DISCOVERY, AUTHENTICATION AND ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

SPEAKERS:
BROOKE BARNETT-BERNAL, MICHAEL A. PATTERSON
AND EDWARD J. WALTERS JR.

SATURDAY, JULY 23, 2016 • 8 - 9 AM

BATON ROUGE BENCH BAR

CONFERENCE 2016

DISCOVERY, AUTHENTICATION AND ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

PRESENTED BY

Michael A. Patterson
S. Brooke Barnett-Bernal
Long Law Firm, LLP
4041 Essen Lane, Suite 500
Baton Rouge, Louisiana 70809

Edward J. Walters, Jr.
Walters, Papillion, Thomas, Cullens, LLC
12345 Perkins Rd
Baton Rouge, Louisiana 70810
JULY 2016

TABLE OF CONTENTS

Table of Contents 1

Biographies of Authors 2

I. Introduction 3

II. The Discovery of Social Media 3

A. *In camera* Review 5

B. Stored Communication Act 5

C. Privacy 5

D. The Answer: Proportionality 6

E. Some Thoughts on Snapchat 7

III. Authenticity and Admissibility of Social Media Evidence 8

A. Authentication 8

B. Checklist for Authentication 21

C. Hearsay 22

D. Original Writing Requirement 23

IV. Conclusion 24

MICHAEL A. PATTERSON is a graduate of the LSU Law Center and is the senior litigation partner with Long Law Firm in Baton Rouge, Louisiana. He received a Certificate and LLM in Dispute Resolution from Pepperdine University. He is the managing member of The Patterson Resolution Group which provides mediation and arbitration services throughout the State of Louisiana in complex legal matters. He serves on the adjunct faculty of the LSU Law Center and, along with Ed Walters, teaches a course in trial advocacy and evidence. He is the author of many legal articles and is the chapter author of *Louisiana Trial Procedure, Hearsay*. He is a past president of the Louisiana State Bar Association and the Baton Rouge Bar Association. He is past Chairman of the Louisiana Supreme Court Committee on Bar Admissions. He received the LSU Law Center Distinguished Achievement Award in 2013.

BROOKE BARNETT-BERNAL is a partner with the Long Law Firm, L.L.P. in Baton Rouge, Louisiana. Mrs. Bernal attended Louisiana State University, where she graduated summa cum laude with a Bachelor of Arts degree in 2003 and a Bachelor of Science degree in 2004. Mrs. Bernal double majored in Spanish and International Trade and Finance. In May 2007, she graduated from Louisiana State University's Paul M. Hebert Law Center, earning a Juris Doctorate degree and a Bachelor of Civil Law degree. During law school, she clerked for Long Law Firm and since joining the firm, her clients have included accountants, attorneys, architects, engineers, small business owners and government agencies. Mrs. Bernal is an active member of the LSBA and BRBA and currently serves on the LSBA Legislation Committee and BRBA Bench Bar Committee, among others. She is the co-author of the Ins and Outs of Rule 19 – How it Works and What You Need to Know (LSU Law Center CLE, October 2009), Construction Legislation 2010 Indemnity Clauses in Construction Contracts (BRBA Construction Law CLE Seminar, March 2011), and ESI: Electronically Stored Information – Securing, Safeguarding, Submitting and Screwups (Spoliation) (LSBA Uncorked: A CLE Adventure in California's Wine Country, March 2014). Mrs. Bernal was named as a "Rising Star" by Louisiana Super Lawyers in 2015 and 2016.

EDWARD J WALTERS, JR. a partner in the Baton Rouge law firm of Walters, Papillion, Thomas, Cullens, received his B.S. from LSU in 1969 and his J.D. from the LSU Law Center in 1975. He has practiced in the Baton Rouge area for over 38 years representing plaintiffs in personal injury cases. He is Board Certified in Civil Trial Advocacy and Civil Pretrial Advocacy by the National Board of Trial Advocates and is a Fellow of the American College of Trial Lawyers and the International Academy of Trial Lawyers. He is an Adjunct professor of law at the LSU Law Center where he and Mike Patterson jointly teach a trial skills course entitled "Advanced Trial and Evidence Seminar." He is a frequent lecturer and writer on litigation, evidence, ethics and professionalism topics and has been the editor of the Baton Rouge Bar Association's monthly magazine *Around the Bar* for over 28 years.

I. INTRODUCTION

A lack of understanding, fear and outright prejudice against social media has resulted in a hodgepodge of mostly ad hoc decisions which illustrate a failure of the bench and bar to grasp how these sites work. This lack of understanding has resulted in overly restrictive discovery limitations, overly broad discovery of this type of information, and the exclusion of evidence that clearly meets the requirements of La. Code Evid. art. 901. A better understanding will assist all members of the bench and bar.

