Commentary: Authenticating Social Media Evidence in California, the Social Media Capital of the World

by
Rahul Gupta*

Hollywood, California, is known as the movie capital of the world. But Silicon Valley, California, has become the social media capital of the world. Social media companies such as Facebook, YouTube, and Twitter now reach more than two billion people around the world every day.[1] Americans alone spend approximately 6½ hours per week on social media, which equates to checking their social media almost 17 times per day and at least once every waking hour.[2] The dramatic increase in social media activity has created a treasure trove of evidence for both criminal and civil attorneys. This article will highlight three California cases that provide guidance on how to authenticate and lay the proper foundation for social media evidence.

I. What Type of Evidence Is Social Media?

In California, social media evidence presented in the form of documents, photographs, or videos are simply considered writings.[3] For example, a Facebook post could be offered as a screenshot printed as a document or photograph or a YouTube

* Senior Deputy District Attorney, Orange County, CA District Attorney's Office.

1 Joe Hyrkin, *Silicon Valley Is Now the Media Capital of the World*, RECODE (Nov 17, 2016), https://www.recode.net/2016/11/17/13667434/silicon-valley-media-capital-content-distribution.

2 *2016 Nielsen Social Media Report Social Studies: A Look at the Social Landscape*, NIELSEN, http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2017-reports/2016-nielsen-social-media-report.pdf (last visited Jan. 2, 2018).

3 CAL. EVID. CODE § 250 (2017) ("'Writing' means handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing, any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record

video would be introduced on a CD or DVD. This provides an easy way for the witness and jurors to view the evidence and also allow it to be marked as evidence without the necessity of the original cell phone or laptop from which it came. As a practical matter, social media evidence will usually take the form of a document, photo, or video because it is often impractical and unnecessary to admit the original cell phone, laptop, or even server upon which the social media evidence was created. In many instances attorneys may not have the original electronic device which contains the social media evidence. Even if such evidence is available, displaying the social media content on such a device to the jury is often impractical and may jeopardize the integrity of the original evidence.[4]

II. What Type of Authentication Is Necessary for Writings?

Authentication of social media evidence in the form of a document, photo, or video requires the proponent to make a sufficient showing that the evidence is what it purports to be by any means provided by law.[5] In California, there is no restriction on the means by which a writing may be authenticated, including but not limited to, a percipient witness, content, location, statutory presumption, or even circumstantial evidence.[6] The most common challenge to authenticating social media evidence will be from the opposing counsel objecting to the evidence as "doctored" or "photo-shopped." However, the proponent's threshold authentication burden for admissibility is not to establish validity or negate falsity in a categorical fashion, but rather to make a showing on which the trier of fact reasonably could conclude the proffered writing is authentic.[7] The fact that con-

---

thereby created, regardless of the manner in which the record has been stored."). *See also* People v. Goldsmith, 59 Cal. 4th 258 (2014).

4 *See* Paul W. Grimm et. al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1 (2017); Nicole A. Keefe, Note, *Dance Like No One Is Watching, Post Like Everyone Is: The Accessibility of "Private" Social Media Content in Civil Litigation*, 19 VAND. J. ENT. & TECH. L. 1027 (2017).

5 CAL. EVID. CODE § 1400 (2017).

6 CAL. EVID. CODE §§ 1410, 1400.

7 People v. Valdez, 201 Cal. App. 4th 1429 (2011).

flicting inferences can be drawn regarding authenticity goes to the document's weight as evidence, not its admissibility.[8]

III. The Challenge of Authenticating Social Media Evidence in Court

The challenge with social media evidence is often that the greater value it has to a case, the less likely one may be to have a witness to authenticate the evidence. These three California cases, *People v. Valdez*,[9] *In re KB*,[10] and *Kinda v. Carpenter*,[11] highlight different ways to overcome that challenge and provide guidance in authenticating social media evidence no matter what jurisdiction you practice in.

A. *The Myspace Page*

In *People v. Valdez*,[12] the court dealt with the most common situation, the introduction of social media evidence from a traditional profile page of a known individual's public Myspace account. In *Valdez*, the prosecutor introduced a photograph and printouts from the defendant's Myspace social media account which assisted in securing convictions for attempted murder, firearm possession, and gang enhancements. On appeal, the reviewing court upheld the conviction and found that the Myspace photo had been properly authenticated. The court affirmed the conviction based upon the testimony of the investigator who located the defendant's Myspace page and the pervasive consistency of gang indicia found throughout the social media account.

