Presentation for WV State Bar meeting:

Dealing with social media evidence at trial.

By L. Richard Walker, Esq.[1]

Updated March 4, 2024

I. Introduction

Social media plays an enormous role in American life. The number of social media users worldwide has swelled to a record 4.9 billion people globally. What's more, this number is expected to jump to approximately 5.85 billion users by 2027. These aren't users tied to a single platform, either. The average user now spreads their digital footprint across a staggering six to seven platforms every month. Every minute users post 216,000 photos on Instagram, tweet 277,000 times, and share almost 2.5 billion pieces of content on Facebook.

Facebook is the most visited social media. Facebook commands 53% of all social media site visits in the United States. It's a supremacy that remains unchallenged to date. Other platforms, despite their individual strengths and popularity, continue to find themselves in Facebook's shadow across desktop, mobile and tablet devices. The other prominent social medial platforms include Instagram, X, YouTube, Pinterest, LinkedIn, and, last but not least, Tik Tok.

Social media's importance is observed in criminal and civil cases. Digital information yields millions of potentially valuable pieces of evidence. Courts recognize the importance of social media, with jurisdictions both setting parameters and limiting discoverable content. A judge from a New York state court noted, "[i]n recent years, social media has become one of the most prominent methods of exercising free speech, particularly in countries that do not have very many freedoms at all." *People v. Harris*, 949 N.Y.S. 2d 590, 597 (N.Y. Crim. Ct. 2012). Trial counsel in civil and criminal cases can and should use social media to gather evidence, establish connections between parties, create chronologies, locate witnesses, learn about admissions, and identify aggravating factors. This requires in-depth study and adds additional layers of diligence and preparation to what is already a demanding area of practice.

---

[1] L. Richard Walker is the First Assistant Federal Public Defender for the Northern District of West Virginia. He is a supervisor and active trial lawyer. The preparation of these materials would not have been possible without the dedication and invaluable assistance of Stanley McLaughlin, the Computer Systems Administrator and tech expert at the Federal Defender Office, and Jessica Ray, a law student at the WVU College of Law and outstanding research assistant.

II. What is social media?

In the 1970s, when most of us were dictating letters to staff and using electric typewriters, Randy Suess and Ward Christensen introduced the Computerized Hobbyists Bulletin Board System, which was initially designed to help the inventor network with fellow members of a computer club in Chicago and generate content for their club's newsletter. This network eventually grew to support 300-600 users.

Later, in 1997, the first social networking sites launched: Bolt and Six Degrees. Dan Pelson designed Bolt as a platform for 15 to 20-year-olds to use for email, voice mail, voice chat, message boards, and instant messaging. Six Degrees founder Andrew Weinreich is sometimes referred to as the father of social networking. Six Degrees was a platform to help people connect with people they didn't know yet.

A lot has changed since 1997. Today, social media is ubiquitous. It is defined as: "A form of mass media communications on the Internet (such as on websites for social networking and microblogging) through which users share information, ideas, personal messages, and other content (such as videos). Social networking and social media are overlapping concepts, but social networking is usually understood as users building communities among themselves while social media is more about using social networking sites and related platforms to build an audience."

III. How do we gather social media evidence?

A. *Subpoenas.*

There are numerous methods available to gather social media evidence in criminal and civil cases. Subpoenas are uncomplicated and commonly used. For example, in *United States v. Hambrick*, 2000 WL 1062039 (4th Cir. 2000), on March 14, 1998, J.L. McLaughlin, a police officer with the Keene, New Hampshire Police Department, connected to the internet and entered a chat room called "Gay dads 4 sex." McLaughlin's screen name was "Rory14." In this chat room, Detective McLaughlin encountered someone using the screen name "Blowuinva." Based on a series of online conversations between "Rory14" (Det. McLaughlin) and "Blowuinva," McLaughlin concluded that "Blowuinva" sought to entice a fourteen-year-old boy to leave New Hampshire and live with "Blowuinva." Because of the anonymity of the internet, Detective McLaughlin did not know the true identity of the person with whom he was communicating nor did he know where "Blowuinva" lived. "Blowuinva" had only identified himself as "Brad."

To determine "Blowuinva's" identity and location, McLaughlin obtained a New Hampshire state subpoena that he served on "Blowuinva's" internet service provider, MindSpring, located in Atlanta, Georgia. The New Hampshire state

subpoena requested that MindSpring produce "any records pertaining to the billing and/or user records documenting the subject using your services on March 14th, 1998 at 1210HRS (EST) using Internet Protocol Number 207.69.169.92." MindSpring complied with the subpoena.