II. THE DISCOVERY OF SOCIAL MEDIA

Social media content is playing an ever increasing role in litigation due to its near ubiquitous presence. There are over 2 billion Facebook users. Adults between 25 and 34 comprise 30% of users. The high usage of social media has not gone unnoticed by the practicing trial and bench bar. For instance, a recent survey of members of the American Academy of Matrimonial Attorneys found 66% had indicated they have found evidence on Facebook.[1]

The early cases involving discovery of social media sites has been decidedly mixed. For example, in a Pennsylvania state court case, *Mazzarella v. Mount Airy #1, LLC,*[2] a premises liability case, the plaintiff objected to a discovery request seeking the username and password on the grounds of privacy. The court, ruling on a motion to compel, simply said the information requested could lead to relevant information. The court further stated those that use social media waive an expectation of privacy.

In an employment discrimination case, a federal magistrate judge ordered the production of social media account passwords, reasoning that social media was like a file folder called

[1] John G. Browning, *Digging for Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU SCI. & TECH. L. REV 465, 467 (2011).
[2] 2012 WL 6000678 (Pa.Com.Pl. 11/7/12).

"Everything About Me," which individuals voluntarily shared with others. Therefore, the presumption is that it should be produced.[3]

In another case, *Beswick v. North West Medical Center, Inc.,* the defendant submitted an interrogatory asking for the plaintiff's social media username and password. The court found such a request was sufficiently specific. The court further stated the plaintiff's entire private Facebook account was discoverable because it was clearly relevant.[4]

Another equally unsatisfactory approach taken by courts, where a party is seeking access to a litigant's social media, requires a preliminary showing by the mover that the public portion of a litigant's social media site has relevant information (which contradicts the position taken in the suit). If such a showing is made, then complete access to the remainder of the litigant's site is granted. A good example of this approach is *Romano v. Steelcase.*[5] In that case, the plaintiff claimed her injuries largely confined her to her house and bed. There were photos on the public portion of her page contradicting that allegation. As a result, the court ordered the plaintiff to execute a consent to Facebook and MySpace granting defendants access to all of plaintiff's social media information.

However, in *Tompkins v. Detroit Metropolitan Airport,*[6] a plaintiff claimed physical injuries from a slip and fall at the Detroit airport. The defendant sought access to the private portion of the plaintiff's Facebook page, claiming the public content postings conflicted with the claims in the lawsuit. To support the request, the defendants relied on a photo of the plaintiff at a birthday party holding a very small dog. However, the court rejected the request, finding the photo was not inconsistent with the claims. The court denied any access to the private Facebook content.

---

[3] *EEOC v. Original Honeybaked Ham Co. of Georgia*, Inc., 2012 WL 5430974, at *1 (D. Colo. Nov. 7, 2012).
[4] 2011 WL 7005038 (Fla. 17th Cir. Ct. Nov. 3, 2011).
[5] 907 N.Y.S. 2d 650 (Sup. Ct. Suffolk County 2010).
[6] 278 F.R.D. 387, 388-89 (E.D. Mich. 2012).

A. *IN CAMERA* REVIEW

Another approach is to order the parties to provide the court with the user's password directly.[7] In *Barnes v. CUS Nashville, LLC,* the court ordered a non-party witness to accept the magistrate judge as a Friend on Facebook so that an *in camera* review of the Facebook contents could take place.[8]

B. STORED COMMUNICATION ACT[9]

Parties may not obtain the content of a user's social media page directly from the social media company without the user's consent. However, the act does not protect users from being ordered by a court to give consent.[10]

C. PRIVACY

Privacy settings are an integral feature of social media sites. Public means that anyone who goes to the website can see the information. Private limits the audience to selected viewers. The public or private nature of the content is meaningless when discussing discovery. A private setting does not make that material off limits to discovery. Although users expect some privacy for "private" content areas, courts have held there is no constitutional right, common law protection or statutory privilege that protects "private" social media content from discovery.[11] There are two legal principles at play in the issue of privacy. The first principle is the reasonable expectation test and the second is the third-party disclosure rule. These legal principles make it difficult to argue that information is private when it is posted to a social media account which exists for the purpose of sharing information with other people.

---

[7] *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371, at *1-2 (M.D. Pa. June 22, 2011).
[8] *Barnes v. CUS Nashville, LLC*, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).
[9] 18 U.S.C. Sec. 2701 (2012).
[10] Orin S. Kerr, *A User's Guide to the Stored Communication Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213 (2004).
[11] *Trail v. Lesko*, 2012 WL 2864004 (Pa. Ct. Com. Pl. July 5, 2012).

In *United States v. Jones,* Justice Sotomayor, in concurrence, made these observations:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to a third party. This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers, the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post,* at 962, and perhaps not. One doubts that people would accept without complaint the warrantless disclosure to the government of a list of every website they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. One would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

132 S.Ct. 945, 957 (2012) (concurring opinion).

D. THE ANSWER: PROPORTIONALITY

Social media should be handled like any other form of evidence. The producing party bears the burden of determining what is responsive and needs to be produced. The discovery request should be drafted in a way that includes all forms of social media and is sufficiently narrowly drawn. All discovery requests that seek social media evidence should be specified to closely relate to the litigation.

In re Air Crash Near Clarence Ctr., N.Y. on Feb. 12, 2009 is a good example of how a requesting party should draft the request.[12] In that case, the defendant requested the production of all electronic communications during a certain time period, "including social media accounts, emails, text messages and instant messages," that were related to the plaintiff's domicile on the date of the crash.

