FALL 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss social media discovery and important strategic legal insights and spooky innovative technologies.

Social Media Evidence Authentication – Verifying It Is What It Is

The FBI published an interesting story on its website about authentication of evidence in the context of a major art fraud that provides lessons relevant to authentication of social media evidence. In order to sell fake paintings, an infamous art dealer faked not only paintings, but also concocted provenances, which are written records that evidence the authenticity of a particular art piece. The key evidence in pursuing the fraudster was the spooled ribbon in an old typewriter that was used to forge bills of sale and letters that connected the dealer to the forgeries. After discovering the typewriter and the spooled ribbon that had recorded what was written, the FBI managed to place the forged documents close enough to the dealer to obtain a conviction on a $1.45 million fraud scheme. This anecdote highlights the importance of authenticating evidence and the clever ways in which authentication can be approached. For authenticating social media postings for admission in court, however, there is obviously no vintage typewriter with a spooled ribbon recording what was written (but certain metadata may be analogous), so key steps in this essential process of authentication are more difficult yet clearly not insurmountable, especially in certain jurisdictions. In this article, we look at the elements of social media authentication, and the case law guiding the process.

An Existential Test

The first goal of authenticating social media content is to prove that “it is what it is,” which in essence separates the content from the account. Federal Rule of Evidence 901 (a) establishes the hurdle of “sufficient evidence,” and 901 (b) provides for four possibilities to clear it: (1) testimony by a knowledgeable witness; (2) distinct identifying characteristics; (3) evidence about a process or system; and (4) self-authentication. A proposed amendment, which should become effective on December 1, 2017, will add to this list “affidavit of a qualified person” to authenticate electronically stored information, including social media account information, as long it complies with Rule 902 (11) and (12).

In the absence of contemporaneous evidence of authorship, e.g. video of the person posting the content in question, authentication starts with verifying that the evidence presented is a true copy of the social media account of the person who is identified in the subject profile. With regard to the account, there are several ways to establish that account is in control of the person identified as the profile holder.

(1) Direct testimony of the account holder. If the account holder will identify the social media account as being an account they created, or had someone create for them, and that they are in control of the account, courts will be satisfied.

(2) Totality of evidence approach. When direct testimony of the account holder is available or forthcoming, courts accept a totality of evidence that connects the account to the presumed holder. That evidence includes the following list, and the more that can be compiled, the better:

(A) Username and password information in control of the individual;

(B) Identifying data: date of birth and other biographical data like location of birth and current residence, schooling and employment records, and family members linked via the account to the holder;

(C) Nicknames or aliases listed by the holder that correspond to those elicited in discovery;

(D) Photographs of the holder which appear on the account, including those in which the account holder is not the poster but "tagged;"

(E) Verifiable check-ins to locations and events where the account holder can be placed;

(F) Activity consistent with the accounts holder's known activity.

In short, the totality of evidence approach to authenticating the account relies upon demonstrating a pattern of facts and behavior substantially consistent with known and verifiable details of the presumed account holder. How much of the information on the account points directly to the presumed account holder? The more there is, the stronger the connection.

How Much is Enough?

Courts differ on exactly how much evidence is enough to establish an adequate connection, unless faced with direct testimony from the account holder. In *U.S. v. Browne,* (834 F. 3rd 403, 3d, Cir. 2016), the court required that Facebook chats be authenticated before accepting that printouts were relevant as business records, comparing the records to a postal receipt not being adequate to substantiate the contents of the envelope. The court further held that "the great ease with which a social media account may be falsified or a legitimate account may be accessed by an imposter," raised the bar on authentication of the social media account. The totality of evidence that convinced the court was: testimony of other participants in the chats; meetings between chat participants following the chats; the defendant conceding he was the account holder and owned the device from which subject messages were sent; and biographical data such as that listed above. Placing the defendant in the chats required a device under the account holder's control, the identification of the defendant as the account holder, the corroboration of the other participants, and resulting actions of the defendant consistent with the chat content.