The question before the court was whether the court must suppress the information obtained from MindSpring, and all that flowed from it, because the government failed to obtain a proper subpoena. When the defendant surfed the internet using the screen name "Blowuinva," he was not a completely anonymous actor. It is true that an average member of the public could not easily determine the true identity of "Blowuinva." Nevertheless, when the defendant entered into an agreement to obtain internet access from MindSpring, he knowingly revealed his name, address, credit card number and telephone number to MindSpring and its employees. The court found that the MindSpring materials were not protected and, therefore, the predicate for the motion to suppress the materials seized from the defendant's home failed.

B. *Discovery requests.*

In *Richards v. Hertz*, 100 A.D.3d 728, 953 N.Y.S.2d 654 (App. Div. 2012), the plaintiff alleged personal injuries that limited enjoyment of life and physical activity. However, the defense saw pictures on Facebook showing the plaintiff skiing and requested the court to allow access to the site. The court denied the request for discovery and, instead, ordered the plaintiff to turn over pictures to the defense. The defense argued that the pictures proved there may be more information on Facebook relevant to the case. The court indicated that along with the possibility of more evidence, there would also be private material that was not relevant to the case. In an abundance of caution, the court decided to videotape the site and then decide what more to turn over to the defense and what to exclude.

In *CineTel Films, Inc. v. Doe*, 853 F.Supp. 2d 545, 555-56 (D. Md. 2012), on August 30, 2011, plaintiffs, CineTel Films, Inc. ("CineTel"), and Family of the Year Productions, LLC ("Family") filed a complaint against 1,052 John Doe defendants alleging they used a file-sharing protocol called BitTorrent to illegally obtain their copyrighted, pornographic motion picture I Spit on Your Grave. Attached to the complaint was a chart listing the Internet Protocol addresses ("IP addresses") of the 1,052 Doe defendants — the only identifying information provided to the court — together with the date and time each defendant allegedly accessed the torrent network for the purpose of downloading unlawful copies of the plaintiffs' copyrighted motion picture.

The court ruled that an internet subscribers' First Amendment right to speak anonymously is not enough to bar discovery of their subscriber identity information.

By sharing the identity information with the internet service provider, the subscriber loses his/her reasonable expectation of privacy.

In the case, *Vasquez-Santos v. Mathew*, 168 A.D.3d 587 (N.Y. App. Div. 2019), a central point at issue was whether private social media information was discoverable. The plaintiff in the case was at one point, a semi-professional basketball player. He claimed he became disabled as a result of a car accident and could no longer play basketball.

Through an extensive social media investigation, the defendant found contradicting evidence. The defendant submitted social media pictures of the plaintiff playing basketball after the accident. In these pictures, the plaintiff was "tagged" by friends.

The plaintiff claimed these were old photos and were thus inadmissible. In response, the defendant requested an order to have a third-party data mining company be given access to the subject's private content to investigate these claims.

The trial court denied this request. However, the appellate court reversed that decision and allowed access to the plaintiff's private content due to its probative value and the defense's right to any content which would show the defendant performing physical activities.

This ruling further shows that private social media evidence can be discoverable, so long as it "contradicts or conflicts with a plaintiff's alleged restrictions, disabilities, and losses, and other claims." *Id.* In this case, the court granted the defendant the access to this private Facebook information, limited in time and subject matter, to defend against the plaintiff's claims of injury.

It is also of particular interest to note that in this case the plaintiff did not post the original photos in question himself. Rather, they were taken by a friend and he was only tagged in them. The court found it was "of no import" that the plaintiff did not personally take or post the photos, because "he was 'tagged' thus allowing him access to" the content. *Id.* at 588.

C. *Search warrants.*

Search warrants are another commonly used method of collecting social media evidence. It should come as no surprise that often they are challenged by defendants seeking to exclude their social media from criminal trials. For instance, in *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017), the 11th Circuit Court of Appeals examined the constitutionality of a search warrant for a defendant's entire Facebook account. The warrant at issue required Facebook to hand over the full contents of the defendant's account and then to let law enforcement agents mine the account for evidence of the defendant's alleged prostitution ring. The court

indicated that such a broad warrant–one lacking a time frame or description of the particular data sought–may be insufficiently particular to satisfy the Fourth Amendment.