[12] 2011 WL 6370189, at *6 (W.D.N.Y. Dec. 20, 2011).

The most recent amendment to Fed. R. Civ. P. 26 probably will solve some of the issues in the current case law. Rule 26(b)(1) defines the scope of discovery as "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." The rule identifies six factors to be considered in determining whether the discovery is proportional to the needs of the case. They include the importance of the issues at stake, the amount in controversy, the relative access to information, the parties' resources, the importance of the discovery and whether the burden or expense outweighs its likely benefit. Privacy settings could be considered in weighing the "burden" of proposed discovery that could outweigh the marginal benefit of that information.

E. SOME THOUGHTS ON SNAPCHAT

Snapchat is an application intended to facilitate self-destructing video, photo, or chat communications.[13] When a user sends a photo he or she sets a timer that sets how many seconds the viewer can see the photo before it disappears from the screen. The maximum time is ten seconds. Normally, the viewer will only be able to view the Snapchat once before it disappears.

A party is under an affirmative obligation to preserve all relevant social media once he or she is placed on notice that another party is seeking information in the private sections of the party's social media accounts. It seems that in the Snapchat discovery arena, the biggest questions will be how to prove relevance and spoliation.

Currently, there is no consistent method to retrieve a sender's Snapchat history.[14] A litigant using Snapchat during litigation, or where litigation is foreseen, can simply push the save button

[13] Larry Magid, *What is Snapchat and Why Do Kids Love It and Parents Fear It?* (updated), FORBES.COM (May 1, 2013, 4:14 PM), http://perma.cc/8WPA-57KG.
[14] Molly McHugh, *Yes You Can Recover Dead Snapchats and Here's the Video Proof*, DIGITAL TRENDS (May 19, 2013), http://perma.cc/JLK8-PZYE.

to preserve the Snap. If she fails to do so, a court will likely find some fault with a resulting sanction.

III. AUTHENTICATION AND ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

The admissibility of social media evidence remains a prevalent issue in litigation today. To be admissible, social media evidence, like any other kind of evidence, must (1) be relevant, (2) be authentic, (3) be non-hearsay, (4) meet the original writing requirement and (5) not be unfairly prejudicial. Determining whether social media evidence is relevant or whether its probative value outweighs its prejudicial effect does not require a different analysis than for more traditional types of evidence. Pamela E. Carter & Shelley K. Napolitano, *Social Media: An Effective Evidentiary Tool*, 61 La. B. J. 332, 334 (2014). However, social media evidence does require "new considerations in the areas of authentication, hearsay and form." *Id.*

A. AUTHENTICATION.

Information obtained from the internet was once viewed by many courts as inherently unreliable and untrustworthy. For example, in *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, the United States District Court for the Southern District of Texas famously referred to the "evidence" the plaintiff sought to introduce from the Internet as "voodoo information." 76 F. Supp. 2d 773, 774-775 (S.D. Tex. 1999). In fact, the court reacted to the plaintiff's attempt to rely on such information with extreme skepticism, stating:

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo and misinformation. . . . Anyone can put anything on the Internet. No website is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation . . . .

Id. While the concerns echoed by the United States District Court for the Southern District of Texas in *St. Clair* still exist, many courts have relaxed their views about the reliability and trustworthiness of the information obtained from the internet and social media websites.

No laws have been enacted to specifically and separately address the authentication of social media evidence. Instead, most courts have adapted the traditional rules of evidence to determine whether information obtained from social media websites, such as Facebook and Twitter, is authentic. Carter & Napolitano, *Social Media*, 61 La. B. J. at 334; *See also*, *Smith v. State,* 136 So. 3d 424, 432 (Miss. 2014).

The authentication standard for both Louisiana and federal courts requires that the evidence be "sufficient to support a finding that the matter in question is what its proponent claims." La. C.E. art. 901(a); Fed. R. Evid. Art. 901(a). Authentication is a condition precedent to admissibility. *Id*. Louisiana Code of Evidence Article 901(b), like its federal counterpart, provides a non-exclusive list of methods for authenticating evidence.

Preliminary questions about whether evidence is authentic, and thus, admissible, are determined by the judge. La. C.E. art. 104(a); Fed. R. Evid. 104(a); *State v. Robertson,* 2012-0743 (La. App. 1 Cir. 12/21/12); 2012 WL 6681830, at *8. When the proponent of the evidence makes a *prima facie* showing of authenticity, the evidence goes to the jury, which will ultimately determine how much weight, if any, should be given to the evidence. Honorable Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. 433, 458 (2013). On the other hand, if the judge is presented with plausible evidence of both authenticity and inauthenticity, he is faced with a conditional relevance issue under Rule 104(b). *Id.* at 460; *See also*, *Lorraine v. Markel Am. Ins. Co.,* 241 F.R.D. 534, 539-

540 (D.Md. 2007).[15] In that case, the judge should admit the evidence and allow the jury to ultimately resolve whether the evidence admitted is that which the proponent claims. *Id; See also*, Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 460-461; *State v. Smith,* No. 2015-K-1359 (La. App. 4 Cir. 4/20/16).

