# Introducing Digital Evidence in California State Courts[i]

## 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 to 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. Br*owne (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. Valde*z (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 achieved website].)

The underlying challenge for web sites in 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, at 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 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. Golds*mith (2014) 59 Cal.4th 258, 274; *People v. Lop*ez (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.

The elements of the published compilation hearsay exception are: (1) the proffered statement must be contained in a compilation; (2) the compilation must be published; (3) the compilation must be generally used in the course of a business; (4) it must be generally relied upon as accurate in the course of such business; and (5) the statement must be one of fact rather than opinion. *(People v Mooring* (2017) __ Cal. Rptr.3d. __ [2017 WL 4277567] [Pharmaceutical pill identification Internet web site was within the published compilation exception].)

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].)

---

[i] 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.