However, the court ultimately did not have to decide the particularity question, as it determined that law enforcement executed the warrant in good faith, and, therefore, the good faith exception to suppressing evidence applied. Nonetheless, the court stated that, in the future, law enforcement should specifically identify the data they seek, rather than requesting the contents of an entire social media account.

Blake demonstrates the complexities of applying the Fourth Amendment to the modern social media landscape, as well as the importance of having an experienced criminal defense attorney to make creative Fourth Amendment arguments.

IV. What methodology should we use to gather social media evidence?

The methodology used to gather social media evidence and the preservation of this evidence are very important considerations. Proper tools and methods for collecting digital evidence, such as social media information, involve a systematic approach to ensure the integrity and admissibility of the evidence in court. Normally, an expert or experienced investigator will be required to assist in this process. Here are the critical steps:

Create a forensic image: Make a complete copy of the digital device to preserve its state without altering the original data.

Process or index the data: Organize the collected data into manageable folders like photos, emails, texts, etc., which may require significant time.

Analyze the data: Use specialized tools and techniques to examine and interpret the collected evidence thoroughly.

Maintain a well-documented chain of custody: Document every movement and location of the evidence to ensure authenticity.

Understand how to preserve evidence from different devices: Different devices may require specific preservation methods to prevent data loss or alteration.

Select an extraction method: Choose appropriate extraction methods based on time constraints and the type of data being retrieved.

By following these steps and using recognized forensic tools, professionals can collect digital evidence effectively, ensuring its reliability and usability in legal proceedings.

V. What tools should we use to gather social media evidence?

The use of proper tools is equally important. Some common tools used for digital evidence collection include:

X1 Social Discovery: A suite of automated tools used to create forensically sound copies of social media sites such as Facebook, Instagram, X (f.k.a. Twitter), and YouTube.

WebPreserver: A web browser plug-in used for obtaining state-in-time copies of social media pages, videos, pictures, etc.

Pagefreezer: Allows for creating an archive of social media pages as well as keyword monitoring.

TweetBeaver: Uses X (f.k.a. Twitter) analytics to understand account and identity connections.

These tools play a crucial role in retrieving, preserving, and analyzing digital evidence in a forensically compliant manner, aiding investigators in legal proceedings.

VI. How do we avoid problem with use of social media for our clients?

Lawyers are required to keep abreast of changes in the law and its practice to include keeping up with "the benefits and risks associated with relevant technology." ABA Rule 1.1, comment 8. Therefore, we are required to develop an understanding of social media and provide competent advice to clients. And we need to develop a set of instructions. There are simple ways to help clients avoid exposing themselves and creating evidence which is incriminating or otherwise harmful:

Avoid using social media. It is critical to advise all clients not to communicate about a case online. This stops problems from occurring in the first place.

Lock down all devices for maximum privacy. At least this will limit access to friends and family, but we should not assume anyone is completely trustworthy.

Do NOT delete and do NOT destroy. This is extremely important for clients and lawyers to understand. This avoids claims of spoilation and even worse, obstruction of justice charges.

To illustrate this point, in *Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (2013), Isaiah Lester and his wife, Jessica, were involved in a tragic car accident when an Allied Concrete Co. truck lost control and flipped onto their vehicle. Jessica later passed away from her injuries. The driver of the truck pled guilty to

manslaughter. A year later, Lester filed a civil suit against Allied Concrete Co. seeking compensation for monetary and non-monetary losses following the death of his wife. An attorney for Allied Concrete issued a discovery request for Lester's Facebook page, including photos, statuses, and messages. After notifying him of the discovery request, Lester's attorney instructed him to "clean up" his Facebook page and delete certain photos that could "blow up" at trial. Lester proceeded to delete 16 photos from his profile, and later on deactivated his account entirely and claimed to have no Facebook profile in court.

Then, Allied Concrete received notice of this action and filed a motion to compel discovery. Even after Lester reactivated his Facebook profile, the 16 photos in question remained deleted (though most were ultimately produced in the course of litigation). The court granted the defendant sanctions against both Lester and his attorney for spoliation of evidence.