In the above matter, the connection was substantial, but that isn't always the case, nor, is such a high standard always applied. The Maryland approach that rises from *Griffin v. State* (419 Md.

343, 19 A.3d 415, Md. 2010) and the Texas approach, the genesis of which is *Tienda v. State* (358 S.W.3d 633, Tex. Crim. App, 2012), have become the barometers of strict versus relaxed standards for social media authentication. Under *Griffin*, the Maryland court required direct testimony of the author, a search of the alleged author's computer, or corroboration from the social media site itself. On the other end of the spectrum, the Texas court ruled that a tweet is as easily forged as "a letter or any other kind of writing," thus not requiring a higher level of authentication. Irrespective of venue, however, accumulating a totality of evidence continues to withstand challenge.

Hearsay Challenges and Authenticating Content

Once the account is authenticated, the content of the relevant posting may be challenged as hearsay. Hearsay is a statement made outside the court that is offered in court as evidence of the truth of an assertion. The classic example is a witness testifying that a 3rd party said something about a party to the action – e.g., "Sally told me that John said he sent the email." With regard to social media postings, generally the content of a message is considered a statement made out of court. The fact that posts are written statements doesn't necessarily clarify the content of the statement nor exclude potential misinterpretation.

In *Fairweather v. Friendly's Ice Cream* (2014 U.S. Dist. LEXIS 100755, 12 fn 11 D. Me. July 24, 2014), the plaintiff attempted to introduce a Facebook post made by another employee of the defendant, intending to demonstrate an excessive volume of customer complaints against the restaurant in general, as opposed to just the plaintiff. The post, in part, read that the poster was "sick and tired" of the customer complaints. The court determined the statement inadmissible as hearsay because the plaintiff was attempting to use the statement as evidence of truth of the volume of complaints, a key assertion.

Admissibility of social media content can hinge upon the ability of the presenter to make the case that the post is not the assertion, but evidence which the jury can weigh. In *People v. Valdez* (201 Cal.App.4th 1429 2011), the court overruled the defendant's hearsay objection because, "the nature of the evidence here did not consist of declarative assertions to be assessed as truthful or untruthful, but rather circumstantial evidence of Valdez's active gang involvement." The court ruled that a reasonable jury would know that they were not adjudicating the veracity of Valdez's statements on Myspace, rather, that the Myspace content was evidence of a pattern of behavior and added weight to witness testimony. The content itself was not a mirror of the assertion, and therefore, not hearsay.

The closest it may be possible to come to that vintage typewriter with a spool of ribbon is a search of mobile devices and personal computers under the control of the account holder. Such is the case in *Kinda v. Carpenter* (247 Cal.App.4th 1268 2016), where the closest that the plaintiff came to placing the defendant in Yelp postings was to prove that the routers which provided internet access to the devices on which the postings were made registered IP addresses assigned to the defendant, and devices that were connected to the internet were located at the defendant's home and place of business. The court allowed that this was enough information, despite objections by the defendant, that the jury would be able to impart the appropriate weight to the evidence. Of particular note is that this ruling was made on appeal of the trial court's ruling which barred the evidence as insufficient for authentication.

Authenticating social media may present obstacles inherent in the electronic environment in which content is created, but the rules that govern its admissibility are the same as those that cover that vintage typewriter. That's the beauty of those rules – they apply to our processes, and

not just to specific situations, allowing us to refer to the cases that came before, because whether the evidence was created on a smartphone, typewriter, or a sheet of paper: it is what it is.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

Relativity Fest
Chicago, IL: October 22-25, 2017

National eDiscovery Leadership Institute
Kansas City, MO: October 30, 2017

"The Exchange" Data Privacy and Cybersecurity Forum
Washington, DC: November 1, 2017

39th Global eDiscovery Confex
San Francisco, CA: November 1, 2017

The Sedona Conference Working Group 1 Annual Meeting 2017
Phoenix, AZ: November 2-3, 2017

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: