California LAWYER
"the Web portal for California's lawyers"

MCLE

Using Email as Evidence at Trial

A number of issues may come up when using email as evidence.

BY MARK MERMELSTEIN AND CHRISTIN J. HILL | AUGUST 2015

CONTINUE TO TEST

Email evidence has dramatically changed the way cases are tried. Not only do juries expect to hear from live witnesses, they also want to see the emails and text messages relating to the dispute. An email properly deployed at trial may well eclipse even live testimony. For example, if a key witness's independent recollection of events (also a focal point at trial) is inconsistent with a contemporaneous email, the testimony may well be viewed as irrelevant—or worse, as indicating the witness is lying.

But be warned: Just because the communication is an email does not mean it's admissible into evidence. Indeed, even more so than traditional documents, emails are ripe for challenges based on both authenticity and hearsay. For example, emails do not contain a handwritten signature, and often times they omit even an electronic signature. Furthermore, emails are highly susceptible to manipulation after the fact: An email forwarded to another recipient can be altered with ease and often without detection. Also, with long email chains there may be multiple layers of hearsay, not to mention the possibility of conflicting time stamps if senders and recipients reside in different time zones. But perhaps most problematic of all, email has become so ubiquitous that senders often do not apply much forethought or discretion when shooting off what they perceive to be a casual message. Such a message may be loaded with charged language or insensitive humor that is easily taken out of context.

Despite all the inherent challenges, email is here to stay. Therefore, it is essential for advocates to understand how to effectively use email communications at trial.

The approach a litigator takes to email will differ depending on whether the email in question is helpful or harmful to the client. The proponent of the email needs to know the rules to make sure to get it in front of the fact finder, and to use it effectively. At the same time, the opponent of the email needs to know the rules to try to keep it out, or at least how to deal with a harmful email that will be admitted into evidence.

Hypothetical Case

Consider this hypothetical: Brian, the CEO of a large pharmaceutical company (Large Pharma, Inc.) faces criminal prosecution for agreeing with Alex, the CEO of a competing company (Rival Drug Co.), to divide up the world market for a new vitamin supplement. Their respective companies are the only significant players in the relevant market. Through discovery, the prosecutor has obtained a copy of an email exchange between Brian and his assistant, Charlie:

Charlie Smith

From: Charlie Smith <Charlie@LargePharma.com>
Sent: Thursday, April 1, 2015 3:00 PM
To: Brian Jones@LargePharma.com
Subject: Dinner with Alex

Hi Brian,

How did dinner with Alex go yesterday? Did you agree to split?

Charlie

Charlie Smith
Executive Assistant to CEO Brian Jones
Large Pharma

Brian Jones

From: Brian Jones <Brian@LargePharma.com>
Sent: Thursday, April 1, 2015 3:10 PM
To: Charlie Smith@LargePharma.com
Subject: Dinner with Alex

Charlie,
Please see me!
Brian

Authentication Dynamics

The prosecutor will seek admission of the email as evidence that Brian discussed with Alex an illegal scheme to "split up" the vitamin market and that Brian knew this was illegal, since he directed a subordinate (Charlie) to take the conversation offline.

The prosecutor will first need to authenticate the email. California law provides that authentication of a writing is required before it may be received into evidence. (See Cal. Evid. Code §§ 1401.) The parallel federal rules articulate the basic test: "[T]he proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." (Fed. R. Evid. 901(a).) And remember, if there is a chain of emails, authentication will be required for each "link" of the chain. (See *SDS Korea Co., Ltd. v. SDS USA, Inc.*, 732 F. Supp. 2d 1062 (S.D. Cal. 2010).)

The main authentication challenge to emails is authorship. How can you verify the true sender of an email? Even in the presence of an electronic signature or the sender's name, it is conceivable that someone other than the purported sender logged into the author's account and drafted and sent the email. Furthermore, there is an ever-present risk of manipulation, alteration, or corruption of the email after the fact.

In our hypothetical, let's assume that Brian will not testify because in a criminal prosecution he has the right to remain silent under the Fifth Amendment. Therefore, the prosecutor will need to authenticate the email without relying on Brian's testimony. There are several options to accomplish this:

• The prosecutor can ask the defendant to stipulate to the authentication of emails. (See *County of Alameda v. Risby* 28 Cal. App. 4th 1425, 1430 (1994).) Because it is likely that Brian will have emails that he wants to use in his defense, the prosecutor may wish to offer a stipulation that allows for authentication of all emails produced from the company's server. In federal court, this issue can be raised early on at the Rule 26 conference that precedes the onset of discovery.

• The prosecutor could have Charlie authenticate the email through testimony.

• The email may be self-authenticating. Under federal law, documents are self-authenticating when there is "[an] inscription, sign, tag, or label purporting to have been affixed in the course of business and indicating origin, ownership, or control." (Fed. R. Evid. 902(7).) Even if it is not truly self-authenticating, an email can be authenticated based on its distinguishing features, such as "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." (See Fed. R. Evid. 901(b)(4); *United States v. Safavian*, 435 F. Supp. 2d 36, 39–40 (D.D.C. 2006), rev'd on other grounds, 528 F.3d 957 (D.C. Cir. 2008).)

• In the civil context, a request for admissions may be used to authenticate email. (See *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 553 (D. Md. 2007).)

Keeping It Out

Understanding the negative implications the email may provoke—and the import juries ascribe to email communications in general—defense counsel will likely challenge the admissibility of the Brian-Charlie emails. To do so, defense counsel should consider a motion in limine. Such a motion will allow the opponent of the email to argue the admissibility issue outside the presence of the jury. If the opponent's argument is successful, the jury could be precluded from even learning of the email's existence.

In challenging authentication, defense counsel often argue that an email message should be excluded because it could have been altered or manipulated. It is certainly possible that Charlie—or someone else—altered the email to fabricate evidence. However, absent real evidence of affirmative manipulation, this argument is unlikely to be persuasive. Numerous courts have held that the existence of a mere possibility of manipulation does not automatically lead to exclusion of electronic evidence on authentication grounds. (See *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988); *Safavian*, 435 F. Supp. 2d at 39–40 ("The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents)." (emphasis by the court)).)

However, when there is concrete evidence of manipulation, opponents should vigorously seek exclusion on authentication grounds.

Is It Relevant?

An alternative challenge is to argue that the communication is not relevant. For evidence to be admissible, it must be relevant to the case without being unfairly prejudicial. (Fed. R. Evid. 402, 403; Cal. Evid. Code §§ 350, 352.) Going back to our hypothetical, defense counsel could argue that there is no evidence that Brian's email occurred after Charlie's email (because the time stamps may be off). And if Brian's email came first, it could merely show a boss asking for a meeting with his assistant in an irrelevant exchange.

Defense counsel could also argue that any probative value from the email is outweighed by the time-consuming and prejudicial endeavor of determining what the word *split* means. In this regard, there would no doubt be a pitched battle over the term: Defense counsel would argue *split* refers to splitting the dinner bill; the prosecution would assert that it refers to criminal collusion to split the market. Defense counsel will argue that this skirmish would result in an unnecessary departure from the real issues, in effect amounting to a diversionary "trial within a trial." (See *People v. Hamilton*, 45 Cal. 4th 863, 930 (2009) (finding that the trial court did not abuse its discretion under Cal. Evid. Code § 352 by excluding evidence that "would have required 'a mini-trial.' ").)

A final means of excluding the email would be a motion in limine based on hearsay. All first-year law students (and many fans of television courtroom dramas) know that hearsay is presumptively inadmissible. (See Fed. R. Evid. 802; Cal. Evid. Code § 1200.) Email, like all evidence, is subject to the hearsay rule.

Defense counsel would likely argue that the email in question constitutes hearsay, and it certainly does meet the basic definition of that term: an out-of-court statement offered for the truth of the matter asserted.

Is It an Admission?

The first and simplest way to avoid the hearsay rule is to sidestep it entirely by arguing the email is not hearsay at all. Both the California Evidence Code and the Federal Rules provide that admissions by a party opponent do not constitute hearsay. (See Cal. Evid. Code § 1220; Fed. R. Evid. 801 (d)(2).). In our hypothetical, the prosecution could argue there has been an adoptive admission because Brian did not deny "splitting" when he responded to Charlie.