Making matters worse, the jury received an adverse-inference instruction, allowing them to conclude that the Facebook content that the plaintiff deleted would have been damaging to his case. The court also found that Lester and his attorney had violated Rule 3.4(a) of the Virginia Rules of Professional Conduct in attempting to destroy or conceal evidence that had been subject to a discovery request by the defendant. In addition to the adverse-interference instruction, Lester and his attorney were instructed to pay the defendant $722,000 in expenses and attorney fees. Lester's attorney was also subsequently suspended from practicing law for 5 years for instructing Lester to obstruct Allied Concrete's access to evidence.

VII. How to deal with social media evidence at trial?

A. Motion to Suppress

For a party confronted with negative social media evidence, a motion to suppress is the first line of defense. This response is unique to criminal cases. The objective is to attack the seizure and search forming the basis for the social media evidence and to request suppression and exclusion from the court as a defendant would with any other type of physical evidence. There are many grounds to support a motion to suppress. All motions to suppress are entirely fact specific.

For example, in *United States v. Meregildo*, 883 F.Supp. 2d (S.D.N.Y. 2012), the Defendant moved to suppress evidence gathered from his Facebook account pursuant to a search warrant. The government used a cooperating witness, who was one of Defendant's Facebook friends to access his account. The Court held that "[w]hen a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private

and may be constitutionally protected. *Id*. at 525. The court also stated, "[w]here Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment." *Id*. at 526. Here, Defendant posted information about his gang involvement, which was accessible to his Facebook friends, including the government's cooperating witness. Therefore, he could not suppress information provided to the government from his Facebook friend/cooperating witness.

In *United States v. Gatson*, 214 WL 7182275 (D. N.J. 2014), the Defendant was indicted for conspiracy to transport and receive stolen property. Pursuant to a search warrant, federal agents seized a laptop and tablet, which linked to his Instagram account. Law enforcement officers also used an undercover account to become Instagram friends with defendant, who accepted the friending invitation. As a result, law enforcement officers were able to view photos and other information the defendant posted to his Instagram account. Defendant argued there was no probable cause to search and seize information in his Instagram account. Defendant's Instagram account displayed photographs of himself with large amounts of cash and jewelry, which were possibly the proceeds from the underlying offense. The court held that no search warrant is required for the consensual sharing of this type of information and denied his motion to suppress.

In *U.S. v. Correy Cawthorn*, 2023 WL 5163359, No. 19-CR-36, (D. MD 2023), the court suppressed Instagram evidence, secured by a search warrant, where government delayed the review of the evidence for over two years. As to Instagram evidence that was reviewed promptly, will rule on whether government failed to segregate relevant data from irrelevant data – which would also require suppression. Although Rule 41 does not prescribe the method by which such later review must occur, in the warrant execution context, as elsewhere, Fourth Amendment reasonableness kicks in. Thus, courts agree that such review must occur within a reasonable amount of time … [and] that the government may not seize and retain items outside the scope of a warrant. It is imperative that searches of electronic information strictly comply with the parameters outlined in the warrant to avoid effectively converting a search warrant supported by probable cause into the sort of general warrant forbidden by the Fourth Amendment.

B. Motion to quash subpoena.

Similarly, in *People v. Harris,* 949 N.Y.S.2d 590 (Crim. Ct. 2012), the Defendant was charged with disorderly conduct after marching on roadway of the Brooklyn Bridge and the prosecutor sent Twitter a subpoena seeking information from his account related to the ongoing prosecution. Defendant moved to quash the subpoena, as did Twitter (stating it would not comply with the subpoena until the Court ruled on Defendant's motion to quash).

The court held that the defendant had no proprietary interest in the user information on his Twitter account, and he lacked standing to quash the subpoena. Twitter then moved to quash and did not comply with its own subpoena. The Court held that Twitter must provide information relevant to the dates of the investigation, but information outside the investigation's scope could be obtained only through a search warrant. The Court noted in its decision "[i]f you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private email, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the Internet that now exist. Those private dialogues would require a warrant based on probable cause in order to access the relevant information." *Id.* at 595.

C. Motion in Limine.

If the social media evidence does not comport with the rules of evidence, a motion *in limine* is a preferred method to deal with it. This method permits counsel to address the authenticity and admissibility of social media evidence sufficiently in advance of trial. It is easier and often more effective for counsel to make written objections in the form of a motion *in limine*. This provides the court more of an opportunity to arrive at the correct ruling. The grounds are the same as the grounds for trial objections (listed below), but the pleadings are developed, detailed, supported by specific authority, and may be submitted weeks in advance of trial.

D. Trial Objections.

1. Lack of authentication.

The state of the law regarding social media evidence admissibility is somewhat murky. Courts and academic writings have split the case law into different approaches. In general, admission hinges on how the moving party can show circumstantial evidence to prove the exhibits taken from social media are what they are purported to be. The majority of jurisdictions follow a less restrictive approach, where the judge is the gatekeeper for the evidence and the jury makes the final decision as to the reliability and weight of that evidence.

For instance, in *Brown v. State*, 300 Ga. 466, 796 S.E. 2d 283 (2017), the Defendant appealed his conviction for murder and other charges, arguing that the introduction of the improperly-authenticated evidence at trial required a reversal of all his convictions. During the trial, three witnesses testified that he held a shotgun, and two of the three testified they saw him firing it at the homicide victim. During the trial, a city investigator and expert witness in criminal street crimes and gang activity testified she believed defendant belonged to the Young Choppa

Fam gang. The State then presented her with the eight exhibits—taken from YouTube, Facebook, and Twitter—showing Defendant's activity in the Young Choppa Fam gang. The witness testified she obtained the images through a public internet search. The Supreme Court of Georgia determined that these exhibits had not been properly authenticated, and, for that reason, it granted the motion for new trial only with respect to the count of criminal gang activity.

In *State v. Palmer*, the West Virginia Supreme Court of Appeals upheld the admission of an email containing a reference to a Facebook post and the post's comments which reflected a character trait of the petitioner. *State v. Palmer,* No. 14-0862, 2016 W. Va. LEXIS 445, at *12 (June 3, 2016). The petitioner appealed his conviction of first degree murder of his father-in-law and raised the issue of authentication of the email with the Facebook post. *Id.* at *2. The Facebook post stated the petitioner had a mental list of people he was going to "strike" because they id him and his wife wrong. *Id.* at *12 n.9. A concerned citizen provided petitioner's Facebook post containing these threats to the State to prove the threatening character of the petitioner by specific instances of conduct under W. Va. R. Evid. 405(b). *Id.* at *12. The trial court authenticated the Facebook post through the testimony of the concerned citizen who had a conversation with the petitioner on Facebook. *Id.* at *12 n.11. The testimony was enough to authenticate the Facebook post and trace it back to the petitioner because the content of the testimony included a belief that the manner of speech used in the post, the Facebook profile picture, and content of the conversation was such that only the petitioner would have knowledge of it. *Id.* at *12. Although the trial court additionally conducted an in camera review of the exhibit before admission, no such review is required and the testimony alone was enough to authenticate the Facebook post.

In *State v. Benny W.,* 242 W. Va. 618, 625, 837 S.E.2d 679, 686 (2019), the West Virginia Supreme Court of Appeals held "social media text messages may be authenticated in numerous ways including, for example, by a witness who was a party to sending or receiving the text messages, or through circumstantial evidence showing distinctive characteristics that link the sender to the text messages." *Benny W.,* at 634, 837 S.E.2d at 685. The "petitioner was convicted by a jury of six counts of sexual assault in the second degree, seven counts of sexual abuse by a custodian, and one count of sexual abuse in the first degree." *Id.* at 621, 837 S.E.2d at 682. One issue raised on appeal was whether Facebook Messenger text messages were properly authenticated. *Id.* at 621, 837 S.E.2d at 683. The petitioner's daughter, who was one of the victims, authenticated the Facebook messages when she testified that the content of the messages were conversations between her and her father, the petitioner. *Id.* at 626, 837 S.E.2d at 687. All that was required for authentication of social media messages was a party to the messages affirming the

content was between the party and the petitioner. The same standard of authentication applies to other forms of electronic communication such as text messages. *Hasan v. W. Va. Bd. of Med.*, 242 W. Va. 283, 295, 835 S.E.2d 147, 159 (2019). Additionally, though not required to prove authenticity, the court in *Hasan* found additional evidence showing distinctive characteristics that linked the female and the petitioner to the text messages. *Id.* (holding text messages through text message applications to disguise phones numbers were authenticated when a party to the messages testified the contents of the messages were between herself and the petitioner).