When dealing with social media evidence, courts have struggled with consistently applying a uniform standard, and essentially, two approaches have emerged. One approach sets a high bar for authentication by only allowing the evidence to be admitted if the court definitively determines the evidence is authentic. The other approach sets a lower bar for the admissibility of social media evidence and focuses on whether there is sufficient evidence for a reasonable juror to conclude the evidence is authentic. Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 441, 449.

The more stringent approach for the authentication of social media evidence is best exemplified in *Griffin v. State,* 419 Md. 343, 19 A.3d 415 (Md. 2011). In *Griffin*, the State used printouts from the public MySpace profile of the defendant's girlfriend, which contained the statement "FREE BOOZY [defendant's nickname]!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!," to show she had threatened the State's key witness prior to trial by posting that warning on her MySpace page. *Id.* at 362-363. The State did not question the girlfriend about the post in question; rather, the State only offered the testimony of its lead investigator in an attempt to authenticate her MySpace profile page. *Id.* at 348-351. The investigator testified he knew it was the girlfriend's MySpace page from the photograph of her and the defendant (Boozy) on the front, through references to Boozy and their children, and from her birth date shown on the page. *Id*.

[15] Authentication under Rule 901 is viewed as a subset of relevancy, because "evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims."

The Maryland Supreme Court observed that, with "relative ease," a person "can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password." *Id.* at 352-353. Therefore, the court concluded that, considering "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user," a printout from a social media account "requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site." *Id.* at 357-358. Accordingly, the Maryland Supreme Court held the photograph of the defendant's girlfriend, coupled with her personal information and references to "freeing Boozy," were not sufficient "distinctive characteristics" on a MySpace profile page to authenticate its printout, given the possibility that someone other than the girlfriend not only could have created the MySpace account but also posted the "snitches get stiches" comment. *Id.*

The court then identified three proper methods of authenticating printouts of postings from social media sites. The first method is to ask the purported creator if he created the profile and also if he authored the posting in question, i.e., "testimony of a witness with knowledge that the offered evidence is what it is claimed to be." *Id.* at 363; *See also*, La. C.E. art. 901(b)(1); Fed. R. Evid. 901(b)(1). The second method is to search the computer of the alleged owner of the social media account, and examine the computer's internet history and hard drive to determine whether that computer was used to generate the profile page and posts in question. The third option is to obtain information directly from the social media network provider to connect the profile to the person who allegedly created it and the posts in question to the person who allegedly authored them. *Id.* at 363-364.[16]

[16] In *Sublet v. State*, the Maryland Supreme Court appears to have adopted a less stringent standard than the one announced in *Griffin.* 442 Md. 632, 113 A.3d 695 (Md. 2015). First, the court specifically noted the three methods

Similarly, in *Commonwealth v. Williams*, a witness testified the defendant's brother –using the MySpace screen name "doit4it" – contacted her through four instant messages on her MySpace page to tell her not to testify against the defendant or to claim a lack of memory regarding the events at her apartment the night of the murder (with which the defendant was charged). 926 N.E.2d 1162, 1165, 1172 (Mass. 2010). The trial court admitted the witness' testimony about the messages but did not admit the printouts of the brother's MySpace page. The Supreme Judicial Court of Massachusetts analogized the MySpace messages to a phone call, stating that "a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.'" *Id.* at 1172. In addition, the court noted the State did not offer any evidence about "how secure such a Web page is, who can access a MySpace page, whether codes are needed for such access, etc." *Id.* at 1172-1173.

The court concluded that while the State laid sufficient foundation to establish the messages were sent by someone with access to the MySpace account of the defendant's brother, "it did not identify the person who actually sent the communication." *Id.* Nor did the State produce any expert testimony to show that no one other than the defendant's brother could communicate from his MySpace page. *Id.* Therefore, the court held the trial court should not have admitted the witness' testimony regarding the MySpace messages because there was insufficient evidence presented by the State to authenticate them. *Id.* at 1173.

---

for authenticating social media postings articulated in *Griffin* were *non-exclusive*. Second, the court expressly stated it was embracing the standard for authenticating social media evidence adopted by the United States Court of Appeals for the Second Circuit in *United States v. Vayner,* 769 F.3d 125 (2nd Cir. 2014), i.e., that the authentication "requirement is satisfied if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification." *Id.* at 664, 666-667. Under this standard, preliminary determinations about authentication are made by the trial judge as to whether "the proof advanced is sufficient to support a finding that the item in question is what its proponent claims it to be…so that a reasonable juror could find in favor of authenticity." *Id.* at 666.

Likewise, in *State v. Eleck*, the defendant tried to impeach one of the State's witnesses, Simone Judway, with private messages purporting to be sent from her Facebook account. 130 Conn.App. 632, 635, 23 A.3d 818, 820 (Conn.App. Ct. 2011). The defendant, using his own testimony to authenticate printouts of the Facebook messages, stated that (1) he downloaded and printed the messages directly from his own computer, (2) the username "Simone Danielle" belonged to the witness, (3) the Facebook profile contained photographs and other entries identifying the witness as the creator of the account, and (4) when he logged into his Facebook account after the previous day's testimony, he had been removed from her list of friends. *Id.* at 635-636, 820-821. The State's witness testified that, although the messages came from her Facebook account, her account had been "hacked" and she had been unable to access it for some time. *Id.* at 635, 820. The trial court refused to admit the Facebook messages and the Appellate Court of Connecticut affirmed, explaining:

> The need for authentication arises in this context because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended. Additionally, passwords and website security are subject to compromise by hackers. Consequently, proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship.

Id. at 638-639, 822-823. Even though the appellate court noted the witness' testimony - that her Facebook account had been "hacked" - was "dubious under the particular facts at hand, given that the messages were sent before the alleged hacking of the account took place," it found her testimony highlighted the general lack of security of social media sites and raised the issue as to whether a third party could have sent the messages from her Facebook account. *Id.* at 642, 824.

These decisions appear to harbor the same skepticism regarding information obtained from the Internet and social media sites as did the U.S. District Court for the Southern District of Texas in *St. Clair*.[17] In the second line of cases, courts more appropriately evaluate whether there is sufficient evidence of authenticity for a reasonable jury to conclude the social media evidence is what the proponent claims it to be. Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 449. The judge acts as the gatekeeper and the jury is the ultimate decision maker regarding the authenticity of social media evidence. *Id.* at 456-461; *See also*, *Campbell v. State,* 382 S.W. 3d 545, 549 (Tex.App. – Austin 2012).

For instance, in *Campbell,* over the defendant's objection, the trial court admitted a printout of private messages the defendant purportedly sent from his Facebook account to his girlfriend, whom he was accused of assaulting. *Campbell,* 382 S.W.3d at 548. To authenticate the messages, the State offered the testimony of the girlfriend, who stated she (1) had received the Facebook messages from the defendant a few days after the alleged assault, (2) did not send the messages to herself, and (3) did not have access to defendant's Facebook account after the alleged assault. *Id.* at 551. The appellate court noted that "printouts of emails, internet chat room dialogues, and text messages have all been admitted into evidence when found to be sufficiently linked to the purported author so as to justify the admission to the jury for its ultimate determination." *Id.* at 549. However, the appellate court observed that:

> [W]ith respect to identity, Facebook presents an authentication concern that is twofold. First, because anyone can establish a fictitious profile under any name, the person viewing the profile has no way of knowing whether the profile is legitimate. Second, because a person may gain access to another person's account by obtaining the user's name and password, the person viewing communications on or from an account profile cannot be certain that the author is in fact the profile owner. Thus, the fact that an electronic communication on its face purports to originate from a certain person's social networking account is generally insufficient

[17] *See also*, *People v. Beckley,* 185 Cal.App. 4th 509, 110 Cal. Rptr. 3d 362 (2010).

> standing alone to authenticate that person as the author of the communication. (internal citations omitted).

Id. at 550. As a result, the court explained the most appropriate method for authenticating social media evidence, as with any other kind of evidence, "will often depend on the nature of the evidence and the circumstances of the particular case." *Id.*

In affirming the trial court's decision, the appellate court found the undisputed testimony showed (1) the defendant had a Facebook account, (2) only he and his girlfriend had access to that account, and (3) his girlfriend received messages from his Facebook account. The court further found the Facebook messages contained "distinctive characteristics," including speech that was consistent with the defendant's - a native of Jamaica - and references to the alleged assault and potential charges, "which at the time the messages were sent, few people would have known about." *Id.* at 551-552. While the court did note the evidence did not conclusively establish the defendant sent the messages, it held the State was not required to "rule out all possibilities inconsistent with authenticity or prove beyond any doubt that the evidence is what it purports to be." *Id.* at 552.

Similarly, in *Parker v. State,* the State used Facebook posts allegedly authored by the defendant after a physical altercation between her and the State's witness regarding a mutual love interest, to demonstrate the defendant's role in the incident and discredit her theory of self-defense. 85 A.3d 682, 683 (Del. 2014). The exhibit containing the defendant's Facebook posts also included her name, a photograph of her and a time and date stamp for each entry. *Id.* at 684. The State offered the testimony of the witness, who had "shared" or "reposted" the Facebook posts purportedly sent by the defendant on her own Facebook page, to authenticate them. *Id.* The trial court admitted the Facebook posts, finding the entries contained sufficient distinctive characteristics to satisfy Rule 901's authentication requirements. *Id.* In rendering its decision, the

trial court specifically rejected the more stringent approach adopted by the Maryland courts in favor of the more lenient rule adopted in Texas. The trial court noted Delaware follows the "distinguishing characteristics" rationale, which has allowed courts to authenticate handwritten letters of prisoners using solely the nicknames of the parties involved and references to the crimes, as well as emails using only the sender's email address. Therefore, the trial court determined the State had adequately authenticated the defendant's Facebook posts using witness testimony and circumstantial evidence. *Id.* at 688.

The Delaware Supreme Court affirmed the trial court's ruling and concluded social media evidence should be subject to the same authentication requirements under Rule 901 as any other evidence. *Id.* at 687. Therefore, the supreme court held that when a party seeks to introduce evidence obtained from social media networks, "he or she may use any form of verification under Rule 901 – including witness testimony, corroborative circumstances, distinctive characteristics or descriptions and explanations of the technical process or system that generated the information – to authenticate a social media post."[18] *Id.* at 687-688.

In a recent Mississippi Supreme Court case, the court cited to cases adopting the more stringent approach for authenticating social media evidence, as well as cases applying the more lenient standard, in holding the State had failed to adequately authenticate Facebook messages allegedly sent by the defendant. *Smith,* 136 So. 3d at 434-435. In *Smith,* the State presented evidence the Facebook account belonged to someone with the defendant's name, evidence the Facebook page contained a "grainy" photograph allegedly of the defendant, and testimony from a witness who said the defendant had sent the messages to her. *Id.* at 434. No other identifying information was provided and no testimony regarding the security of or access to the defendant's

[18] *See also*, *Tienda v. State,* 358 S.W.3d 633 (Tex.Crim.App. 2012); *State v. Assi,* 2012 WL 3580488 (Ariz. Ct. App. 8/21/12); *People v. Valdez,* 201 Cal.App.4th 1429, 135 Cal.Rptr.3d 628 (2011).

Facebook account was elicited (the court specifically noted the susceptibility of social media accounts to security breaches). *Id.* at 434-435.

The Mississippi Supreme Court concluded that "something more" other than a low-quality photograph and a name was needed to properly authenticate the Facebook account and messages in question. In its opinion, the Mississippi Supreme Court observed the court in *Tienda v. State* had surveyed cases involving the authentication of social media evidence and provided an illustration of what that "something more" may be to adequately present a prima face case of authentication, including:

> the purported sender admits authorship, the purported sender is seen composing the communication, business records of an internet service provider or cell phone company show that the communication originated from the purported sender's personal computer or cell phone under circumstances in which it is reasonable to believe that only the purported sender would have access to the computer or cell phone, the communication contains information that only the purported sender could be expected to know, the purported sender responds to an exchange in such a way as to indicate circumstantially that he was in fact the author of the communication, or other circumstances peculiar to the particular case. . .

Id. at 433, citing *Tienda v. State,* 358 S.W.3d 633, 639-641 (Tex.Crim.App. 2012). It is unclear which, if any, of the two approaches for authenticating social media evidence was adopted by the Mississippi Supreme Court in *Smith;* however, it appears the court applied a higher burden for the authentication of social media evidence than what is required by the more lenient approach embraced in Texas and Delaware, or any other states.

In Louisiana, all five appellate courts have allowed social media evidence to be admitted into evidence. Grant Guillot, *Evidentiary Implications of Social Media: An Examination of the Admissibility of Facebook, MySpace and Twitter Postings in Louisiana Courts,* 61 La. B.J. 338 (2014). For instance, in *Boudwin v. General Ins. Co. of America,* the plaintiffs were allegedly injured in an automobile accident but the jury did not award them any damages for past and future

mental pain and suffering, physical disability or loss of enjoyment of life and future medical expenses. 2011-2270 (La. App. 1 Cir. 9/14/11); 2011 WL 4433578. At trial, the plaintiffs were questioned about their Facebook posts and photographs from their Facebook profiles, which showed they routinely engaged in physical activities after the accident, including jogging, engaging in the P90X exercise program and playing softball. *Id.* at *3. The Louisiana First Circuit Court of Appeal upheld the jury award, noting "the record clearly shows that neither [plaintiffs] have experienced any significant limitations or impairments as a result of the injuries they sustained in the . . . accident." *Id.*

In addition, in *State v. Wood,* the Louisiana Third Circuit Court of Appeal upheld the trial court's finding there was no conspiracy between the defendant and his alleged co-conspirator based on the review of information obtained from cellphone records, computers, emails and MySpace and Facebook accounts belonging to the defendant and his alleged co-conspirators. 08-1511 (La. App. 3 Cir. 6/3/09); 11 So. 3d 701, 709-710. Furthermore, in *State v. Wiley,* the State offered the testimony of the mother of one of the co-defendants who identified the defendant and her son from several photographs posted to her son's MySpace page. 10-811 (La. App. 5 Cir. 4/26/11); 68 So.3d 583, 588. The State also called the manager of safety, security and compliance for MySpace.com as a witness to testify regarding the MySpace user numbers, user names and locations of the defendant and co-defendants, and that they were all MySpace friends with each other. *Id.* The Louisiana Fifth Circuit Court of Appeal found no error in the trial court admitting evidence related to the defendant and co-defendant's MySpace accounts. *Id.* at 591.

Even though each of the Louisiana courts of appeal have been required to determine the admissibility of social media evidence, there has been virtually no discussion by the courts as to

the requirements for the authentication of social media evidence, until very recently. *State v. Smith,* No. 2015-K-1359 (La. App. 4 Cir. 4/20/16).