Hearsay Exceptions

Even if an email qualifies as hearsay, numerous exceptions have been applied to email communications. In fact, the vast majority of corporate emails are introduced under the business-records exception. The standard for electronic business records is the same as for paper business records. For a document to be admissible as a business record, the following conditions must be satisfied: (1) the writing was made in the regular course of business, (2) it must have been made at or near the time of the act, condition, or event it describes, (3) a qualified witness testifies to the identity of the record and how it was prepared, and (4) the method and time of preparation of the record were such as to indicate its trustworthiness. (See Cal. Evid. Code § 1271; Fed. R. Evid. 803(6).)

Courts have applied this exception to admit emails as business records. (See *Pierre v. RBC Liberty Life Ins.*, No. 05-1042-C, 2007 WL 2071829, at *2 (M.D. La.) (finding that emails fell within Rule 803(6) because they "were prepared by ... employees during the ordinary course of business.").) Even so, application of the business-records exception is not automatic. Failure to establish that emails were actually prepared in the regular course of business can result in their exclusion. (See *State of New York v. Microsoft Corp.*, 2002 WL 649951, at *2 (D.D.C.) (declining to admit emails under the business-records exception because there was a "complete lack of information regarding the practice of composition and maintenance of [the] e-mails."); *United States v. Ferber*, 966 F. Supp. 90, 99 (D. Mass. 1997) (declining to admit emails as business-records because the author of the emails "was under no business duty to make and maintain" them.).)

State of Mind

Our hypothetical email may also qualify under the state-of-mind exception to the hearsay rule. California law provides for the admissibility of out-of-court statements when "[t]he evidence is offered to prove the declarant's state of mind, emotion, or physical sensation at that time or at any other time when it is itself an issue in the action." (Cal. Evid. Code § 1250; see also Fed. R. Evid. 803(3).) Bear in mind that in this context the "immediacy" of the memorialization of events will be critical.

An email may also qualify as a "past recollection recorded." However, in that instance the email itself may not actually come into evidence, but it can still be useful as a tool to refresh a witness's faded memory. (See Cal. Evid. Code § 1237; Fed. R. Evid. 803(5).)

Using the Email

Assuming that our hypothetical email has been admitted into evidence, how should counsel take advantage of it?

The prosecutor's goal will be to establish that Brian's "please see me" was a deliberate avoidance of Charlie's question so as to avoid a paper trail of illegal conduct. To accomplish this, the prosecutor would likely call Charlie to testify. After authentication of the email, the prosecutor might enlarge an image of the email on a video screen and then question Charlie about the conversation that took place after the message was received.

In taking this approach, it is to the proponent's benefit to introduce the email *before* the witness has an opportunity to give testimony that deviates from the email's content, so that the witness is locked into the statements in the email and disinclined to tell another story. At this point, the prosecutor will want Charlie to confirm that Brian moved the conversation offline, as the text of the email suggests.

In response, defense counsel will likely have some cleaning up to do. The first step for dealing with a harmful email is to contextualize it. Defense counsel would be well served to introduce other situations in which Brian liked to have oral conversations about innocuous topics simply because it was more convenient than corresponding via email. Also helpful would be evidence showing that Charlie used the word *split* to refer to splitting the dinner tab as opposed to splitting up the market. Finally, evidence indicating that Charlie was not aware of any illegal scheme (and therefore could not be inquiring about illegal conduct) would be helpful. In any event, it is crucial to learn about Charlie's view of the email in advance.

As the trial court recognized in *Safavian*, "[w]e live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world." (435 F. Supp. 2d at 41.) Indeed, email evidence is a powerful tool that can bolster consistent testimony or undercut inconsistent evidence. For that reason, trial lawyers should devote considerable time to analyzing the admissibility issues surrounding email communications. Lawyers who master these points will be best equipped to deal nimbly with email in the midst of trial.

Mark Mermelstein is a Los Angeles–based partner and Christin J. Hill is a San Francisco–based senior associate at Orrick, Herrington & Sutcliffe. Mermelstein also chairs the firm's Cybersecurity and Data Privacy Group.

CONTINUE TO TEST