2. Relevance.

Issues relating to weighing admissibility of social media evidence are determined by the rules of every jurisdiction. Normally, the rules of evidence are patterned after the Federal Rules of Evidence ("FRE"). Like any evidentiary question, the first question is whether the potential evidence is relevant. FRE 401 defines relevant evidence to "mean[] evidence, including evidence relevant to the credibility of a witness or hearsay declarant, having any tendency in reason to prove or disprove any disputed fact that is of consequence to the determination of the action." Evidence is relevant if it has some tendency, even a slight tendency, to prove or disprove an issue in the case. *See People v. Carpenter*, Cal.4th 1016,1048 (1999); *Dortch v. Fowler*, 588 F. 3d 396, 401 (6th Cir.2009) ("[A] piece of evidence does not need to carry a party's evidentiary burden in order to be relevant; it simply needs to advance the ball."). Asking whether social media evidence is relevant is like generically asking whether testimony is relevant. There is nothing inherent in social media evidence that provides any special rules in favor or against a finding of relevancy.

3. Hearsay

Likewise, social media evidence can be hearsay in ways identical to others forms of evidence. Exceptions to the rule against hearsay allow messages to be admissible evidence for many different reasons and social media evidence is always admissible when admitted not for the truth of the matter asserted. *See United States v. Boswell*, 530 F. App'x 214, 216 (4th Cir. 2013) (holding text messages are admissible because "evidence is not hearsay when it is used only to prove that a prior statement was made and not to prove the truth of the statement"); *Commonwealth v. Koch*, 2011 PA Super 201, 39 A.3d 996, 1002-05 (Pa. Super. Ct. 2011) (explaining text messages could be admitted under the exception to the hearsay rule for admission of a party opponent).

This holds true universally and applies equally to statements made over the telephone, through text messages, by emails, or using social media such as Twitter. *Atkins v. Commonwealth*, 68 Va. App. 1, 8, 800 S.E.2d 827, 831 (2017). Social

media messages authored by the defendant are not hearsay when they are admitted as they are statements made by a party opponent. *United States v. Hernandez*, No. 1:17-cr-00183-TWP-TAB, 2020 U.S. Dist. LEXIS 17627, at *8 (S.D. Ind. Feb. 4, 2020). Where there is sufficient evidence to identify the defendant as a participant in a social media chat acting under a social media username, the social media chat is admissible against hearsay objections because any statement of the defendant in the chat transcript is admissible nonhearsay and the statements of the other participants are admissible as context for the defendant's messages. *United States v. Needham*, 852 F.3d 830, 837 (8th Cir. 2017). Further, it is important to remember that photos within social media posts are admissible and not hearsay. *Atkins*, at 10 n.9, 800 S.E.2d at 832 (citing *Bynum v. Commonwealth*, 57 Va. App. 487, 493, 704 S.E.2d 131, 134 (2011)).

4. Unfairly prejudicial (FRE 403)

Even if social media evidence is relevant, the evidence may be excluded under Rule 403 of the Federal Rules of Evidence. This is the last line of defense. Based on the premise that admissibility has limits, Rule 403 of the Federal Rules of Evidence provides that relevant evidence "may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of issues, or misleading the jury." Fed. R. Evid. 403.

However, the "balance under Rule 403 should be struck in favor of admissibility, and evidence should be excluded only sparingly." *United States v. Lentz*, 524 F.3d 501, 525 (4th Cir. 2008). "[T]he mere fact that the evidence will damage the [opposing party's] case is not enough—the evidence must be unfairly prejudicial, and the unfair prejudice must substantially outweigh the probative value of the evidence." *United States v. Williams*, 445 F.3d 724, 730 (4th Cir. 2006) (internal quotation marks and alteration omitted). "Evidence is unfairly prejudicial and thus should be excluded under Rule 403 'when there is a genuine risk that the emotions of a jury will be excited to irrational behavior, and that this risk is disproportionate to the probative value of the offered evidence.'" *Id.*

VIII. Conclusion

Social media provides civil and criminal trial attorneys critical information and evidence to develop themes, theories, and defenses. Social media evidence is unavoidable and, therefore, we should become experts handling and dealing with it at trial. However, counsel must be aware the origin, means of collection, governing rules of evidence, and ethical considerations in their respective jurisdictions. Counsel should become diligent students of this subject and develop methods for dealing with social media prior to and during trial, while adhering to the ethical boundaries and guidelines. In this vast and ever-evolving field, trial lawyers should

keep abreast of relevant case law and ethics opinions to aid them in the pursuit of justice.