In *Valdez*, the defendant was faced with gang charges, and his Myspace social media account contained a wealth of valuable gang evidence for the prosecutor, including the defendant's profile picture. The Myspace profile picture was a close up of the defendant's hand in front of his face displaying his gang hand sign. The prosecutor sought to admit the social media evidence to corroborate the victim's identification of the defendant and foundation for the gang expert's opinion. Additionally, throughout

---

8 *Id.* at 1430.

9 *See id.*

10 238 Cal. App. 4th 989 (2015).

11 247 Cal. App. 4th 1268 (2016).

12 201 Cal. App. 4th 1429.

the defendant's public Myspace pages, there were specific references to the defendant's gang, his gang moniker, posts between the defendant and his sister, and other information that circumstantially linked the defendant to the gang.

Although the court relied on the investigator's testimony, he was not uniquely qualified in social media expertise or even computers. The district attorney investigator had stumbled upon the defendant's Myspace profile page one year *prior* to the defendant's crime. As part of his ongoing gang research, the investigator simply did a Google search of the gang's name and city which revealed the defendant's public Myspace page. At trial, the investigator testified that he did not have a computer science degree, advanced computer training, or even specialized expertise in social media. The investigator testified that he had basic user experience with Myspace and described for the court how an account and profile is created, and how profiles can be viewed by the public, but that only the person with the password to the account can upload and edit the content on the pages of the account. Even more remarkable was what the investigator admitted not knowing. The investigator testified that he did not know who actually created the Myspace account, who uploaded the photos, or how many people may have shared the password to edit content on the account. The investigator never subpoenaed any records from Myspace or spoke to any custodian of records.

Despite the lack of computer expertise of the investigator, the court found the Myspace photo and printouts were properly authenticated:

> [T]he writings on the page and the photograph corroborated each other by showing a pervading interest in gang matters . . . this consistent, mutually-reinforcing content on the page helped authenticate the photograph and writings, with no evidence of incongruous elements to suggest planted or false material . . . "The page was password-protected for posting and deleting content, which tended to suggest [Valdez], as the owner of the page, controlled the posted material.[13]

Valdez is instructive because it establishes that public social media evidence found using Google can be authenticated without calling an expert witness and without calling a witness having a personal relationship to the party against whom the evidence is being introduced. The court's reliance on the relevant content of

---

13 *Id.* at 1430.

the social media to assist in its own authentication along with the emphasis on the account being password protected provides crucial guidance for litigators.

B. *The Instagram Post*

In the case of *In re KB*,[14] the court dealt with another common type of scenario, the introduction of social media evidence from a recent Instagram post. Here, the prosecutor introduced photographs identical to those the defendant had uploaded to Instagram, which ultimately led to his conviction for illegal firearms possession. The court again affirmed the conviction based upon testimony describing the basic functionality of the social media by the investigating officer, corroborating information from the social media content itself, and the fact that the social media account was password protected.

In this case, the defendant was one of three suspects possessing illegal firearms inside an apartment. The defendant was on probation and therefore prohibited from possessing any type of firearms. Nevertheless, the defendant posted photos of himself holding two different guns inside of his apartment but did not show his face. The photos posted online depicted only the firearms lowered near the waists of the three suspects. Also visible in the Instagram photos were the clothing worn by the three suspects and the interior of the apartment which appeared to have camouflage curtains. The defendant argued the Instagram photos could not be authenticated because no witness was called to testify to seeing him or his compatriots actually holding the firearms.

An officer from the San Francisco Police Department had become familiar with Instagram and had been using it to follow various suspects and probationers, including the defendant. The officer's familiarity and use of Instagram as an investigative tool earned him the nickname, the "Instagram Officer."[15] Soon after seeing the Instagram post and confirming the defendant's address and probation status, officers went to the defendant's residence and from the outside observed the same camouflage curtains depicted in the social media post. All three suspects

14 238 Cal. App. 4th 989.

15 *Id.* at 992.

were arrested wearing the same clothing depicted in the Instagram post, two firearms were collected that also matched those held by the suspects in the photos, and a cell phone was collected that belonged to a suspect, not the defendant. At the station, an analysis of the cell phone revealed photos of three suspects holding the two firearms that were identical to those the defendant had uploaded to his Instagram account. Although the Investigating Officer testified about the defendant's Instagram account and the firearm photos uploaded on the account, the prosecutor actually admitted the identical photos that were retrieved from the cell phone found at the scene that did not belong to the defendant.

