los Angeles County District Attorney's Office, January 1999. Material from that document was used with Mr. Goldberg's permission. This material was updated in 2016 by Robert Morgester and Howard Wise, Senior Deputy District Attorney, Ventura County District Attorney's Office.

Admitting Digital Evidence



Presented by:
Howard Wise, Senior Deputy District Attorney
Ventura County District Attorney's Office
(805) 662-1736
Howard.wise@ventura.org
February 13, 2017- VCD AO

October 2010



Thanks to:

- Justin Fitzsimmons, SEARCH
- Robert Morgester, California AGO
- Everyone on Digital DA Listserv
- AUTHORS OF WRITTEN MATERIALS

Disclaimer

- The opinions expressed are my personal opinions and not the official positions of the Ventura County DA's Office.
- The challenges of applying brick and mortar law to cyberspace will cause the law to evolve.
- Advice will necessarily be factbased, upon prevailing and often conflicting law.
- Consult your own legal counsel for legal advice

Written Materials on CD

- **Introducing Digital Evidence in California State Courts (Morgester and Wise)**
- **Digital Evidence chapter(2016) from Jefferson's CA Evidence Benchbook.**
- **Hot off the Press: *People v. Goldsmith* Provides a Roadmap for Authenticating Digital Evidence, CDAAs Firewall article.**
- **All case opinions from this lecture**
- **This powerpoint**

Key cases

- California (and other important) cases^(v.7/25/15)
- **People v. Goldsmith**- CA Supreme case on admitting digital evidence in general and automatic traffic cameras specifically.
- **In re KB**- foundation needed for Instagram records post Goldsmith (*July 2015*)
- **Beckley and Valdez**- Two cases pre-Goldsmith that discuss admitting Facebook records.
- **Kinda v. Carpenter**- most recent case reinforces conflicting inferences go to weight not admissibility"

A Digital Document must be ALL of the following

- Relevant, AND
 - Might not be relevant if you cannot show D received or sent the communication.
- Authenticated, AND
 - It is what it purports to be
- An exception to the Hearsay rule
 - or NOT Hearsay

Motion in limine

- Better resolved by Pre-trial Motion *in Limine*.
- Authentication- is document what it purports to be.
- Preponderance of the evidence.
- Can a reasonable juror find that it is what it purports to be.
- Essentially, what is necessary is a prima facie case.

- "As long as the evidence would support a finding of authenticity, the writing is admissible. The fact conflicting inferences can be drawn regarding authenticity goes to the document's weight as evidence, not its admissibility.
 - People v. Goldsmith

**Best Evidence Rule
(Can NOT be ignored)**

**Digital Evidence
No Best Evidence Rule**

- California has rejected the best evidence rule in favor of the secondary evidence rule—Evidence Code sections 1552 and 1553 (*Goldsmith*)
 - a printout of a video is presumed to be reliable unless the opponent of the evidence can show unreliability.
 - If unreliability is shown, then the burden of proof switches back to the proponent to prove reliability by a preponderance of the evidence.

CAUTION
**The Presumption of Authenticity Can Shift
back to the proponent**
- People v. Retke(2015)

232 Cal. App. 4th 1237

- Defendant had an expert that had done testing that indicated a problem with the timing on a printout of an Automatic Traffic Camera.
- HELD: The presumption of authenticity of a printout can be overcome by evidence presented by the opposing party. If that happens, the proponent must present evidence showing that by a preponderance, the printouts are accurate and reliable.

Relevance

Cases and Evidence Codes for Relevance

– Relevant

- To be Relevant, evidence has to be tied to the Defendant
- But See *Kinda v. Carpenter* (2016) 247 Cal.App.4th 1268, 1286 (civil case where Court was wrong to exclude Yelp postings not perfectly tied to the defendant)

Relevance Sections

- Evidence Code section 350 and 351- only relevant evidence is admissible and all relevant evidence is admissible.
- Evidence Code section 210 – relevant means having a tendency to prove or disprove any disputed fact, including credibility
 - » Direct evidence of a crime
 - » Circumstantial evidence of a crime
 - » Identity
 - » Intent of perpetrator
 - » Motive
 - » Credibility of a witness
 - » Negate a defense
 - » Basis of expert opinion
 - » Lack of mistake

Authentication (General Principles)

Authentication

- Better resolved by pre-trial Motion *in Limine*.
- Standard - is the document what it purports to be.
 - Preponderance of the evidence.
 - Can a reasonable juror find that it is what it purports to be.
 - Essentially, what is necessary is a *prima facie* case.

Authentication and Digital Evidence (Photos/Automated Traffic Cameras)

- *People v. Goldsmith* is the lead case
- "As long as the evidence would support a finding of authenticity, the writing is admissible. The fact conflicting inferences can be drawn regarding authenticity goes to the document's weight as evidence, not its admissibility.

People v. Goldsmith (2014) 59 Cal.4th 258, 267

Goldsmith Superseded

People v. Beckley

- Beckley is a case often cited by the defense excluded social media evidence.
- And Westlaw does not give it a red flag.
- BUT Goldsmith was interpreted by another CA Appeals Court as superseding Beckley:

To the extent *Beckley* can be read as requiring testimony of the person who actually created and uploaded the image, or testimony from an expert witness that the image has not been altered, we cannot endorse it. Such an analysis also appears to be inconsistent with the most recent language in *Goldsmith* – In re KB (2015) 238 Cal.App.4th 989

Authentication and Digital Evidence (photos)

- Proof may be supplied by:
 - other witness testimony;
 - circumstantial evidence;
 - content, and;
 - location.
- Authentication can also be established "by any other means provided by law" (Evid. Code § 1400), including a statutory presumption such as Evidence Code sections 1552 and 1553.

- We decline to require a greater showing of authentication for the admissibility of digital images merely because in theory they can be manipulated. [Citation omitted.] We have not required testimony regarding the 'acceptability, accuracy, maintenance, and reliability of ... computer hardware and software' in similar situations.

- *Goldsmith*, *supra*, at 27, referring to *People v. Martinez* (2000) 22 Cal.4th 106, 132, quoting *Lugashi*, *supra*, at 642; accord, *People v. Nazary* (2010) 191 Cal.App.4th 727, 755.
- See, material copies of *Lugashi* and *Nazary*

Admission of Digital Evidence

- Circumstantial evidence may establish the authorship and authenticity of a computer record
U.S. v. Siddiqui (11th Cir. 2000) 235 F.3d 1318.
- Should be some evidence as to the SECURITY of the website/email system including password protections and exclusive access by the author.
– *Commonwealth v. Williams*, in the materials
- And "pervasive consistency" of the content, "filled with personal photographs, communications, and other details tending together to identify and show owner-management of [the social media] page devoted to gang-related interests."
• *People v. Valdez* (2011) 201 Cal.App.4th 1429

Personal Knowledge that D is the writer of the content can also come from the D's phone/computer

- Forensics can show circumstantially that D is the writer.
- D's statements can show he is the writer
- Contextual info and date/time stamps from computer.
- External evidence that D was only one that had access.
– Ex. Electronic key access records of other persons w/access.

Witnesses Needed to Authenticate Digital Evidence

A witness's testimony is still usually
needed to show authentication

- In *Goldsmith* a traffic officer familiar with the ATES system was required.
 - However, testimony from the company that developed and operates the ATES software was not required.
 - Note the strong affirmation of *People v. Lugashi* (1988) 205 Cal.App.3d 632; and *People v. Hawkins* (2002) 98 Cal.App.4th 1428
- In re KB – An officer very familiar with Instagram and familiar with Cellebrite was enough.

Authentication by Custodian's Affidavit

Law Change
Documents received by Search Warrant
AND
Custodian AFFIDAVIT

- SW records Admitted the same as records received by Subpoena Duces Tecum
- Now no need to re-subpoena documents received by search.
- Do not have to go to Clerk like SDT records.
- Amended Evidence Code sections 1561-1563.
 - See also, PC 1524.2(b)(4) for ECS records.
- Leg. history makes clear LE does not pay for copies obtained by SW and SDT in CA.

Business records via Custodian AFFIDAVIT NOT always self-authenticating

- In very limited instances authentication can be shown based on a CUSTODIAN'S AFFIDAVIT/Self Authentication.
 - But admissible items may be limited to "normal business functions made reliable by repetition, including":
 - Date and time message was sent or posted
 - Address on file for message or post
- BUT NOT: the CONTENT of message without OTHER circumstantial means of showing the content is reliable.**

See United States v. Givens (3d Cir., Aug. 23, 2016, No. 14-1190) 2016 WL 4473226 (13 page was not self-authenticating as a business record but was authenticated by other means)

Do Not be afraid to draft your OWN tailored Custodian's Affidavit

- For use with a COOPERATIVE Electronic Service Provider (ESP).
- They will be cooperative if the ESP's other option is sending a witness.
- Get language from ESP employees.
- Leave time for their lawyers to review.
- KEY: DETAILED description identifying records and MODE OF PREPARATION

Sample Expanded Custodian Affidavit See, DDA Wise

- Statement how the ESP relies on the trustworthiness of the records (Evid. C. 1271)
- Detailed description of how the records were maintained.
- What the acronyms in the records mean.
- Anything else the Custodian would testify to if called to court.

Authentication by Employee of
Facebook, Google, Verizon etc.
(ECS)

Prove Authentication by a Custodian or
other ECS employee

1. Using an ECS Employee to Prove how the
ECS works.

- Evid. Code 1271 allows a custodian or other **QUALIFIED WITNESS** testifies to the identity and mode of preparation.
- It can be any employee generally familiar with the way the company maintains and produces its records.
- It can be the company's security officer who does not have formal computer training.
- Witness can rely on hearsay conversations with other employees at the company with more experience.

- See, People v. Lugashi

People v. Lugashi (1988)
205 Cal. App.3d 632

- A person who generally understands the [record] system's operation and possesses sufficient knowledge and skill to properly use the system and explain the resultant data, even if unable to perform every task from initial design and programming to final printout, is a "qualified witness" for purposes of Evidence Code section 1271.

Authentication by Person Who made the
Social Media Post or Wrote the Email

Authentication by Personal/Direct
knowledge is NOT required

- Preferred but not required.
- Opinions often wonder why the proponent/writer is not used to authenticate the ESI.
 - Com. v. Williams; U.S. v. Safavian (2006), 435 F. Supp 36, 40.
- But, actual writer/witnesses may be hostile, undependable or be unwilling to commit to the ESI being what was written.

Authentication by
Computer Forensic Examiner

Working with the CFE to prepare for testimony

- They will teach you a lot
- Do it well in advance of testimony
- See DDA Wise for sample direct exams.
- Do you understand how forensics work?
 - Do you have recovered/deleted images
- Was evidence recovered from a cache?

Issues for DDA to Anticipate

- CHAIN OF CUSTODY
 - Do you have the right witnesses subpoenaed to show the computers the CFE examined were the ones seized from D's house?
 - The CFE on the scene might be different than the one who did the examination?
 - Might need the bag and tag cop from SW
- How are you going to going to make the exhibits?

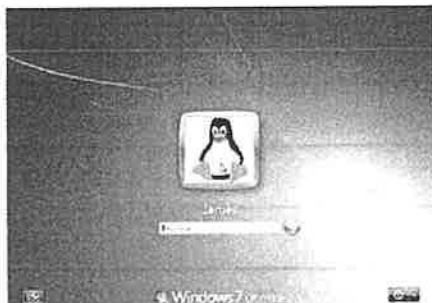
Making Digital Evidence into Exhibits

- Will it be in hard copy (paper), digital (DVD) or both?
 - Make sure the DVD is the type that works in a DVD Player (as opposed to a computer)
- Will the hard copy (paper) exhibit include the metadata?
 - Metadata such as the filepath
 - Judges go both ways on this
- PRACTICE TIP: Prepare an Ex. 1 – with no meta data and a 17A which includes metadata

Computer forensic reports can be confusing



Evidence can be displayed to show how suspect's computer looked (VMWare)



Prove Authentication by a LE Witness OK but NOT Favored

1. Using a Detective to Prove how the ECS works.
 - *Experienced* witness must have sufficient training and experience to testify they are familiar with how Instagram, Facebook etc.. works.
 - See, *In re KB in materials*.
 - Important that user needed to know the password that allowed access to the account.
 - Does NOT need to be a Facebook/Social Media employee just someone that has a reliable foundation for their opinions

Witness testimony is still needed to show authentication

- In *Goldsmith* a traffic officer familiar with the ATES system was required.
- Testimony from the company that developed and operates the ATES software was not required.
 - Note the strong affirmation of *People v. Lugashi* (1988) 205 Cal.App.3d 632; and *People v. Hawkins* (2002) 98 Cal.App.4th 1428

In re KB – A Police Officer very familiar with Instagram and familiar with Cellebrite was enough

- "Officer Steven Wood testified that after appellant and his associates were arrested, he used Cellebrite computer software technology to retrieve information from Mendez's cell phone. Once a Cellebrite search is conducted, the information in the cell phone is sent to a computer. The officer then simply pushes a button, and a Cellebrite report is generated. The report lists all of the information stored in the cell phone—photographs; incoming, outgoing, and missed calls; text messages; app information; and emails."
 - Any Cal ECPA problems with this???