In *Smith,* the Louisiana Fourth Circuit Court of Appeal was faced with the challenge of deciding the proper standard for the authentication of social media evidence under Louisiana law. *Id.* The State sought to introduce printouts containing a purported photograph of the defendant holding a gun and threatening messages allegedly made by the defendant to the victim. The State presented the testimony of only one witness – the investigating officer – who testified the victim had shown her the threatening "text messages" allegedly from the defendant on her cellphone; however, no testimony was offered to demonstrate how the messages had been copied or reproduced on paper. Furthermore, these so-called "text messages" were actually social media messages sent from an unknown social media platform, which the investigating officer could not identify. Moreover, the investigating officer testified she made no attempt to independently verify where the purported photograph of the defendant or social media messages had come from. *Id.*

In determining the appropriate standard to be applied in Louisiana, the Fourth Circuit specifically noted the authentication of social media evidence is an area of the law where "Louisiana courts have dispensed limited guidance." *Id.* As a result, the court of appeal looked to the approaches adopted by other state and federal courts for the authentication of social media evidence. Ultimately, the Fourth Circuit, relying on the Maryland Supreme Court's decision in *Sublet*, held the proper inquiry under Louisiana law "is whether the proponent has adduced

sufficient evidence to support a finding that the proffered evidence is what it is claimed to be." *Id.*;[19] *See also*, *Sublet,* 442 Md. at 678, 113 A.3d at 722.[20]

Applying this standard to the facts of *Smith,* the Louisiana Fourth Circuit Court of Appeal concluded the trial court had abused its discretion in ruling the social media evidence offered by the State was admissible. In reaching its decision, the court of appeal found the State had offered no evidence or testimony (1) to prove the defendant was the creator of the social media account, (2) as to whether the defendant, assuming he had, in fact, created the account, allowed others to access it using his password, or (3) of any "unique qualities" regarding the social media messages "from which one may assert [the defendant] sent the messages." *Id.* In fact, the Fourth Circuit found the State had "presented *no evidence at all* to authenticate the social media posts;" and instead, had simply asserted "it intend[ed] to authenticate the social media posts at trial." *Id.* Consequently, the court of appeal held the State failed to carry its burden of proof, and remanded the matter to the trial court to conduct an evidentiary hearing for the State to present evidence pursuant to La. C.E. art. 901 to authenticate the social media posts for the trial court to rule on their admissibility at trial. The Fourth Circuit expressly directed the trial court to determine, on remand, whether the State has supplied sufficient "evidence (direct or circumstantial) to support a reasonable jury conclusion that the evidence it seeks to introduce at trial is what the State purports it to be." *Id.*

[19] The Fourth Circuit noted that sufficient proof for authenticating social media evidence will vary from case to case, which proof may be direct or circumstantial; and thus, the type and quantum of evidence will depend on the context and the purpose of its introduction. The Fourth Circuit further noted that "evidence which is deemed sufficient to support a reasonable juror's finding that the proposed evidence is what it is purported to be in one case, may be insufficient in another."

[20] Whereby the Maryland Supreme Court concluded the appropriate standard in Maryland should be whether "there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be." This approach is different than the approach adopted four years earlier by the Maryland Supreme Court in *Griffin, supra.*

Because the bar for authentication of evidence is not particularly high, Louisiana courts should follow the more lenient approach for the authentication of social media evidence. This approach "affords the appropriate deference to the interplay between the evidence rules that govern the admissibility of social media evidence: Rule 104(a) and (b), Rule 901 and Rule 401." Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 456. Thankfully, the Louisiana Fourth Circuit Court of Appeal, in *Smith,* ***correctly*** decided to embrace the more lenient approach for the authentication of social media evidence, which has been adopted in Texas and Delaware, and more recently, in Maryland.

B. CHECKLIST FOR AUTHENTICATION

When it comes to authenticating social media evidence be prepared and plan ahead. There are three methods listed under La. C.E. art. 901(b) and Fed. R. Evid. 901(b) that are particularly applicable for authenticating social media evidence, including:

1. **Rule 901(b)(1) – Someone with Personal Knowledge**. If you are trying to authenticate someone's Facebook profile, call the person who created the account and ask if he or she made or authorized the postings in question.

2. **Rule 901(b)(3) – Use of an Expert or Comparison by Fact Finder**. This method would likely involve retaining a computer forensic expert to authenticate the social media account and subject postings. The downside to this method is it is costly, and further, it is difficult to predict how the jury would respond to the use of expert testimony to authenticate social media content.

3. **Rule 901 (b)(4) – Distinctive Circumstances or Characteristics.** This is may be one of the most useful ways to authenticate social media evidence. However, it requires a person who has personal knowledge of the social media content to explain how the social media evidence was created or an expert who can provide opinion testimony.

Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. at 468-472; *See also*, *Lorraine,* 241 F.R.D. at 545-548.[21]

[21] While many of the cases cited in *Lorraine* "involve digital evidence from Internet sites other than social media sites, the methods approved by those cases apply with equal force to social media evidence." Grimm, Bergstrom & O'Toole-Loureiro, *Authentication of Social Media Evidence*, 36 Am. J. Trial Advoc. at 461.