At trial, just as in *Valdez*, the Investigating Officer testified to his user experience knowledge of Instagram, describing how an account is created, how photos are uploaded, how they are shared, and that each account is password protected. However, beyond that, just as in *Valdez*, the officer did not testify to having any specialized computer training or knowledge. Nor did the officer subpoena any documents from Instagram or speak to a custodian of records. The officer testified about the corroborating evidence between the Instagram posts and his observations at the scene. The appellate court upheld the conviction and stated, "when appellant was arrested, he was wearing the same clothes and was in the same location depicted in the photographs. He was arrested along with several of the same individuals who appear with him in the photographs."[16]

This case demonstrates that the timing, location, and content of a social media post corroborated by evidence observed and collected near the time of the post can establish authentication. Again, the court here relied upon a witness that explained how the social media account is created and whether it is password protected. Although, in both *Valdez* and *In re KB* both witnesses that supplied the foundation happened to be law enforcement officers, neither court held that was a requirement. Using these cases, any competent witness with sufficient familiarity with the social media account creation process could provide the court with adequate foundation to authenticate the social media.

---

16 *Id.* at 998.

C. *The Anonymous Yelp Review*

In *Kinda v. Carpenter*,[17] the court dealt with a particularly difficult and growing phenomenon, the introduction of social media from an unknown person's Yelp post. *Kinda* began as a commercial dispute between a tenant and landlord that grew into a defamation lawsuit. The plaintiff's rug business was housed in the defendant's commercial building. After the lawsuit arose, the plaintiff obtained a temporary restraining order against the defendant. That same day and on the following two days, negative Yelp reviews of the plaintiff's rug business were posted by anonymous accounts. The plaintiff could not reconcile the descriptions of poor service stated in the negative Yelp posts with actual customer orders. The timing of the posts made the plaintiff believe the defendant was behind the anonymous posts and the plaintiff obtained the IP addresses for the anonymous posts. The IP addresses came back to the defendant's residence and his commercial building address. The plaintiff added a cause of action for defamation against the defendant.

At the motion in limine hearing for the defamation suit, the plaintiff introduced the printed Yelp postings under a statutory presumption[18] and the IP address records with witness testimony from the custodian of records from the various internet service providers. The defense objected, claiming the printed anonymous Yelp posts could not be authenticated, and argued that the IP addresses information was lacking. The defense claimed that any of the defendant's employees at his business or any unauthorized person using his home wifi connection could have posted the negative Yelp reviews. The trial court agreed, stating, "[B]efore it comes into evidence, you have to give me some connection that you can prove he posted them. If you can't do that, I'm not going to let it into evidence."[19] The trial court excluded the evidence and issued a directed verdict for the landlord on the defamation action.

The plaintiff appealed and the higher court reversed the trial court's ruling to exclude the Yelp evidence and held the trial court applied the wrong standard for the authentication of the

---

17 238 Cal. App. 4th 989.

18 CAL. EVID. CODE § 1552.

19 *Kinda*, 247 Cal. App. 4th at 1285

social media evidence. The court discussed the circumstantial evidence that supported authentication as: 1) the date of the issuance of the temporary restraining order against the defendant, 2) the date of the subsequent negative anonymous Yelp reviews appearing immediately after, 3) the plaintiff's inability to reconcile the negative reviews with real customers, and 4) the IP addresses linked back to the defendant's residence and business. Although it did not establish a direct link showing the defendant posted the anonymous Yelp review, the appellate court found the slight circumstantial evidence surrounding the social media sufficient to meet the proponent's burden. "Even slight evidence in support of the fact to be inferred has been held to be sufficient. It is up to the jury to assess the credibility and judge the weight of the evidence proffered in support of and in opposition of the fact it is asked to infer."[20]

Kinda shows that even anonymous social media evidence can be authenticated through the use of modest circumstantial evidence. Similar to *In re KB*, the *Kinda* court recognized that the timing, location, and content of a social media post corroborated by evidence observed and collected near the time of the post can establish authentication.

IV. Conclusion

There are a myriad of ways to authenticate social media evidence for criminal and civil attorneys. These three cases are just a few examples that demonstrate how social media evidentiary issues are handled in courts across California. Since California is the social media capital of the world, hopefully these cases may also provide some guidance for you in your jurisdiction.

---

[20] *Id.* at 1289, *citing* Fashion 21 v. Coalition for Humane Immigrant Rights of Los Angeles, 117 Cal. App. 4th 1138, 1149 (2004).