LEO Shows the Data copied or obtained **RELIABLY**

- Obtaining and copying data using software to copy the website.
 - Camtasia can show you what the officer is seeing in real-time
 - Snag it is better at getting all of the hyperlinks
- Also, screen captures such as Snipping Tool and print screen
- Also, just taking photos of the screen with a digital camera.
- **NOTE: Content on webpage changes frequently, especially the Ads.**

Ways of Authenticating Digital Evidence

- IMP: Use as many methods as you can
- CA Evid. C. 1410- Authentication can be proved in any manner.

Authentication by

Comparison to Authentic Samples

- Originally involved its use for authenticating handwriting or signatures. See CAEvid. C. §1417, Fed. R. Evid. 901(b)(3).
- E-mail messages "that are not clearly identifiable on their own can be authenticated ... by comparison by the trier of fact (the jury) with 'specimens which have been [otherwise] authenticated'-in this case, those e-mails that already have been independently authenticated under Rule 901(b)(4).". *Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 546 (Seminal digital authentication case)

Authentication by Circumstantial Evidence Coupled with Distinctive Characteristics CA Evid. C. § 1421

[FRE 901(b)(4)]

- "[t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety," including authenticating an exhibit by showing that it came from a "particular person by virtue of its disclosing knowledge of facts known peculiarly to him," *Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 546
- Identified by :
 - Appearance
 - Contents
 - Substance
 - Internal Patterns
 - Other distinctive characteristics

Proving authenticity by LOCATION

- Authentication can be proved by circumstantial evidence of content and location.
- The digital records were seized from the defendant or referred to items seized from the defendant.

- *People v. Miller* (2000) 81 Cal.App.4th 1427, 1445 [deceased victim's charge account records authenticated in part because items described were found in defendant's possession];
- *U.S. v. Moran* (9th Cir.2007) 493 F.3d 1002, 1010–1011 [computer files authenticated where computer was seized from defendant's home, access to files was protected by password, one account was in defendant's name, and files contained records related to defendant's business, including data about its principals, clients and programs].
- *People v. Smith* (2009) 179 Cal.App.4th 986, 1002
- *People v. Gibson* (2001) 90 Cal.App.4th 371, 383;

Authentication by Substance Known Only to Declarant CA Evid C. § 1421

- A writing may be authenticated by evidence that the writing refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the proponent of the evidence to be the author of the writing.

Authentication by Circumstantial Evidence -Distinctive Characteristics (examples)

- Showing it came from a person b/c:
 - Discloses facts particularly known to the speaker;
 - See, *Com. v. Purdy* (email described unusual set of services provide by massage parlor)
 - See, *In the Interest of F.P.* (2005)(878 A.2d 91)(Instant Messages authenticated by specific details)
 - See, *Lorraine* at 546 for other examples

Authentication by Circumstantial Evidence Responsive documents CA Evid. C. § 1420

- A writing may be authenticated by evidence that the writing was received in response to a communication sent to the person who is claimed by the proponent of the evidence to be the author of the writing.
- Example is a responsive email.
- D's authenticated response can authenticate all of the earlier e-mails in the chain.
 - See, *U.S. v. Safavian* (2006), 435 F. Supp. 36.

Circumstantial Authentication by Metadata

- Commonly described as 'data about data,' is defined as 'information describing the history, tracking, or management of an electronic document.'
- Many potential reasons for unreliability.
- Despite its lack of conclusiveness, however, metadata is a useful tool for authenticating electronic records by use of distinctive characteristics.

Lorraine v. Markel American Ins. Co. (D. Md. 2007) 241 F.R.D. 534, 548

Authentication

Because Document is a Public Record

"[p]ublic records are regularly authenticated by proof of custody, without more.

– *Lorraine* at 548

– FRE 901(b)(7)

- Note that Public records also often have less exacting standards as a hearsay exception than the business records exception.

Other means of authenticating

– Authentication

- Evidence Code section 1400 – introduce sufficient evidence to sustain a finding that the writing is what you say it is.

- Evidence Code section 1411 – subscribing witness' testimony unnecessary

- Authentication does not involve the truth of the document's content, but rather only whether the document is what it is claimed to be *City of Vista v. Sutro & Co.* (1997) 52 Cal.App.4th 401, 411-412

- Evidence Code section 1410 – the means by which a writing may be authenticated is not limited.

Specific Ways to Authenticate an E-mail

- Chain of custody following the route of the message via Internet Protocol address, coupled with testimony that the alleged sender had primary access to the computer where the message originated.
- Security measures such as password-protections for showing control of the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- The content of the email writing refers to matters that only the writer would have been aware.

Specific Ways to Authenticate a Social Media Posting

- Testimony from a witness, including a police officer, with training and experience regarding the specific social media outlet used testified about what s/he observed. – (*In re K.B.* (2015) 238 Cal.App.4th 989.)
- What is on the website or app, at the time the witness views it, should be preserved in a form that can be presented in court.
- Evidence of social media postings obtained from a phone, tablet or computer taken directly from the sender/receiver, or in the sender/receiver's possession.

Specific Ways to Authenticate a Social Media Posting

- Testimony from the person who posted the message.
- Chain of custody following the route of the message or post, coupled with testimony that the alleged sender had primary access to the computer where the message originated.
- The content of the post refers to matters that only the writer would have been aware.
- After the post on social media, the writer takes action consistent with the content of the post.

Specific Ways to Authenticate a Social Media Posting

- The content of the post displays an image of the writer. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- Other circumstantial evidence including that the observed posted images were later recovered from suspect's cell phone and the suspect was wearing the same clothes and was in the same location that was depicted in the images. (*In re K.B.* (2015) 238 Cal.App.4th 989.)
- Security measures for the social media site such as passwords-protections for posting and deleting content suggest the owner of the page controls the posted material. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.)

Ways to Authenticate Text Messages

- Only UNpublished CA cases and cases from other jurisdictions (as of 8/16).
- Victim testified he knew the number from which text was sent because Defendant told him the number. The contents of the texts referred to victim as a snitch. The defendant called the victim during the course of the text message conversation. [(*Butler v. State*, 459 S.W. 3d 595 (Crim. Ct App. Tx. April 22, 2015).)]

Ways to Authenticate Text Messages

- Only UNpublished CA cases and cases from other jurisdictions (as of 8/16).
- Murder victim's cell phone recovered from scene of crime. Forensic tools used on phone recovered texts back and forth between victim and defendant. (*People v. Lehmann* (Cal. Ct. App., Sept. 17, 2014, No. G047629) 2014 WL 4634272 [Unpublished].)

Text- Unpublished

- Defendant laid an inadequate foundation of authenticity to admit, in prosecution for assault with a deadly weapon, hard copy of e-mail messages (Instant Messages) between one of his friends and the victim's companion, as there was no direct proof connecting victim's companion to the screen name on the e-mail messages. (*People v. Von Gunten* Unpublished (2002 Cal.App.3d Dist.) 2002 WL 501612. [].)

Authenticating Text Messages (other jurisdictions)

- Testimony of records custodian from telecommunications company, explaining how company kept records of actual content of text messages, the date and time text messages were sent or received, and the phone number of the individuals who sent or received the messages, provided proper foundation for, and sufficiently authenticated, text messages admitted into evidence in trial on armed robbery charges. (Fed.Rules Evid.Rule 901(a), *U.S. v. Carr* (11th Cir. 2015) 607 Fed.Appx. 869.)

Authenticating Text Messages (other jurisdictions)

- Ten of 12 text messages sent to victim's boyfriend from victim's cellular telephone following sexual assault were *not* properly authenticated to extent that State's evidence did not demonstrate that defendant was author of text messages. (*Rodriguez v. State* (2012) 128 Nev. Adv. Op. 14, [273 P.3d 845].)

Ways to authenticate webpages

- Testimony from a witness, including a police officer about what s/he observed. (See *In re K.B.* (2015) 238 Cal.App.4th 989.)
 - What is on the website or app, at the time the witness views it, should be preserved in a form that can be presented in court.
- Testimony from the person who created the site.
- Website ownership/registration. This is a legal contract between the registering authority (e.g. Network Solutions, PDR Ltd, D/B/A PublicDomainRegistry.com, etc.) and the website owner, allowing the registered owner to have total dominion and control of the use of a website name (domain) and its content. (See *People v. Valdez* (2011) 201 Cal.App.4th 1429 [password protection suggest the owner of the page controls the posted material].)

Ways to authenticate Chat such as Facebook Messenger or Kik

- Evidence that the sender used the screen name when participating in a chat room discussion. For example, evidence obtained from the Internet Service Provider that the screen name, and/or associated internet protocol (IP address) is assigned to the defendant or evidence circumstantially tying the defendant to a screen name or IP address.
- Security measures such as password-protections for showing control of the account of the sender and excluding others from being able to use the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- The sender takes action consistent with the content of the communication.
- The content of the communication identifies the sender or refers to matters that only the writer would have been aware.
- The alleged sender possesses information given to the user of the screen name (contact information or other communications given to the user of the screen name).

Ways to authenticate Chat such as Facebook Messenger or Kik

- The alleged sender possesses information given to the user of the screen name (contact information or other communications given to the user of the screen name).
- Evidence discovered on the alleged sender's computer reflects that the user of the computer used the screen name. (See *U.S. v. Tank* (9th Cir. 2000) 200 F.3d 627.)
- Defendant testified that he owned account on which search warrant had been executed, that he had conversed with several victims online, and that he owned cellphone containing photographs of victims, personal information that defendant confirmed on stand was consistent with personal details interspersed throughout online conversations, and third-party service provider (Facebook) provided certificate attesting to chat logs' maintenance by its automated system. (*U.S. v. Browne* (3d Cir. Aug.25, 2016) 2016 WL 4473226, at 6.)

Hearsay Exceptions and Non Hearsay Purposes

ESI and HEARSAY EXCEPTIONS

- Exception for Statements of a Party Opponent
 - E.g. texts, chats sent by D
 - Rule of completeness allows for admission of response texts.

Statements Not Offered for their Truth are NOT hearsay

- When D is lying.
- Exception for computer records that are not a statement of a person (Evid. Code §§ 175, 225)
 - E.g. Internet Protocol (IP) records; connection dates and times.
- Operative facts
 - a/k/a verbal conduct
 - a/k/a res gestae

Operative Facts

- Where "the very fact in controversy is whether certain things were said or done and not ... whether these things were true or false, ... in these cases the words or acts are admissible not as hearsay[,] but as original evidence." (1 Witkin, Cal. Evidence (4th ed. 2000) Hearsay, § 31, p. 714.)
- In an identity theft prosecution, there will be no hearsay issue for the majority of your documents.
 - The documents are not being offered for the truth of the matter asserted; they are operative facts.

Non-hearsay Purpose- Hearer Acted in Conformity Witness Did Next

- The statement imparted certain information to the hearer and that the hearer, believing such information to be true, acted in conformity with that belief. The statement is not hearsay, since it is the hearer's reaction to the statement that is the relevant fact sought to be proved, not the truth of the matter asserted in the statement.
- Not in Evidence Code
- Still must survive Evid C. 352 analysis
- Limiting instruction

• *People v. Scatzi* (1981) 126 Cal App 3d 901, 807.
• *Jefferson*, Cal. Evidence Benchbook (1978 supp.) § 1.5, p. 21;
• *People v. Samuels* (2005) 36 Cal.4th 96, 122, 30 Cal.Rptr.3d 105, 113 P.3d 1125 [out-of-court statement properly admitted to explain witness's subsequent actions].

Digital Evidence offered for Non Hearsay Purposes

- The words forming an agreement are not hearsay (*Jazayeri v. Mao* (2009) 174 Cal.App.4th 301, 316 as cited by *People v. Mota* (Cal. Ct. App., Oct. 8, 2015, No. B252938) 2015 WL 5883710 (Unpublished))
- A deposit slip and victim's identification in a burglary case introduced to circumstantially connect the defendant to the crime. (*In re Richard* (1979) 91 Cal App.3d 960, 971-979.)
- Pay and owes in a drug case. (*People v. Harvey* (1991) 233 Cal. App.3d 1206, 1222-1226.)
- Items in a search to circumstantially connect the defendant to the location. (*People v. Williams* (1992) 3 Cal.App.4th 1535, 1540-1543.)

Digital Evidence offered for Non Hearsay Purposes

- Invoices, bills, and receipts are generally hearsay unless they are introduced for the purpose of corroborating the victim's damages. (*Jones v. Dumrichob* (1998) 63 Cal. App. 4th 1258, 1267.)
- Defendant's social media page as circumstantial evidence of gang involvement (*People v. Valdez* (2011) 201 Cal App.4th 1429.
- Logs of chat that was attributable to Defendant were properly admitted as admissions by party opponent, and the portions of the transcripts attributable to another person were properly classified as "non hearsay", as they were not "offered for the truth of the matter asserted." Replacing screen names with actual names appropriate demonstrative evidence. (*U.S. v. Burt* (7th Cir., 2007) 495 F.3d 733.)

Digital Evidence offered for Non Hearsay Purposes

- "To the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all—and thus fall outside the ambit of the hearsay rule." (*Perfect 10, Inc. v. Cybernet Ventures, Inc.* (C.D. Cal. 2002) 213 F.Supp.2d 1146, 1155.)
- Generally, photographs, video, and instrument read outs are not statements of a person as defined by the Evidence Code. (Evid. Code §§ 175, 225; *People v. Goldsmith* (2014) 59 Cal.4th 258, 274; *People v. Lopez* (2012) 55 Cal.4th 569, 583.)

Hearsay Exceptions From article by San Diego DDA Jeff Dort

- ☐ Admission § 1220/adoptive admissions § 1221
- ☐ Excited utterance, explaining an event § 1240
- ☐ Present sense impression/contemporaneous § 1241
- ☐ Past recollection recorded § 1237
- ☐ State of mind/mental or physical state § 1250

- ☐ Prior consistent statement § 1236
- ☐ Prior inconsistent statement § 1235
- ☐ Reputation in the community § 1320
- ☐ Comm. list/directory/phonebook/relied on in biz § 1340
- ☐ Not offered for truth/for listener's reaction⁹

**Published Tabulations exceptions-
Be Careful**

- Evid. C. section 1340
- ONLY for published tabulations, lists, directories, or registers.
- REQUIRED - the evidence contained in the compilation is generally used and relied upon by the business community and that it will have no commercial value unless it is accurate.

Be Careful

***People v. Franzen* (2012) 210 Cal. App. 4th 1193**

- Entersect Online phone directory did NOT qualify:
 - (1) Publisher must have made a financial investment in the publication, and is exposed to potential loss if it fails to sell;
 - (2) it means that the content is *limited in quantity*, such that the publisher must exercise some kind of editorial discretion, probably including steps to confirm the accuracy of the matters included;
 - (3) its content is also *fixed in time*, meaning that inaccuracies will persist (and the publisher's reputation will remain exposed to harm by their presence) into the indefinite future; and (4)
 - The work is generally *circulated as a whole*, creating a risk for the publisher that all errors will eventually be exposed.

Internet Postings that are NOT statements made by declarants testifying at trial need indicia of trustworthiness

- Any info that is Hearsay can be excluded, even if it meets an exception.

- *People v. Johnson* (N.Y. Co. Ct., Dec. 31, 2015) 2015 N.Y. Slip Op. 25431
- *United States v. Jackson*, 208 F.3d 633, 638 [7th Cir.2000] (declining to admit web postings where defendant was unable to show that the postings were authentic, and holding that even if such documents qualified under a hearsay exception, they are inadmissible "if the source of information or the method or circumstances of preparation indicate a lack of trustworthiness") (quoting *United States v. Croft*, 750 F.2d 1354, 1367 [7th Cir.1984]); see also *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, *supra*, 76, F. Supp.2d at 775 ("[A]ny evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules.") *Novak v. Tucows, Inc.*, 2007 WL 922306, *5, 2007 U.S. Dist. LEXIS 21269, *15-16 [E.D.N.Y. Mar. 26, 2007], 25431

Other Potential Exceptions to the Hearsay rule

- Hearsay

- Evidence Code section 1523(d) – voluminous records
- Evidence Code section 1280 – record by public employee.

Confrontation Clause

Confrontation Clause

- Emerging Area
- How can the defendant cross-examine a Business Records custodian?
- Similarly, is cross-examining a police officer testifying about records the same as confronting a Facebook employee who actually knows about how records are kept.

Confrontation Clause Claims
Do Not Affect the Video portions of
Business Records

- Because the video evidence was not hearsay, the defendant did not have any confrontation clause claims. *People v. Goldsmith (CA)*

CAL ECPA
Penal Code section 1546



Consider how SEALING will affect your
trial prep

- How will you handle discovery?
 - Do you discover everything on computers or received by search warrant?
 - Even if you as the prosecutor have not seen it because it has been sealed?
- Cal ECPA allows the prosecutor/LEO to get a court order to re-examine and unseal records.

Thank you for your attention!!!



CERTIFICATE OF ATTENDANCE FOR CALIFORNIA MCLE

Top portion of form to be completed by the MCLE Provider

Provider Name: Ventura County District Attorney's Office

Provider Number: 1130

Title of Activity: Admitting Digital Evidence & Cal ECPA update

Date(s) of Activity: February 13, 2017

Time of Activity: 10:00 am - 11:30 am

Location of Activity (City, State): HOA: Lower Plaza Assembly Room Ventura, CA

Total California MCLE Credit Hours for the above activity are 1.50, including the following sub-field credits:

- Legal Ethics _____
- Elimination of Bias in the Legal Profession _____
- Prevention, Detection and Treatment of Substance Abuse/Mental Illness that Impairs Professional Competence _____

Bottom portion of form to be completed by the Attorney after participation in the above-referenced activity

By signing below, I certify that I participated in all, or some*, of the activity described above and am therefore entitled to the following MCLE credit hours -

Total California MCLE Credit Hours 1.50, including the following sub-field credits

Legal Ethics _____

Elimination of Bias in the Legal Profession _____

Prevention, Detection and Treatment of Substance Abuse / Mental Illness that Impairs Professional Competence _____

(You may not claim credit for sub-fields unless the Provider is granting credit in those areas and you participated in those portions of the activity)

Print Your Name _____

Your California State Bar Number _____

Signature _____

* partial participation hours must be pro-rated

ACTIVITY EVALUATION FORM FOR CALIFORNIA MCLE

Please complete and return to Provider (Please Print)

Provider Name: Ventura County District Attorney's Office Provider Number: 1130

Title of Activity: Admitting Digital Evidence & Cal ECPA Update

Date(s) of Activity: February 13, 2017

Time of Activity: 10:00 am - 11:30 am

Location of Activity: HOA: Lower Plaza Assembly Room Ventura, CA

Please indicate your evaluation of this course by completing the table below

Question	Yes	No	Comments
Did this program meet your educational objectives?	<input type="checkbox"/>	<input type="checkbox"/>	
Were you provided with substantive written materials?	<input type="checkbox"/>	<input type="checkbox"/>	
Did the course update or keep you informed of your legal responsibilities?	<input type="checkbox"/>	<input type="checkbox"/>	
Did the activity contain significant professional content?	<input type="checkbox"/>	<input type="checkbox"/>	
Was the environment suitable for learning (e.g., temperature, noise, lighting, etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	

Please rate the instructor(s) of the course below

Instructor's Name and Subject Taught	On a scale of 1 to 5, with 1 being Poor and 5 being Excellent, please rate the items below	Rate 1 – 5
Marc Leventhal, Sr. DDA - Cal ECPA Update	Overall Teaching Effectiveness	—
	Knowledge of Subject Matter	—

Instructor's Name and Subject Taught	On a scale of 1 to 5, with 1 being Poor and 5 being Excellent, please rate the items below	Rate 1 – 5
Howard Wise, Sr. DDA - Admitting Digital Evidence	Overall Teaching Effectiveness	—
	Knowledge of Subject Matter	—

Instructor's Name and Subject Taught	On a scale of 1 to 5, with 1 being Poor and 5 being Excellent, please rate the items below	Rate 1 – 5
	Overall Teaching Effectiveness	—
	Knowledge of Subject Matter	—

Upcoming MCLE class:

Topic: **Admitting Digital Evidence & Cal ECPA Update**
Date: February 13, 2017 (Court holiday)
Time: 10:00 – 11:30 am
Place: HOA: Lower Plaza Assembly Room
Speaker: Howard Wise
MCLE: 1.50 hours general credit
**Attendance: General Criminal Division (Mandatory),
SAFPU (Recommended)**

In a digital world where anything theoretically can be “spoofed”, prosecutors face unique challenges in proving authentication and meeting hearsay, best evidence and confrontation clause challenges. This class will address these issues as well as other search and seizure issues related to obtaining digital and “cloud” evidence. A portion of the lecture will be an update of Cal ECPA and our Office’s policies for complying with it.

The Ventura County District Attorney’s Office is a State Bar of California approved MCLE provider. The above listed class will qualify for 1.50 hours general credit by the State Bar.

Introduction

Since January 2016, searches of electronic files and data by California government agents have been regulated by the California Electronic Communications Privacy Act, or “Cal ECPA.”¹ Adapting to Cal ECPA has been a challenge for law enforcement. It is a challenge we must meet, as failure to comply could jeopardize successful prosecution of any crime in which the proof depends on electronic evidence.

This memo summarizes Cal ECPA and introduces forms the District Attorney has designed to help agencies comply with it. Using standardized forms will help ensure that electronic evidence is obtained legally and admissible in court.

Cal ECPA’s Core Mandate

Cal ECPA enhances privacy protection for electronic data in five basic ways:

1. It generally requires a search warrant with special terms limiting the search.
2. It permits some warrantless searches.
3. It forbids searches other than those it authorizes.
4. It requires the government to provide notice of most searches.
5. It authorizes suppression of evidence obtained in violation of its provisions.

Cal ECPA’s scope is broad: It applies to searches of electronic information stored on any device or with any service provider. Service providers include not only companies that offer communication and data management services to the public, but also private or government employers and conceivably individuals who provide such services to others.

Cal ECPA only covers government access to stored data. It does not cover seizure of a device if data is not accessed. Such seizures remain subject to traditional Fourth Amendment principles.

Cal ECPA Search Warrant Requirements

A warrant to search data stored on a device or with a service provider must include the following terms:

¹ Cal ECPA was passed as Senate Bill 178 in October 2015. It took effect on January 1, 2016 and is codified in Penal Code §§ 1546-1546.4. In September 2016, SB 1121 was passed to amend certain provisions of Cal ECPA. The amendments take effect on January 1, 2017. This memo summarizes Cal ECPA, as amended.

1. A particularized description of the information sought, including: (a) the target individuals or accounts; (b) the types of information sought; (c) the applications or services covered; and (d) the time period covered.²
2. An order requiring that information obtained through execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not used or disclosed except pursuant to court order.
3. An order authorizing delayed service of notice of the warrant, if delay is sought and approved.
4. If the warrant is directed to a service provider, an order directing the service provider to produce an affidavit signed by a custodian authenticating the records produced.

Many warrant applications submitted since Cal ECPA took effect have been deficient. Descriptions of targeted data have been variously too broad, too specific, or missing. Some warrants have lacked the mandatory order protecting unrelated information. Some warrants have left out an order delaying notice, even when the application requested one. The forms the District Attorney has designed include prompts to ensure every Cal ECPA warrant includes the required terms.

Cal ECPA makes two exceptions to the rule requiring unrelated evidence to be sealed and not used or disclosed: (1) The prosecution may disclose such evidence to comply with discovery obligations; and (2) The court may order review, use, or disclosure of such evidence if there is probable cause to believe it is relevant to an active investigation, or if disclosure is required by law. The case agent and prosecutor must coordinate to make sure proper disclosure is made to the defense in any filed case, and that seized electronic evidence outside the scope of a search warrant is not accessed unless a subsequent court order authorizes it.

Warrantless Searches Under Cal ECPA

Cal ECPA limits government access to electronic evidence without a warrant.

Information Held By Service Providers

The government may only search electronic information held by a service provider without a search warrant in the following situations:

1. Pursuant to a wiretap order.
2. Pursuant to a pen register or trap and trace order.

² If the facts support it, the court may order the search of a device for relevant data with no time period restriction. All warrants seeking data from service providers must include a time period restriction.