In addition, in civil cases, if social media evidence was produced by the opposing party in response to a request for production, most courts will "recognize that there is presumption of authenticity." *Id.* at 468; *See also, Lorraine,* 241 F.R.D. at 552.[22] Furthermore, in civil cases, requests for admissions are a perfectly acceptable way to authenticate social media evidence. Finally, in all cases, parties can stipulate to the authenticity of social media evidence. *Id.*

C. HEARSAY.

There are no general hearsay guidelines when it comes to information obtained from social media websites. Carter & Napolitano, *Social Media*, 61 La. B. J. at 335. In order for the social media evidence to be considered hearsay, it must be a statement, made by a declarant, offered for the truth of the matter asserted, and not be excluded from the definition of hearsay or fall into one of the hearsay exceptions.[23] To qualify as a statement, there must be an assertion. *Id.* In *Perfect, 10 Inc. v. Cybernet Ventures, Inc.,* the court held images and text, which were introduced to show they were found on the defendant's website, were not "statements" because, in effect, they were not asserting anything. 213 F.Supp.2d 1146, 1155 (C.D. Cal. 2002). Similarly, in *Firehouse Rest. Grp, Inc. v. Scurmont, LLC*, the court concluded printouts of websites that merely depicted a logo or use of the word "firehouse" in a business name did not quality as "statements." 2011 WL 3555704, at *5 (D.S.C. Aug. 11, 2011).

Social media evidence is frequently offered to prove the truth of the matter asserted, i.e., to show the declarant was at a particular place at a particular time using photographs posted on Facebook or statements made on Twitter. But that is not always the case. For instance, in *U.S. v. Siddiqui,* the United States Court of Appeals for the Eleventh Circuit determined emails between

[22] Citing *Indianapolis Minority Contractors Ass'n v. Wiley*, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998) ("The act of production is an implicit authentication of documents produced.")
[23] *Lorraine* provides a very thorough analysis of the various hearsay considerations involving ESI.

the defendant and a third-party had been admitted to show the relationship between the two that it was customary for them to communicate by email, not that the statements made in the emails were true; and thus, they were not hearsay. 235 F.3d 1318, 1323 (11th Cir. 2000).

If, on the other hand, social media evidence is being offered for the truth of the matter, it may fall into one of the hearsay exceptions or exclusions. Various hearsay exceptions and exclusions that may be applicable to social media evidence include: admissions of a party-opponent,[24] present sense impression,[25] excited utterance (will "OMG" be sufficient?),[26] then existing state of mind or condition.[27] Finally, watch out for multiple hearsay in social media evidence, such as "friends" of the declarant making statements on social media regarding statements made by the declarant or intentions of the declarant. Re-tweets on Twitter or re-posts on Facebook are simply repeating what someone else said and likely do not quality as admissions.

D. ORIGINAL WRITING REQUIREMENT

The original writing rule requires that an original or duplicate original be admitted into evidence "[t]o prove the content of a writing, recording, or photograph." La. C.E. arts. 1002 and 1003, Fed. R. Evid. Rules 1002 and 1003. A printout of a social media page can qualify as the "original" document or the "best evidence of computer-generated information." Carter & Napolitano, *Social Media*, 61 La. B. J. at 335. Indeed, both the Louisiana and federal rules of evidence provide that if "data [is] stored in or copied onto a computer or similar device . . . any printout or other output readable by sight, shown to reflect the data accurately, is an "original."'

[24] Carter & Napolitano, *Social Media*, 61 La. B. J. at 335; *See also*, *Siddiqui,* 235 F.3d at 1323*; Lorraine,* 241 F.R.D. at 567-568; *Perfect 10, Inc.,* 213 F.Supp.2d at 1155; *United States v. Safavian,* 435 F.Supp.2d 36 (D.D.C. 2006). Again, while most of these cases involve emails, the analysis should apply equally to social media evidence.
[25] La. C.E. art. 801(1); *See also, Lorraine,* 241 F.R.D. at 569-570. This exception "may be a gold mine for attorneys because many social media users have constant access to their accounts on their cell phones. Carter & Napolitano, Social Media, 61 La. B. J. at 335.
[26] La. C.E. art. 801(2); *See also, Lorraine,* 241 F.R.D. at 569-570.
[27] La. C.E. art. 801(3); *See also, Lorraine,* 241 F.R.D. at 570*; Safavian,* 435 F.Supp.2d at 44 (admitting e-mails that contained statements of defendant's state of mind under Rule 803(3)).

La. C.E. art. 1001; Fed. R. Evid. 1001. In fact, in *Laughner v. State,* the Indiana appellate court held a printout of an instant messaging conversation, which was copied and pasted into a blank document and then printed, met the original writing requirement. 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002), *abrogated (on other grounds)* by *Fajardo v. State,* 859 N.E.2d 1201 (Ind. 2007).

IV. CONCLUSION

Knowledge of how social media works is critical to the advocate. If you do not understand it, you cannot explain why it is discoverable or should be admissible to the court. You need to be prepared to "educate" the court a little more than you would expect in order to put the court at ease that the discovery is narrowly tailored to the specific issues in the case and the proffered exhibit is what it purports to be.