3. With consent of an authorized possessor of the account.³
4. If the government is the addressee or intended recipient or a member of the intended audience of a communication, including when the originator does not know the government is receiving it.
5. If a service provider produces information in an emergency involving danger of death or serious physical injury to a person, in which case the government must, within three court days, apply for an order declaring the emergency. If the court finds no emergency occurred, it must order the data destroyed. Notice must be given as described below.
6. The government may obtain information from a service provider to locate a device that has called 911.
7. If a service provider voluntarily discloses information to the government, provided the disclosure is not prohibited by law and within 90 days the government seeks an order authorizing retention of it.
8. If the service provider is, or discloses information to, a prison or jail, and all participants to the communication were informed in advance that the provider may disclose the information to the government.
9. If the information sought is subscriber information (name, street address, phone number, email address, account number, and length and type of service), the government may obtain it via subpoena or traditional (non-Cal ECPA) search warrant.

Information Stored on Devices

The government may only search electronic information stored on a device without a search warrant in the following situations:

1. Pursuant to a wiretap order.
2. Pursuant to a pen register or trap and trace order.
3. Pursuant to a tracking device search warrant.
4. With consent of its authorized possessor.
5. With consent of its owner if it has been reported lost or stolen.

³ In practice, consent searches of accounts occur only when the consenting party allows an officer to log on to or view the account. Service providers do not give law enforcement account access or records based on consent.

6. If an emergency involving danger of death or serious physical injury to any person requires access to it, provided that the government must apply for an order within three court days, and must give notice as described below.
7. If it appears to be lost, stolen, or abandoned, but only to identify its owner or authorized possessor.
8. If it is seized from an inmate or found in an inmate-accessible area of a prison or jail, provided it is not known or believed to belong to an authorized visitor.
9. If it is seized from a person on parole or post-release community supervision.
10. If it is seized from a probationer, provided he is its authorized possessor and his probation terms clearly subject him to an electronic device search.⁴
11. The government may ping a device that has called 911 in order to locate it.

Cal ECPA Notice

Cal ECPA requires the government to provide written notice when it executes a warrant to search a device or an account, or when it obtains device or account data in an emergency. The notice must:

1. Inform the recipient information about him/her has been obtained; and
2. Reasonably specify the nature of the investigation; and
3. Include a copy of the warrant, but not the statement of probable cause.

How notice is given depends on if there is an “identified target” when the warrant is issued. Notice is to be given to an identified target by personal service, mail, email, or other effective means. If there is no identified target, notice must be uploaded to a dedicated web portal operated for that purpose by the California Department of Justice.⁵

⁴ If a probationer possesses a device but he is not its authorized possessor – for instance, if he is suspected of having stolen it or borrowed it without permission – a warrant or consent to search from the owner must be obtained.

⁵ Cal ECPA does not define “identified target,” which could mean either “known suspect” or “known owner of the device or account being searched.” “Target” suggests the former, but we often search devices or accounts whose owner is not known, or which are known to belong to a non-suspect. It would make little sense to require notice to a suspect if the device or account searched were not his. If a case agent has a good faith claim that there is no identified target *when the warrant is issued* – which is what the statute says, he should consider immediately uploading notice to DOJ, rather than seeking delayed notice. This is because: (1) notice sent to DOJ will not jeopardize an investigation; and (2) once notice is sent to DOJ, no further notice is required, even if a “target” is identified later. Thus, when it can be justified, sending proper notice immediately to DOJ eliminates the risk of failing to provide or providing deficient notice.

Unless a delay is ordered, notice must be served when the warrant is executed; or, in an emergency, within three court days of when the data is obtained. The court can order notice delayed for up to 90 days if immediate notice may cause an “adverse result,” defined as: (1) danger to life/physical safety; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) witness intimidation; (5) serious jeopardy to the investigation; or (6) undue trial delay. A delay order can be renewed if the justification persists.

Thus, an officer applying for a warrant or responding to an emergency must decide if immediate or delayed notice is appropriate. Delayed notice must be justified in the application to the court.

Delayed notice differs from contemporaneous notice, and must include:

1. All information contemporaneous notice requires; and
2. A statement of the grounds that supported delayed notice; and
3. A copy of all information obtained or a summary of it that includes, at a minimum: (a) the number and types of records; and (b) when the earliest and latest records were created.⁶

Agencies should maintain written proof of service of Cal ECPA notice, including: (1) who served it; (2) who received it; (3) the time, date, location, and manner of service; and (4) a copy of the notice. A similar proof of service should memorialize any Cal ECPA notice uploaded to DOJ.

An order authorizing delayed notice under Cal ECPA is not the same as an order sealing the warrant or a nondisclosure order to the party served with the warrant. The justifications may be similar, but the requests and orders should appear separately.

Suppression Under Cal ECPA

Since 1982, evidence could not be excluded in a California criminal case unless the court found the government obtained it in violation of the United States Constitution. Evidence obtained in violation of any other law could not be suppressed; only constitutional violations mattered. Thus, with respect to government searches and seizures of private property, a Fourth Amendment violation, as defined by the Supreme Court, had to be found for evidence to be excluded.

⁶ Case agents should ordinarily summarize the information produced, rather than provide a copy of all of it, as the more detailed disclosure could compromise the investigation. Cal ECPA imposes a mere *notice* requirement, not a *discovery* requirement, so a simple statement of the number and types of and date range covered by the records is all that is required. If the data consisted of Gmail account records, the notice would only need to identify the account, indicate the start and end dates of the records produced, and estimate the number of emails produced.

Today this remains the law for all types of evidence *except* electronic information. Cal ECPA authorizes suppression of electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution *or the provisions of Cal ECPA*.

Cal ECPA also authorizes *anyone* to seek suppression. This breaks with established law, under which: (1) only a charged defendant could move to suppress evidence offered against him; and (2) only a defendant with a reasonable expectation of privacy in property the government allegedly seized and/or searched illegally could move to suppress it.

Cal ECPA authorizes suppression for violations without articulating any standards for when it should or should not be ordered. It does not provide for less drastic remedies for minor, technical, or unintentional violations.

So far no cases have interpreted suppression under Cal ECPA. Eventually defendants will file suppression motions based on claims that the government obtained electronic evidence in violation of Cal ECPA, even if not in violation of the Fourth Amendment. Such motions might include the following claims:

- A search warrant did not order that unrelated information is to be sealed and not used or disclosed.
- A search warrant did not include a time period limitation, or it otherwise failed to describe targeted information.
- Notice was not given or was given deficiently.
- Consent was not given by an authorized possessor of a device or account.
- A probationer was not authorized to possess a device seized from him and searched without warrant.
- A probationer's device was searched without warrant even though his probation terms did not clearly authorize such a search.

Under Cal ECPA, it is not clear if recognized justifications for admitting evidence seized/searched without a valid warrant remain viable for electronic information. For example:

- Cal ECPA defines *emergency* (circumstances involving risk of death or serious physical injury) more narrowly than traditional *exigent circumstances* (which includes circumstances involving risk of escape or flight and damage, destruction, or disappearance of evidence). Will courts suppress electronic evidence accessed without warrant in exigent circumstances that do not

involve risk of death or serious injury but which involve risk of flight or loss of evidence?

- Federal law holds evidence obtained pursuant to a defective search warrant need not be excluded if the officers executing it had a reasonable *good faith* belief it was valid. Will courts suppress electronic evidence accessed with a defective warrant if good faith is proven?⁷
- Federal law provides for exclusion of evidence derived from a constitutional violation as the “fruit of a poisonous tree,” but permits admission of such evidence if: (a) the taint of the violation was attenuated; (b) the evidence was also discovered by a source independent of the violation; (c) the evidence inevitably would have been discovered had the violation not occurred. Will courts suppress electronic evidence accessed in violation of Cal ECPA if an exception to the fruit of the poisonous tree doctrine applies?
- Federal law holds an officer may search private property without a warrant if he has consent from someone who has actual or apparent authority over it, and that if it was objectively reasonable for the officer to believe the party had the authority to consent, the evidence obtained in the search will not be excluded if it turns out the party did not have such authority. Does Cal ECPA’s requirement that consent be given by someone “authorized to possess” a device eliminate the “apparent authority” doctrine for device searches?

Plain View Searches Under Cal ECPA

In the electronic evidence arena, no topic is as controversial as *plain view*. Cal ECPA does not mention plain view. But its provisions – especially the requirement of an order to seal and not to use or disclose evidence unrelated to the objective of the warrant – reflect an interest in restricting law enforcement access to identified evidence for which it has probable cause to search. At its core, Cal ECPA is an “anti-rummaging” statute.

Under Cal ECPA, it remains possible for an officer to observe, in plain view, incriminating electronic evidence that is beyond the scope of an authorized search. Common plain view scenarios include:

1. When an officer searches a device or account pursuant to a warrant targeting evidence of a specific crime against an identified victim, and he notices evidence tending to prove a similar crime against another victim.

⁷ In various cases the court has invoked the good faith doctrine to hold admissible evidence obtained from the execution of warrants deemed facially invalid because of defective or overbroad descriptions of the targeted property. A common feature in those cases is proof that the officers conducted a reasonable and limited search, consistent with the proper objective of the warrant, had it been properly drafted. California courts may or may not recognize a good faith exception to admit electronic evidence obtained pursuant to defective Cal ECPA warrants, but officers can strengthen our claim for one by searching for and extracting only that evidence for which there is probable cause to search (*i.e.*, only that evidence that should have been listed in the property description, had it been properly drafted).

2. When an officer legally searches a device or account pursuant to a warrant targeting incriminating evidence within a particular time period, and he notices incriminating evidence outside of that time period.
3. When an officer legally searches a device or account pursuant to a warrant targeting specific categories of incriminating information, and he notices incriminating evidence outside of all categories of information listed in the warrant.

Because of the risk of suppression, when an officer makes a plain view observation during a device or account search, he should immediately: (1) document the relevant facts, including his authority for doing what he was doing when he observed the evidence, what he observed; and the basis for his belief that what he saw was incriminating; and (b) seek a second (“piggy-back”) search warrant to search the device or account for evidence relating to the crime(s) associated with his plain view discovery.

AB 1924

New exception to allow use of a pen register or trap and trace device.

Here was the problem: In 2015, AB929 provided authority for state courts to issue orders directing the use of a pen register or trap and trace device.¹ However, later in 2015, SB178 (CalECPA) imposed additional limits on access to all electronic evidence, subject to a few specific exceptions. The catch was that a “court order” pursuant to AB929 was not included in the list of exceptions under SB178. Because SB178 was enacted second, the AB929 court order was “chaptered out” and never took effect.

To fix this issue, AB1924 added a new exception in Penal Code §1546.1(b)(5) to allow compelled production of communication information with a court order for a pen register or trap and trace device. AB1924 was passed as “urgency legislation” which means that its provisions took effect as soon as the governor signed the bill.

Changes the notice requirements after using a pen register or trap and trace device. There are two issues with notice: (1) Is the agency required to tell the target; and (2) Can law enforcement prevent the service provider from telling their customer. Before AB1924, section 638.52 did not require law enforcement to notify the suspect and it authorized a sealing order to prevent anyone else from disclosing the order. That sealing could extend “until otherwise ordered” by a judge or to comply with discovery obligations.

Now, the new section 638.54 requires that law enforcement must notify the target of the order within 30 days after the end of the order. Also, the duration of the sealing order (preventing a third party from notifying the target) was changed to match the duration of the order authorizing use of the pen register or trap and trace device. (PC§638.52(g)). This means that while law enforcement must notify the target within 30 days of the end of the order, the service provider is free to give notice as soon as the order expires.

The content of agency-required notice, ability to delay both agency or third party notice, and how to handle notice when the target is not known, all track similar provisions in CalECPA.

Requires payment for pen registers. The new section 638.52(j) requires that any person or electronic communication service that provides assistance as a result of a pen register order be reasonably compensated by the requesting officer’s agency.

Suppression Remedy. The new section 638.55 adds a suppression remedy with universal standing.

¹ A pen register records outgoing address information from an electronic communication. A trap and trace device records information from an incoming electronic communication to identify the source of the communication. Typically, they were used to record phone numbers, but the law applies equally to email, instant messages and other similar platforms. Neither order allows capturing the content of any communication.

Adds several new exceptions to allow access to electronic devices.

Probation / Parole. The new subsections 1546.1(c)(9) and (10) add authority to search devices possessed by probationers and parolees. The important distinction is that a device possessed by a parolee or a person on Post Release Community Supervision (PRCS) may be searched to the same extent, and with the same limitations, as before CalECPA. However, a device in possession of a person on probation, mandatory supervision or pretrial release may only be searched if a specific electronic search clause is a “clear and unambiguous” condition of their release. A possible reason for this distinction is that parole and PRCS search conditions are statutory and unrelated to the offense of conviction. A judge cannot change parole or PRCS conditions. On the other hand, the terms of probation are discretionary and must be rationally related to the offense.

911 calls. The new subsection 1546.1(c)(11) allows the government to access electronic device information to determine the location of a device when responding to an emergency 911 call without a warrant. Likewise, the amended subsection 1546.1(h) removes the requirement to seek court approval after receiving location information from a service provider when responding to a 911 emergency call.² If an emergency is reported through something other than the 911 system, the existing CalECPA rules will still apply.

Phones recovered from jail. The renumbered section 1546.1(c)(8) expands the ability to search a device found in an inmate’s possession or abandoned in a correctional facility. Previously, law enforcement could search a device seized from an inmate, or abandoned in facility under the jurisdiction of the Department of Corrections and Rehabilitation. A warrant was needed to search a device found abandoned in a local county jail. This amendment adds authority to search devices found in local detention facilities if it is recovered from an area where inmates have access and it is not believed to be in possession of an authorized visitor. (A warrant may still be needed for devices recovered from CYA and state hospitals.)

² There are two ways that police commonly receive device information during an emergency:

(1) When a 911 call is initiated, the Enhanced 911 (E911) system displays Automated Location Information (“ALI”). While the call is active, the E911 system allows the dispatcher to periodically request the system to retransmit the ALI. A retransmit is useful because it may show a more precise location or track a phone in motion. When causing the system to retransmit an ALI, the dispatcher is directly accessing device information. Technically, before this amendment, CalECPA would have required notice and court authorization even if the access would not result in criminal prosecution.

(2) After a call has disconnected, police can contact the carrier and request that the carrier “ping” the phone and report back its location. There had been a debate about whether an emergency ping request falls under “direct access” (where the carrier is acting as an agent of the requesting agency) or “voluntary production” (where the carrier was acting under their own authority as sanctioned by the federal ECPA). Previously, the distinction was important because there were different requirements for notice, court authorization and evidence retention.

Driver's License magnetic strip. The amended section PC1546(f) narrows *slightly* the definition of an electronic device. "Electronic Device" is still defined as "a device that stores, generates, or transmits information in electronic form" but the amendment specifically excludes the magnetic strip on a state-issued driver's license or identification card. It leaves in place existing interpretations about other magnetic strips – like credit cards, hotel key cards and school IDs. The amendment was added to allow use of new technology like electronic traffic ticket writing devices and intoxilizer machines that populate the printout in a DUI investigation by swiping the suspect's driver's license.

Includes GPS trackers in CalECPA

GPS trackers. The new subsection 1546.1(c)(3) adds an exception for a tracking device warrant issued pursuant to Penal Code sections 1524(a)(12) and 1534(b). Since a search warrant was already required to use a tracking device, and a search warrant was already included in the warrant-exception in PC1546.1(c)(1), it is unclear if this change has any practical effect. However, there was a debate about whether CalECPA reached government-owned tracking devices at all. This debate was necessary because the contents of the warrant and notice requirements were different. The addition and the change to PC1534(b) cited below answer the debate. All electronic tracking devices fall under CalECPA and the notice requirements are now identical.

Before SB1121, Officers who used a tracking device were required to serve a copy of the warrant on the person tracked or owner of the property that was tracked within 10 days after use of the device ended. (Penal Code §1534(b)(4)). Notice could have been delayed with a court order for "good cause." Now, after SB1121, notice must still be given to the person or owner within 10 days after the end of tracking, but the notice must comply with PC1546.2. This means that in addition to providing a copy of the warrant, officers must also include a statement with reasonable specificity about the nature of the investigation. Notice may be provided by first class mail, email or other means reasonable calculated to be effective. Any request to delay notice must also track CalECPA pursuant to Penal Code §1546.2(b). This means that the delay is limited to 90 days and the court must find that prior notice would have an "adverse result" rather than merely "good cause." Adverse result is defined in PC1546(a) as (1) Danger to the life or physical safety of an individual; (2) Flight from prosecution; (3) Destruction of or tampering with evidence; (4) Intimidation of potential witnesses; (5) Serious jeopardy to an investigation or undue delay of a trial.

****** If law enforcement is seeking real-time location information from a cell phone provider, they must to use a tracker warrant under PC1524(a)(12) and 1534(b), not a Trap & Trace/Pen Register Court order under PC638.52. The later section specifically excludes use of that order to get location information.

Changes to "Time Period" requirement in a warrant

Prior to SB1121, section 1546.1(d)(1) required that all CalECPA warrants include “the time period covered, and as appropriate and reasonable, target individuals or accounts, the applications or services covered, and the types of information sought.” This language arguably invited an argument when searching a device for deleted data or file fragments where the normal time stamps are missing. It also may arbitrarily limit the search for contraband – like child porn – where the time period may not be a relevant factor, or can be easily manipulated by suspects. An amendment to section 1546.1(d)(1) moved “time period” to after the modifier “as appropriate and reasonable.” So, it is no longer a strict rule that warrants must include a date. However, warrants must still describe with particularity the information sought. This means that as a general rule, warrants should still include a time period. But, in appropriate cases, the court can lift that limitation when supported in the affidavit.

Allows limited access to sealed information for discovery.

Prior to SB1121, information unrelated to the objective of the warrant had to be sealed, and not accessed again without a court order. This presented a problem for prosecutors wanting to comply with their statutory and constitutional duty to provide discovery. Originally, CalECPA provided that a court could issue an order to access sealed information, including when “disclosure is required by state or federal law.” This meant that *technically*, prosecutors had to seek court permission to comply with their discovery obligations. This amendment provides additional authority to access sealed information without a court order when the access is “to comply with discovery as required by Sections 1054.1 and 1054.7.” This means that prosecutors and investigators can search for exculpatory information and provide copies to the defense like before CalECPA.

Additional authority for recorded jail calls.

With the originally enacted version of CalECPA, there was a debate about if and how recorded inmate jail calls were affected. Was the jail a communications service provider voluntarily sharing information with law enforcement? Was the jail a party to the communication? Could law enforcement directly access the jail’s server to review calls with the jail’s consent? (And, if the jail is a service provider, do they even have authority to consent to government access to communications content?) Does any of that change if the jail contracts with an outside company to provide the service? These questions are important because the notice and evidence retention rules are different.

The new section 1546.1(g)(4) answers at least one of those questions. Now, law enforcement can retain electronic communication information voluntarily provided by a communications service provider when that provider “is, or discloses the information to, a federal, state, or local prison, jail, or juvenile detention facility, and all participants to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.”

This may require changing the recorded message on jail calls. . . . Or, it may not if courts ultimately find that – due to the open and routine monitoring – the jail is an intended recipient of the communication. (Pursuant to PC1546.1(a)(3), an intended recipient of an electronic communication can share the content without limitation.)

Government owned devices.

There had been a debate about if a government employee who is an authorized possessor of a government-owned electronic device could stop an employer from searching the device by withholding or withdrawing consent. This question centered around the use of police body cams, but could have very wide application. While under normal circumstances, prior consent as a condition of employment should be sufficient, consent can always be withdrawn.

To address this issue, (and rather than simply saying that an employer can access an employer-owned device pursuant to an employment contract) the new section 1546.1(k) says that CalECPA does not prevent a government entity that owns an electronic device from compelling an employee to return the device. Presumably, the employer will then be the authorized possessor and can consent to search their own device.

Changes some time limits from “days” to “court days”

Prior to SB1121, PC1546.1(h) required the government to seek court approval within three calendar days of obtaining electronic information in an emergency. Likewise, section 1546.2 required the government to give notice to the target within three calendar days of obtaining the information. This could prove burdensome for investigations that extend over a weekend or holiday. Therefore, both sections were amended to cite three court days. This means that law enforcement also has three court days to seek and order to delay notice.

However, there is still one anomaly. If the government obtains electronic information in an emergency and there is no known target, section 1546.2(c) still requires the government to provide notice to the Department of Justice within “three days” (i.e. calendar days). And obviously, this also means that any order to delay notice to the DOJ must be obtained within three calendar days.

Changes “emergency request” to “emergency access”

Before SB1121, section 1546.2 gave the rules for giving notice following a “warrant or emergency request.” Now, SB1121 changed this language to say “warrant or emergency access.” To analyze the possible effect of this change, it may be useful to consider the three most common ways that law enforcement obtains electronic information: (1) They can compel a service provider to produce information with a warrant; (2) They can directly access an electronic device with a warrant or in an emergency; or (3) They can request information from a service provider in an emergency – and then if the service provider agrees that there is an

emergency, 18 U.S.C. 2702(b)(8) and (c)(4) allow the service provider to voluntarily produce information without any court involvement.

Arguably, the prior version of SB1546.2 did not require notice following emergency access. (i.e., The direct emergency access was not the result of a “warrant” or “request.”) This amendment fixes that potential loophole and makes it clear that the notice requirement also includes direct access to a device in an emergency. And, as stated above, that notice must be provided within three court days of obtaining the information if there is a known target or three calendar days to DOJ if there is no known target.

But, what’s the notice rule now when law enforcement makes a request for electronic information to a service provider in an emergency?

As an initial point, the notice rules in section 1546.2 only apply to a “government entity that executes a warrant, or obtains electronic information in an emergency pursuant to Section 1546.1.” The emergency-exception is PC1546.1(c)(5) (renumbered by SB1121 as 1546.1(c)(6)) and only applies to access to a device, not a request of service provider records.

CalECPA does not limit the ability of law enforcement to request voluntary production of information.³ Section 1546.1(h) simply gives the procedure for seeking court authorization after the government “obtains” electronic information in an emergency. Use of the word “obtain” rather than “access” seems to imply a broader application that would also include voluntary disclosure after a “request.” That section says that if the court does not agree that there was an emergency, then notice must be provided as described in section 1546.2. However, section 1546.1(h) is silent on whether notice is required if the court agrees that there was an emergency. And now, that subdivision does not apply at all if the emergency request was made to follow-up on a 911 call.

Section 1546.1(g) governs how the government must handle information voluntarily produced by a service provider and is also silent on the issue of notice.

Therefore, it seems that notice is no longer required following emergency disclosure of electronic information from a service provider. With that said, no evidence will be suppressed by giving too much notice.

SB1087

Admission of business records obtained by search warrant

³ Some prosecutors argue, however, that a service provider acting pursuant to an emergency request becomes the agent of the requesting officer so that the service provider’s conduct is legally attributed to the officer. If that interpretation is correct, an emergency request for third-party records becomes the legal equivalent of direct access to a device.

On July 22, 2016, Governor Brown signed SB1087, a bill that will make a major change in how prosecutors use business records obtained by search warrant. Prior to this bill, Penal Code section 1524.2(b)(4) allowed the use of a custodian's declaration to admit business records obtained by search warrant, but only if those records came from a foreign electronic communications services or remote computing service. If, on the other hand, the records came from a bank, retail store, or any other business, use of those records in court required either a live witness or that the same records be requested a second time with a subpoena duces tecum.

CalECPA expanded that rule a bit by extending to all electronic communications service providers – including those incorporated in California and elsewhere. But all other companies – like banks, car rental agencies, and retail merchants – still needed a live witness or a new SDT to admit records originally obtained by search warrant.

SB1087 fixed this second-SDT problem by amending Evidence Code section 1560 (the subpoena-exception for business records) to include nearly all business records obtained by search warrant. The new subdivision (f) states in part:

If a search warrant for business records is served . . . in which the business is neither a party nor the place where any crime is alleged to have occurred, and the search warrant provides that the warrant will be deemed executed if the business causes the delivery of records described in the warrant to the law enforcement agency ordered to execute the warrant, it is sufficient compliance therewith if the custodian or other qualified witness delivers by mail or otherwise a true, legible, and durable copy of all of the records described in the search warrant to the law enforcement agency ordered to execute the search warrant, together with the affidavit described in Section 1561, within five days after the receipt of the search warrant or within such other time as is set forth in the warrant.

The existing section 1562 then allows admission of those records with the custodian's declaration.

Introduction

Searches of electronic files and data by California government agents are now regulated by the California Electronic Communications Privacy Act, or “Cal ECPA.”¹ Adapting to Cal ECPA has been a challenge for the law enforcement community. It is a challenge we need to meet, as failure to comply with Cal ECPA could jeopardize the successful prosecution of any crime in which the proof depends on electronic evidence.

This memo provides a brief overview of Cal ECPA and introduces forms the District Attorney has designed to help agencies comply with it. Using standardized forms will help ensure that electronic evidence is obtained legally and admissible in court.

Cal ECPA’s Core Mandate

Cal ECPA gives enhanced protection to the privacy of electronic information in four basic ways:

1. It generally requires a search warrant with specific terms limiting the scope of the search;
2. It requires the government to provide notice of a search;
3. It strictly limits when a warrantless search is permitted;
4. It authorizes suppression of evidence obtained in violation of its provisions.

The scope of Cal ECPA is very broad: It applies to searches of electronic information stored on any device or with any service provider. Service providers include not only companies that offer communication and data management services to the public, but also private or government employers and conceivably even individuals who provide such services to others.

Cal ECPA treats all electronic information as equally private, requiring the same legal process to obtain it. Only subscriber information is exempt: The government may issue a subpoena or traditional (*i.e.*, non-Cal ECPA) search warrant to a service provider to obtain a subscriber’s name, street address, phone number, email address, account number, and length and type of service.

Cal ECPA Search Warrant Requirements

To comply with Cal ECPA, a warrant to search data stored on a device or with a service provider must include the following terms:

¹ Cal ECPA is codified as Penal Code §§ 1546-1546.4. It was passed in October 2015 as Senate Bill 178, and took effect on January 1, 2016. Cal ECPA was amended in September 2016 by SB 1121, which will take effect on January 1, 2017. This memo summarizes Cal ECPA, as amended.

1. A particularized description of the information sought, including the time period covered (unless the court orders that no time restriction is appropriate under the facts of the case), the target individuals or accounts, the applications or services covered, and the types of information sought;
2. An order requiring that information obtained through execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not used or disclosed except pursuant to court order.
3. An order authorizing a delay in serving notice of the warrant, if delay is sought and the court approves it.
4. If the warrant is directed to a service provider, an order directing the service provider to produce an affidavit signed by a custodian authenticating the records produced.

Many warrants prepared since Cal ECPA took effect have had deficient property descriptions. Some have been too broad; some have been too specific; some have had no description of the information sought. Many warrants have not included the required sealing order. Some warrants have left out an order delaying notice even though the statement of probable cause asked for one. The forms the District Attorney has designed include prompts to ensure that all Cal ECPA warrants include the terms the statute requires.

Cal ECPA makes two exceptions to the rule requiring that unrelated evidence be sealing and not used or disclosed: (1) The prosecution may disclose such evidence to comply with its discovery obligations; and (2) The court may order review, use, or disclosure of such evidence if there is probable cause to believe it is relevant to an active investigation, or if disclosure is required by law. The case agent and prosecutor must coordinate to make sure proper disclosure of seized electronic evidence is made to the defense in any filed case, and that seized electronic evidence outside the scope of a search warrant is not accessed unless a subsequent court order authorizes its examination.

Cal ECPA Notice Requirements

Cal ECPA requires the government to provide written notice when it executes a warrant to search a device or an account or when it obtains device or account data in an emergency. The notice must:

1. Inform the recipient information about him/her has been obtained;
2. Reasonably specify the nature of the investigation; and
3. Include a copy of the warrant - not the statement of probable cause.

Unless a delay is ordered, the notice must be served when the warrant is executed; or, in an emergency, within three court days of when the data is obtained.

How notice is provided depends on if there is an “identified target” when the warrant is issued.² Notice is to be provided to an identified target by personal service, U.S. mail, email, or other effective means. If there is no identified target, notice must be submitted to the California Department of Justice, which operates a dedicated web portal for that purpose.

The court can order notice delayed for up to 90 days if it finds immediate notice may cause an “adverse result,” defined as: (1) danger to life/physical safety; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) witness intimidation; (5) serious jeopardy to the investigation; or (6) undue trial delay. A delay order can be renewed if the justification persists.

Thus, an officer applying for a warrant or responding to an emergency must decide if immediate or delayed notice is appropriate. If a delay is appropriate, the officer must justify it in his or her application to the court.

The contents of delayed notice are different from contemporaneous notice, and must include:

1. All information contemporaneous notice requires (*i.e.*, disclosure that information has been obtained; description of the nature of the investigation; and a copy of the warrant); and
2. A statement of the grounds that supported delayed notice; and
3. Either a copy of all information obtained or a summary of it that includes, at a minimum, the number and types of records and when the earliest and latest records were created.³

² Cal ECPA does not define “identified target,” which sounds like it might mean “known suspect.” But we often search devices and accounts that do not belong to a known suspect. It would make no sense to require notice to a suspect of a search of property that belongs to someone else. A more reasonable interpretation of “identified target” is a person known to be the owner or authorized user of the device or account being searched.

³ Some officers reportedly believe that when delayed notice becomes due a copy of all data obtained must be disclosed, or else they are opting to provide a copy because they are uncertain how to summarize the data. Officers should not be shy about summarizing the data, especially when the investigation could be hampered by a more detailed disclosure. There is no need to provide more than the minimum mandated disclosure, which is a simple description of the number and types and date range covered by the records. For example, if the data obtained via warrant consisted of Gmail account records, the notice would need only to identify the account, the start and end dates of the records produced, and a reasonable estimate of the number of emails produced. No more information need be provided, as this is a mere *notice* requirement, not a *discovery* requirement.

Agencies should develop a protocol to ensure and memorialize notice compliance. Officers are especially at risk to forget notice when a 90-day delay period expires. Agencies should standardize the preparation and maintenance of written proof of service of notice, to include: (1) who served notice; (2) who was served with notice; (3) the time, date, location, and manner of service; and (4) a copy of the notice served. A similar memo should be prepared for any notice submitted to DOJ.

When a Cal ECPA search warrant is sought in an investigation in which there is no identified target, officers should strongly consider immediately uploading notice to DOJ rather than seeking a delay order. This is because: (1) there is effectively no chance uploaded notice to DOJ will come to the attention of a suspect or jeopardize an investigation; and (2) once notice is uploaded to DOJ, no further notice is required, even if a target is identified later.⁴

An order authorizing delayed notice under Cal ECPA is not the same as a sealing order or a nondisclosure order to the party served with a warrant. The justifications may be closely aligned, but the requests should be made separately, and the orders should appear separately in or with the warrant.

Warrantless Searches Under Cal ECPA

Cal ECPA strictly limits the circumstances in which the government may access electronic evidence without a warrant.

Information Held By Service Providers

The government may only search electronic information held by a service provider without a search warrant:

1. Pursuant to a wiretap order;
2. Pursuant to a pen register or trap and trace order;
3. If an authorized possessor of the account allows the government to access to it;
4. If the government is the addressee or intended recipient or a member of the intended audience of a communication, including when the originator does not know the government is receiving it;

⁴ For example, if an officer obtains a warrant to search a house and all electronic devices inside it, *when the warrant is issued* s/he will typically not know what devices s/he will find and/or whose they are, *i.e.*, there will not be an identified target. Under these circumstances Cal ECPA authorizes the officer to discharge his/her duty of notice by uploading it to DOJ when s/he executes the warrant. Even if the officer seizes devices and obtains evidence associating particular people with those devices, Cal ECPA does not require further notice to those people.

5. If a service provider produces information in an “emergency” involving “danger of death or serious physical injury to a person.” In this event, the government must, within three court days, apply to the court for an order that is effectively an after-the-fact warrant. If the court finds no emergency occurred, it must order the data destroyed. Notice must be given in the manner described above;
6. If a device places a 911 call, the government may obtain information from a service provider to locate that device;
7. If a service provider voluntarily discloses the information to the government, provided that disclosure is not prohibited by law and that within 90 days the government seeks an order authorizing retention of the records;
8. If the service provider is, or discloses the information to, a prison or jail, and all participants to the communication were informed in advance that the provider may disclose the information to the government.

Information Stored on Devices

The government may only search electronic information stored on a device without a search warrant:

1. Pursuant to a wiretap order;
2. Pursuant to a pen register or trap and trace order;
3. Pursuant to a tracking device search warrant;
4. With the consent of the authorized possessor of the device;
5. With the consent of the owner of the device if it has been reported lost or stolen;
6. If an emergency involving danger of death or serious physical injury to any person requires access to it, subject to the requirement that the government must apply for an order within three court days after such access, and must provide notice as described above;
7. If the device appears to be lost, stolen, or abandoned, but the search is to be limited to information tending to identify the owner or authorized possessor of the device;
8. If the device is seized from an inmate or found in an inmate-accessible area of a jail, as long as it is not known or believed to belong to an authorized visitor;

9. If the device is seized from a person on parole or post-release community supervision;
10. If the device is seized from a probationer, if s/he is the authorized possessor of the device and if his/her probation terms clearly subject him/her to an electronic device search⁵;
11. If the government “pings” the device to ascertain its location in response to a 911 call placed by that device.

Suppression Under Cal ECPA

From 1982 to 2016, for evidence in a California criminal case to be suppressed, the court had to find that the government obtained it in violation of the United States Constitution, as interpreted by the United States Supreme Court. Evidence obtained constitutionally, even if in violation of another law, was not subject to suppression.

The Fourth Amendment permits only “reasonable” seizures and searches of private property, which has been construed to mean searches pursuant to valid warrants or searches without warrants deemed reasonable under recognized exceptions such as plain view; exigent circumstances; consent; inevitable discovery; independent source/attenuation; parole/probation search; lost/abandoned property; and good faith. Before 2016, as long as the government seized and searched property pursuant to a valid warrant, or under circumstances in which one of these exceptions to the warrant requirement applied, it could not be suppressed.

Cal ECPA has changed this for electronic information stored on devices or in accounts. While every type of property still can only be suppressed if obtained in violation of the Fourth Amendment, Cal ECPA authorizes suppression of electronic information obtained in violation the federal or state constitution or of any of its provisions.

Cal ECPA provides no guidance on when suppression is appropriate. It gives no standards; it merely authorizes suppression for violations. Cal ECPA does not provide for alternative, less punitive remedies for merely technical, unintentional or minor non-constitutional violations.

In addition, Cal ECPA authorizes anyone to seek suppression of electronic evidence obtained in violation of the federal or state constitution or its provisions. This is a dramatic break with established law, under which only a charged defendant could challenge the admissibility of evidence offered against him, and only a defendant with a reasonable expectation of privacy in evidence seized by the government would have standing to move to suppress it.

⁵ If a probationer possesses a device but s/he is not its authorized possessor – for instance, if s/he is suspected of having stolen it or borrowed it without permission – a warrant or consent to search from the owner must be obtained.

No appellate cases have yet interpreted the suppression remedy codified in Cal ECPA. But it is only a matter of time before aggressive defense lawyers seek suppression of electronic evidence based on claims that the government obtained it in violation of Cal ECPA's provisions, even if the evidence was not obtained in violation of the Fourth Amendment. Such motions might include claims that:

- A search warrant did not include the required order providing that unrelated information is to be sealed and not used or disclosed;
- A search warrant did not include the required time period limitation, or was otherwise deficient in specifying the targeted information;
- The required notice was not given, or was given deficiently;
- Alleged consent to search a device or account was not given by an authorized possessor;
- A probationer was not the authorized possessor of a device seized from him and searched without a warrant;
- A probationer's device was searched without a warrant even though his probation terms did not clearly authorize such a search;
- The government searched a device or account under a theory of exigent circumstances that did not involve a danger of death or serious physical injury to a person (*i.e.*, claiming the risk of damage to property or destruction of evidence or flight).

It is not clear how courts will apply suppression under Cal ECPA.

TO be
reused
BY Howard

Introducing Digital Evidence in California State Courts

Rules of Evidence

This material was prepared by Robert M. Morgester, Deputy Attorney General, California Department of Justice, and draws heavily upon Documentary Evidence Primer, by Hank M. Goldberg, Deputy District Attorney, Los Angeles County District Attorney's Office, January 1999. Material from that document was used with Mr. Goldberg's permission. This material was updated in 2016 by Robert Morgester and Howard Wise, Senior Deputy District Attorney, Ventura County District Attorney's Office

updated in 2006.

Introducing Documentary and Electronic Evidence

The focus of this training CD-ROM is on obtaining and using documentary and electronic evidence (e.g., e-mail) in court. For a further discussion of computer records in criminal investigations, please refer to the federal section of this CD-ROM.

Once digital evidence has been obtained in compliance with Cal ECPA, CA Penal Code §§ 1546.1 and 1546.2, there are four steps necessary for introducing documentary and electronic evidence in court. First, it must be relevant. Second, it must be authenticated. Third, it must withstand a "best evidence" objection. Fourth, the contents of the item must not be inadmissible hearsay. Fourth, it must withstand a "best evidence" objection.

In addition, the digital document or evidence may contain metadata (or data about the data) such as the date and time the document was created or last accessed or when and where a photo was taken. The proponent might need to lay a separate foundation to admit the metadata.

I. Relevance

Only relevant evidence is admissible.-(Evid. Code, § 350.) All relevant evidence is admissible, except as provided by statute.-(Evid. Code, § 351.) "Relevant" means having a tendency to prove or disprove any disputed fact, including credibility. -(Evid. Code, § 210.)

One issue that arises in proving that digital evidence is relevant, is that typically the defendant must be tied to the evidence, usually as the sender or receiver. For example, text messages are often sent from one phone number to another. The proponent must tie the defendant to that phone number because if the defendant did not send or receive/read the text, it might lack relevance. Evidence that the defendant is tied to the number can be circumstantial. Similarly, evidence that the defendant received and read a text can be circumstantial.

Theories of admissibility include:

- Direct evidence of a crime
- Circumstantial evidence of a crime
- Identity of perpetrator
- Intent of perpetrator
- Motive
- Credibility of witnesses
- Impeachment
- Negates or forecloses a defense
- Basis of expert opinion
- Lack of mistake

Formatted: Indent: Left: 0.25", No bullets or numbering

II. Authentication

"Authenticating" evidence means introducing sufficient evidence to sustain a finding that the writing is what you say it is. (Evid. Code, § 1400 (a).) While it does not require proving genuineness, it does require a witness to lay basic foundations. In most cases this is accomplished by showing the writing to the witness and asking, "what is this?" and "how do you know that?." It is important to note that the document originator's testimony is not ~~required~~needed.- (Evid. Code, § 1411.) The proponent should present evidence of as many of the grounds below as possible. However, no one basis is required. Additionally, authentication does not involve the truth of the document's content, rather only whether the document is what it is claimed to be. (*City of Vista v. Sutro & Co.* (1997) 52 Cal.App.4th 401, 411-412.) Digital evidence does not require a greater showing of admissibility merely because, in theory, it can be manipulated. Conflicting inferences go to the weight not the admissibility of the evidence. (*People v. Goldsmith* (2014) 59 Cal. App.258, 267) *In Re KB* (2015) 238 Cal.App.4th 989, 291-292) (upholding red light camera evidence). *Goldsmith* superseded *People v. Beckley* (2010) 185 Cal. App.4th 509, which required the proponent to produce evidence from the person who took a digital photo or expert testimony to prove authentication. Documents and data printed from a computer are considered to be an "original. (Evid. Code 255).

Printouts of digital data are presumed to be accurate representation of the data. Evid Code §§ 1552, 1553. However, that presumption can be overcome by evidence presented by the opposing party. If that happens, the proponent must present evidence showing that by a preponderance, the printouts are accurate and reliable. (*People v. Retke* (2015), 232 Cal. App. 4th 1237 [successfully challenging red light camera data.]

A.

You can authenticate documents by:

- Calling a witness who saw the document prepared. (Evid. Code, § 1413.)
- Introducing an expert handwriting comparison. (Evid. Code, § 1415.)
- Asking a lay witness who is familiar with the writer's handwriting to identify the handwriting. (Evid. Code, § 1516.)
- Asking the finder of fact (i.e. the jury) to compare the handwriting on the document to a known

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: 10 pt

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: 10 pt

Formatted: Superscript

Formatted: Font: 10 pt

Formatted: Font: Italic

Formatted: Superscript

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: 10 pt, Not Bold

2. Introducing Digital Evidence in California State Courts

exemplar. (Evid. Code, § 1470.)

- Showing that the writing refers to matters that only the writer would have been aware. (Evid. Code, § 1421.)
- Using various presumptions to authenticate official records with an official seal or signature. (Evid. Code, § 1450-1454.) Official records would include state prison records, Department of Motor Vehicle documents or documents filed with the Secretary of State. There is a presumption that official signatures are genuine. (Evid. Code, § 1530, 1453.)
- Any other way that will sustain a finding that the writing is what you say it is, since the Evidence Code specifically does not limit the means by which a writing may be authenticated and proved. (Evid. Code, § 1410; See also *People v. Olguin* (1994) 31 Cal.App.4th 1355, 1372-1373 [rap lyrics authenticated in gang case even though method of authentication not listed in Evidence Code].)

B. Common ways to authenticate email include:

- Chain of custody following the route of the message, coupled with testimony that the alleged sender had primary access to the computer where the message originated.
- Security measures such as password-protections for showing control of the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429)
- The content of the email writing refers to matters that only the writer would have been aware.
- Recipient used the reply function to respond to the email; the new message may include the sender's original message.
- After receipt of the email, the sender takes action consistent with the content of the email.
- Comparison of the e-mail with other known samples, such as other admitted e-mails.
- E-mails obtained from a phone, tablet or computer taken directly from the sender/receiver, or in the sender/receiver's possession.

In the majority of cases it is a variety of circumstantial evidence that provides the key to establishing the authorship and authenticity of a computer record. For further information, please consult the federal evidence portion of this CD-ROM. [\[click here\]](#) See also, *Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 546 (seminal case law on authenticating digital evidence under F.R.E.)

C. Common ways to authenticate chat room or Internet relay chat (IRC) communication include:

- Evidence that the sender used the screen name when participating in a chat room discussion. For example, evidence obtained from the Internet Service Provider that the screen name,

3 | Introducing Digital Evidence in California State Courts

Formatted: Font: (Default) Arial Unicode MS, 12 pt

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Arial Unicode MS, 12 pt

Formatted

Formatted: Font: (Default) Arial Unicode MS, 12 pt

Formatted: Line spacing: single

Formatted: Font: (Default) Arial Unicode MS, 12 pt

Formatted: Font: (Default) Arial Unicode MS, 12 pt

Formatted: Font: (Default) Arial Unicode MS, 12 pt

Field Code Changed

Formatted: Font: (Default) Arial, 10 pt, Italic

Formatted: Font: (Default) Arial, 10 pt

Formatted: Space After: Auto

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: 10 pt, Not Bold

and/or associated internet protocol (IP address) is assigned to the defendant or evidence circumstantially tying the defendant to a screen name or IP address.

- Security measures such as password-protections for showing control of the account of the sender and excluding others from being able to use the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429)
- The sender takes action consistent with the content of the communication.
- The content of the communication identifies the sender or refers to matters that only the writer would have been aware.
- The alleged sender possesses information given to the user of the screen name (contact information or other communications given to the user of the screen name).
- Evidence discovered on the alleged sender's computer reflects that the user of the computer used the screen name. (See *U.S. v. Tank* (9th Cir. 2000) 200 F.3d 627.)
- In the majority of cases it is a variety of circumstantial evidence that provides the key to establishing the authorship and authenticity of a computer record. For further information, please consult the federal evidence portion of this CD-ROM. [\[click here\]](#)

C. Common ways to authenticate social media postings include:

- Testimony from a witness, including a police officer, with training and experience regarding the specific social media outlet used testified about what s/he observed. (*In re K.B.* (2015) 238 Cal.App.4th 989.) What is on the website or app, at the time the witness views it, should be preserved in a form that can be presented in court.
- Evidence of social media postings obtained from a phone, tablet or computer taken directly from the sender/receiver, or in the sender/receiver's possession.
- Testimony from the person who posted the message.
- Chain of custody following the route of the message or post, coupled with testimony that the alleged sender had primary access to the computer where the message originated.
- The content of the post refers to matters that only the writer would have been aware.
- After the post on social media, the writer takes action consistent with the content of the post.
- The content of the post displays an image of the writer. (*People v. Valdez* (2011) 201 Cal.App.4th 1429)
- Other circumstantial evidence including that the observed posted images were later recovered from suspect's cell phone and the suspect was wearing the same clothes and was in the same location that was depicted in the images. (*In re K.B.* (2015) 238 Cal.App.4th 989.)
- Security measures for the social media site such as passwords-protections for posting and

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Arial Unicode MS, 12 pt

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: 10 pt, Not Bold

deleting content suggest the owner of the page controls the posted material. (*People v. Valdez* (2011) 201 Cal.App.4th 1429

In the majority of cases it is a variety of circumstantial evidence that provides the key to establishing the authorship and authenticity of a computer record. "Mutually reinforcing content" as well as "pervasive consistency of the content of the page" can assist in authenticating photographs and writings. (*People v. Valdez* (2011) 201 Cal.App.4th 1429, 1436.) For further information, please consult the federal evidence portion of this CD-ROM. [\[click here\]](#) For examples of sufficient circumstantial evidence authenticated social media posts see, *Tienda v. State* (Tex. Crim. App. 2012) 358 S.W.3d 633, 642; *Parker v. State* (Del. 2014) 85 A.3d 682, 687. Contrast, *Griffin v. State* (2011) 419 Md. 343, 356–359.

D. Authenticating Texts:

A text message is a writing within the meaning of Evidence Code section 250, which may not be admitted in evidence without being authenticated. (*Stockinger v. Feather River Community College* (2003) 111 Cal.App.4th 1014, 1027–1028.) A text message may be authenticated "by evidence that the writing refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the proponent of the evidence to be the author of the writing" (Evid. Code, § 1421), or by any other circumstantial proof of authenticity (*id.*, § 1410).

As of August 2016, there are no published California cases that specifically discuss what is required for authenticating a text message. Unpublished CA opinions are consistent with the rule set forth above for authenticating e-mails and chats through a combination of direct and circumstantial evidence based on the facts of the case. Because of the mobile nature of smart phones, the proponent must take care to tie the declarant to the phone from which texts were seized or to the phone number listed in records obtained from the phone company. Often this done through cell phone records or the phone being seized from the defendant, his home or car or other witnesses testifying that this was how they communicated with the defendant.

Published opinions from other jurisdictions and unpublished opinions from CA provide some guidance:

- Victim testified he knew the number from which text was sent because Defendant told him the number. The contents of the texts referred to victim as a snitch. The defendant called the victim during the course of the text message conversation. (*Butler v. State*, 459 S.W.3d 595 (Crim. Ct App. Tx. April 22, 2015)).
- Testimony of records custodian from telecommunications company, explaining how company kept records of actual content of text messages, the date and time text messages were sent or received, and the phone number of the individuals who sent or received the messages, provided proper foundation for, and sufficiently authenticated, text messages admitted into evidence in trial on armed robbery charges. Fed.Rules Evid.Rule 901(a), 28 U.S.C.A., *U.S. v. Carr* (11th Cir. 2015) 607 Fed.Appx. 869.
- Ten of 12 text messages sent to victim's boyfriend from victim's cellular telephone following sexual assault were *not* properly authenticated to extent that State's evidence did not demonstrate that defendant was author of text messages. (*Rodriguez v. State* (2012) 128 Nev. Adv. Op. 14, [273 P.3d 845]
- Murder victim's cell phone recovered from scene of crime. Forensic tools used on phone recovered texts back and forth between victim and defendant. *People v. Lehmann* (Cal. Ct. App., Sept. 17, 2014, No. G047629) 2014 WL 4634272, at *8, review denied (Dec. 17,

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: (Default) Arial, 10 pt

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: Not Bold

Formatted: Bulleted + Level: 1 + Aligned at: 0.48" + Indent at: 0.73"

Formatted: Font: Italic

Formatted: Indent: Left: 0.23"

Formatted: Font: (Default) Arial, 10 pt

Formatted: Space After: 12 pt, Bulleted + Level: 1 + Aligned at: 0.48" + Indent at: 0.73"

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: (Default) Arial, 10 pt, Italic

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: Italic

Formatted: Font: (Default) Arial, 10 pt

Formatted: Bulleted + Level: 1 + Aligned at: 0.48" + Indent at: 0.73"

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: 10 pt, Not Bold

E. Authenticating Metadata:

Another way in which electronic evidence may be authenticated is by examining the metadata for the evidence. Metadata, "commonly described as 'data about data,' is defined as 'information describing the history, tracking, or management of an electronic document.' Metadata is 'information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information).' Some examples of metadata for electronic documents include: a file's name, a file's location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept." Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Federal Rule 901(b)(4).

Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because, "[a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide authorization for selected network administrators to override an individual password identification number to gain access when necessary. Metadata markers can reflect that a document was modified when in fact it simply was saved to a different location). Despite its lack of conclusiveness, however, metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics. *Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 547-48 [citations omitted]

F. Challenges to Authenticity

Challenges to the authenticity of computer records often take on one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created.

Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. California state courts have refused to require, as a prerequisite to admission of computer records, testimony on the "acceptability, accuracy, maintenance, and reliability of ... computer hardware and software." (*People v. Lugashi* (1988) 205 Cal.App.3d 632, 642) As *Lugashi* explains, although mistakes can occur, "such matters may be developed on cross-examination and should not affect the admissibility of the [record] itself." *People v. Martinez* (2000) 22 Cal.4th 106, 132.

Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author. For further information, please consult "Defeating Spurious Objections to Electronic Evidence," by Frank Dudley Berry, Jr., [\[click here\]](#) or the federal evidence portion of this CD-ROM. [\[click here\]](#)

6 | Introducing Digital Evidence in California State Courts

Formatted: Font: (Default) Arial, 10 pt, Font color: Black

Formatted: Indent: Left: 0.23"

Formatted: Font: (Default) Arial, 10 pt

Formatted: Space Before: 0 pt, After: 12 pt, Line spacing: single, No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Arial, 10 pt

Formatted: Font: (Default) Arial, 10 pt

Formatted: Space Before: 0 pt, After: 0 pt, Line spacing: single, No bullets or numbering

Formatted: Font: 10 pt, Not Bold

III. Former Best Evidence Rule

Reminder: The Best Evidence Rule has been replaced in California with the Secondary Evidence Rule. The Secondary Evidence Rule allows the admissibility of copies of an original document. (Evid. Code, § 1521.) They are not admissible, however, if "a genuine dispute exists concerning material terms of the writing and justice requires the exclusion," or if admitting the evidence would be "unfair." (Evid. Code, § 1521.)

In a criminal action it is also necessary for the proponent of the evidence to make the original available for inspection at or before trial. (Evid. Code, § 1522.) For email or any electronic document, this is especially important, given the wealth of information contained in its electronic format, as opposed to its paper image.

Of interest, Evidence Code Section 1522 requires that the "original" be made available for inspection. Evidence Code Section 255 defines an email "original" as any printout shown to reflect the data accurately. Thus, the protections offered by Evidence Code Section 1522 are stripped away by Evidence Code Section 255. This is where the protections of Evidence Code Section 1521 are invoked: "It's unfair, your Honor, not be able to inspect the email in its original format."

Also, remember that Evidence Code Section 1552 states that the printed representation of computer information or a computer program is presumed to be an accurate representation of that information. Thus, a printout of information will not present any "best evidence rule" issues absent a showing that the information is inaccurate or unreliable.

Oral testimony regarding the content of an email (writing) is still inadmissible absent an exception. (Evid. Code, § 1523.) Exceptions include where the original and all the copies of the document were accidentally destroyed.

Of course, none of the above rules applies at a preliminary hearing. (See Pen. Code § 872.5 [permits otherwise admissible secondary evidence at the preliminary hearing]; B. Witkin, 2 California Evidence (3rd ed., 1986) § 932, p. 897 ["secondary evidence" includes both copies and oral testimony].)

III.V. Hearsay Rule

The first question to ask is whether or not the information within the document is hearsay. If it is hearsay, then you need an applicable exception, such as business and government records or statement by party opponent. Examples of things that are *not* hearsay include: 1) operative facts and 2) data that is generated by a mechanized process and not a human declarant and, 3) A statement being used to show its falsity not its truth.

Formatted: Font: Italic

A. Operative Facts Documents in General

Formatted: Font: Bold

Formatted: Font: Bold

Where "the very fact in controversy is whether certain things were said or done and not ... whether

Formatted: Font: 10 pt

Formatted: Font: 10 pt, Not Bold

7. Introducing Digital Evidence in California State Courts

these things were true or false. ... in these cases the words or acts are admissible not as hearsay[,] but as original evidence." (1 Witkin, Cal. Evidence (4th ed. 2000) Hearsay, § 31, p. 714. For example, in an identity theft prosecution, there will be no hearsay issue for the majority of your documents. -The documents are not being offered for the truth of the matter asserted; they are operative facts. In *Remington Investments, Inc v. Hamedani* (1997) 55 Cal.App.4th 1033, the court distinguished between the concept of authentication and hearsay. The issue was whether a promissory note was admissible. The court observed that: 'The Promissory Note document itself is not a business record as that term is used in the law of hearsay, but rather an operative contractual document admissible merely upon adequate evidence of authenticity. (Id. At 1043.)

Formatted: Font: 10 pt

Under Remington, promissory notes, checks and other contracts are not hearsay, but operative facts. Moreover, forged checks, false applications for credit, and forged documents are not hearsay. They are not being introduced because they are true. They are being introduced because they are false. Since they are not being introduced for the truth of the matter asserted there is no hearsay issue.

Other examples of non-hearsay operative facts documents would include:

- The words forming an agreement are not hearsay (*Jazayeri v. Mao* (2009) 174 Cal.App.4th 301, 316 as cited by *People v. Mota* (Cal. Ct. App., Oct. 8, 2015, No. B252938) 2015 WL 5883710 (Unpublished).
- A deposit slip and victim's identification in a burglary case introduced to circumstantially connect the defendant to the crime. (*In re Richard* (1979) 91 Cal.App.3d 960, 971-979.)
- Pay and owes in a drug case. (*People v. Harvey* (1991) 233 Cal.App.3d 1206, 1222-1226.)
- Items in a search to circumstantially connect the defendant to the location. (*People v. Williams* (1992) 3 Cal.App.4th 1535, 1540-1543.)
- Invoices, bills, and receipts are generally hearsay unless they are introduced for the purpose of corroborating the victim's damages. (*Jones v. Dumrichob* (1998) 63 Cal.App.4th 1258, 1267.)
- Defendant's social media page as circumstantial evidence of gang involvement. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.
- Generally, photographs, video, and instrument read outs are not statements of a person as defined by the Evidence Code. (Evid.Code §§ 175, 225; *People v. Goldsmith* (2014) 59 Cal.4th 258, 274; *People v. Lopez* (2012) 55 Cal.4th 569, 583.)

Formatted: Font: (Default) Arial, 10 pt

Formatted: Space Before: 0 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Arial, 10 pt, Font color: Black

Although the check itself is not hearsay, the bank's notations placed on the back of the check showing that it was cashed is hearsay. The bank's notations would be introduced for the truth of the matter asserted – that the check was cashed. Evidence Code sections 1270 and 1271 solve this problem by allowing the admission of these notations as a business record.

Two helpful rules that apply to business records. First, it may be permissible to infer the elements of the business record exception. In *People v. Dorsey* (1974) 43 Cal.App.3d 953, the court was willing to find that it was common knowledge that bank statements on checking accounts are prepared daily on the basis of deposits received, checks written and service charges made even though the witness

Formatted: Font: 10 pt, Not Bold

failed to testify as to the mode and time of preparation of bank statements. The second rule is that "lack of foundation" is not a sufficient objection to a business record. The defense must specify which element of the business record exception is lacking. (*People v. Fowzer* (1954) 127 Cal.App.2d 742.)

~~Finally, an official record is very similar to a business record. The chief difference is that it may be possible to introduce an official record without calling the custodian or another witness to authenticate it. (Evid. Code, § 1280.) The foundation can be established through other means such as judicial notice or presumptions. (*People v. George* (1994) 30 Cal.App.4th 262, 274.)~~

Formatted: Font: Bold

B. Computer Records Generated by a Mechanized Process

The first rule is that a printout of the results of the computer's internal operations is not hearsay evidence ~~because hearsay requires a human declarant. Evid. Code §§ 175, 225. The Evidence Code does not contemplate that a machine can make a statement. *People v. Goldsmith* (2014) 59 Cal.4th at 258, 274 (rejecting hearsay claims related to red light cameras); *People v. Hawkins* (2002) 98 Cal.App.4th 1428; *People v. Lopez* (2012) 55 Cal. 4th 569.~~ These log files are computer-generated records that do not involve the same risk of observation or recall as human ~~declarants~~ declarants. Thus, email header information and log files associated with an email's movement through the Internet are not hearsay. ~~The usual analogy is that the clock on the wall and a dog barking are not hearsay.~~ An excellent discussion on this issue can be found on the federal evidence portion of this CD-ROM. [\[click here\]](#) [\[click here\]](#)

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Space Before: 0 pt, After: 0 pt, Line spacing: single, No widow/orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Italic

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Italic

Formatted: Font: (Default) Arial, Font color: Auto

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: Italic

Formatted: Superscript

Formatted: Default Paragraph Font, Font color: Black

Formatted: Default Paragraph Font, Font color: Black

Formatted: No underline, Font color: Auto

Formatted: Font: Italic

Formatted: Font: Bold

Metadata such as date/time stamps are not hearsay nor do they violate the confrontation clause because they are not testimonial. See, *People v. Goldsmith* 59 Cal.4th at 258, 274-275; *People v. Lopez* (2012) 55 Cal. 4th 569, 583.

C. Business Records

Log files and other computer-generated records from Internet Service Providers ~~may will~~ also easily qualify ~~under the business records exception to the hearsay rule as business records. Evid. Code §§ 1270, 1271, 1560, 1561.~~ Remember, you do not need to show the reliability of the hardware or software. *People v. Lugashi* (1988) 205 Cal.App.3d 632. Nor does the custodian of records need to completely understand the computer. *Id.* Additionally, the printout (as opposed to the entry) need not be made "at or near the time of the event." *Aguimatang v. California State Lottery* (1991) 234 Cal.App.3d 769. Finally, a cautionary note from the Appellate Court in *People v. Hawkins* (2002) 98 Cal.App.4th 1428: "the true test for admissibility of a printout reflecting a computer's internal operations is not whether the printout was made in the regular course of business, but whether the computer was operating properly at the time of the printout."

If the computer is used merely to store, analyze, or summarize material that is hearsay in nature, it will not change its hearsay nature and you will need an applicable exception for introduction. Common exceptions for the contents of email include: statement of the party, adoptive admission, statement in furtherance of a conspiracy, declaration against interest, prior inconsistent statement, past recollection recorded, business record, writing as a record of the act, or state of mind.

Note also that records obtained by search warrant, and accompanied by a complying custodian affidavit, are admissible as if they were subpoenaed into court (Evid. Code §§ 1560-1561, effective January 1, 2017) and records obtained from a Electronic Communication Service provider that is a

Formatted: Font: 10 pt, Not Bold

foreign corporation, and are accompanied by a complying custodian affidavit, are currently admissible pursuant to Penal Code § 1524.2(b)(4).

D. Government Records

An official record is very similar to a business record, even if it is obtained from a government website. The chief difference is that it may be possible to introduce an official record without calling the custodian or another witness to authenticate it. (Evid. Code, § 1280.) The foundation can be established through other means such as judicial notice or presumptions. People v. George (1994) 30 Cal.App.4th 262, 274.

Formatted: Font: Bold

E. Published Tabulations

Finally, prosecutors are often plagued with how to introduce evidence that was found using Internet-based investigative tools. For example, if your investigator used the American Registry For Internet Numbers (ARIN) programs (WHOIS, RWhois or Routing Registry Information), how is this admissible without calling the creator of these Internet databases? Evidence Code Section 1340 allows an exception to the hearsay rule, which allows the introduction of published tabulations, lists, directories, or registers. The only requirement is that the evidence contained in the compilation is generally used and relied upon as accurate in the course of business.

Formatted: Space Before: 0 pt, After: 0 pt, Line spacing: single, No widow/orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: Bold

IV. Former Best Evidence Rule

Reminder: The Best Evidence Rule has been replaced in California with the Secondary Evidence Rule. The Secondary Evidence Rule allows the admissibility of copies of an original document. (Evid. Code, § 1521.) They are not admissible, however, if "a genuine dispute exists concerning material terms of the writing and justice requires the exclusion," or if admitting the evidence would be "unfair." (Evid. Code, § 1521.)

In a criminal action it is also necessary for the proponent of the evidence to make the original available for inspection at or before trial. (Evid. Code, § 1522.) For email or any electronic document, this is especially important, given the wealth of information contained in its electronic format, as opposed to its paper image.

Of interest, Evidence Code Section 1522 requires that the "original" be made available for inspection. Evidence Code Section 255 defines an email "original" as any printout shown to reflect the data accurately. Thus, the protections offered by Evidence Code Section 1522 are stripped away by Evidence Code Section 255. This is where the protections of Evidence Code Section 1521 are invoked: "It's unfair, your Honor, not be able to inspect the email in its original format."

Also, remember that Evidence Code Section 1552 states that the printed representation of computer information or a computer program is presumed to be an accurate representation of that information. Thus, a printout of information will not present any "best evidence rule" issues absent a showing that the information is inaccurate or unreliable.

Oral testimony regarding the content of an email [writing] is still inadmissible absent an exception. (Evid. Code, § 1523.) Exceptions include where the original and all the copies of the document were accidentally destroyed.

Formatted: Font: 10 pt, Not Bold

Of course, none of the above rules applies at a preliminary hearing. (See Pen. Code § 872.5 [permits otherwise admissible secondary evidence at the preliminary hearing], B. Witkin, 2 California Evidence (3rd ed., 1986) § 932, p. 897 ["secondary evidence" includes both copies and oral testimony].)

[Return to top](#)

Formatted: Indent: Left: 0.33"

Formatted: Font: 10 pt, Not Bold