TECHNOLOGY AND SOCIAL MEDIA FOR PROSECUTORS:

How to Build a Case Ethically and Competently

SMART PROSECUTION

ASSOCIATION OF PROSECUTING ATTORNEYS

The Language of Social Media
To understand social media, common terms, definitions, and contexts must be understood.

Facebook: Pew reports that Facebook remains the most popular social media platform, which 79% of all online Americans use.[2] Facebook also boasts 1.9 billion users worldwide.[3] Users create a profile that can be tailored to be as public or as private as the user desirers. Once a profile is created, the user can share photos, messages, and information amongst their "friends" and upload and send videos. Facebook includes: messenger –available online and through the users smartphone— which enables users to communicate in real time, much like a SMS text message.

Instagram: The second largest social media platform, its usage is slowly but steadily increasing due to its popularity with younger Americans. According to Pew, 32% of Americans use this platform. Unlike Facebook, Instagram users communicate mostly through photos, primarily taken from their smartphones and uploaded directly to the site. Users hashtag (#) their posts, which link other photos and users with the same hashtag. Instagram users may connect their Instagram account to other social media profiles, enabling them to share photos to those profiles as well. Users follow other users (including celebrities and other well-known figures) to subscribe to their feeds.

Twitter: The third largest social media platform, Twitter users comprise approximately 24% of all online adults. Younger populations also favor this platform: thirty-six percent of online Americans between the ages of 18-29 use Twitter. Twitter mandates users to keep their "tweets" to 140 characters or less. Registered users create a Twitter "handle," with the @ sign following their registered name.

LinkedIn: With a reported 106 million active users in September 2016,[4] LinkedIn's niche is professional networking. Users can share articles, photos, or updates, and can post publications.

YouTube: Also considered a social media platform used to share videos, and has over 1 billion users.[5] Both private individuals and media corporations are able to upload, view, share, rate, and comment on posted content. Unregistered users may only view content.

Pinterest: With 150 million registered users,[6] this site encourages its registers to visually catalog ideas known as "pinboards" in a self-serving fashion.[7] Registered users pin, upload, save, sort, and manage their pinboards as well as browse the content of other users' pinboards in their feed.

Other notable social media platforms include: **Reddit**, **Vine Camera**, **Tumblr**, **Flickr**, and **Google+**.[8]

Prevalence of Social Media in Society and, Increasingly in the Courtroom

Social media plays a large role in American life. Every minute users post 216,000 photos on Instagram, tweet 277,000 times, and share almost 2.5 billion pieces of content on Facebook.[1] Social media's importance also coincides with criminal prosecutions and investigations. Digital information yields millions of potentially 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 in his decision, "In 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."[9] Prosecutors and law enforcement use social media to gather evidence, establish connections between parties, locate witnesses, and identify aggravating factors—such as lack of remorse —at sentencing. Recent court decisions set forth rules when introducing social media into evidence and state bar associations provide guidance about how prosecutors can ethically collect social media to investigate, build, and try cases.

Authenticating Social Media Evidence in the Courtroom- Maryland's and Texas' Diverging Approaches

"The state of the law regarding social media evidence admissibility is murky at best. Courts and academic writings have split the case law into two approaches. These can best be referred to as 'The Maryland Approach'[10] and 'The Texas Approach.'"[11] The distinction between the Maryland Approach and the Texas Approach has been widening.[12] However, admission generally hinges on how the prosecutor can show circumstantial evidence to prove the exhibits taken from social media are what they are purported to be. Fortunately for prosecutors, more jurisdictions follow the less restrictive Texas Approach, where the "judge is the gatekeeper for the evidence and the jury makes the final decision as to the reliability of that evidence."[13]

The Maryland Approach

Under the more restrictive Maryland Approach, courts are skeptical of authenticating social media evidence, finding the odds too great that someone other than the alleged author of the evidence was the actual creator of the account, posting, or tweet.[14] Through two cases, *Griffin v. State*[15] (2012) and *State v. Sublet*[16] (2015), the following conditions must exist for social media evidence to be properly authenticated and offered into evidence: authentication through testimony from the creator of the social media post;[17] through hard drive evidence or internet history from the purported creator's computer;[18] or through information obtained directly from the social media site itself "that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it."[19] The last condition has been established through contemporaneous social media conversational exchanges created in response to events occurring that same day.

In 2011, the Maryland Court of Appeals, the highest court in the state, heard *Griffin v. State*.[20] Griffin was convicted of second degree murder. Prior to the trial, a State's witness testified that defendant's girlfriend threatened the witness; the prosecutor then sought to offer evidence through a state's investigator that the girlfriend posted "...Snitches Get Stitches" on her MySpace account. The Court held that the lower court improperly admitted the MySpace page without the girlfriend's testimony that she created the account. The Maryland Court of Appeals disagreed with the lower court's reasoning that the MySpace profile in question showed the "distinctive characteristics" of the girlfriend, and "that the offered evidence is what it claims to be." The lower court found that it was proper to admit the MySpace page due to "distinctive characteristics" based on the following factors:

the user's account listed the same age, birthday, and city as the girlfriend; a witness testified the user's profile picture was that of the girlfriend; the user mentioned her two children (the same number as the defendant's girlfriend); and finally, the user referenced "Boozy" which was the defendant's nickname. However, in its decision to reverse and remand, the Maryland Court of Appeals cited in part that despite these distinctive characteristics, "the [lower] court failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the 'Snitches Get Stitches' posting."[21] Thus, in Maryland, under Griffin, the proponent must therefore affirmatively disprove the existence of a different creator for the evidence to be admissible.

Four years after *Griffin* in 2015, the Court of Appeals of Maryland, through *Sublet v. State*[22], offered some guidance on what constitutes "distinctive characteristics," permissible to show circumstance evidence in a social media case. *Sublet* established Maryland's standard that a "context-specific determination" whether the proof advanced is sufficient to support finding that the item in question is what its proponent claims it to be.[23] The Court further opined on the importance of the judiciary's role as a gatekeeper in admissibility of social media cases: "The role of judge as "gatekeeper" is essential to authentication, because of jurors' tendency, 'when a corporal object is produced as proving something, to assume, on sight of the object, all else that is implied in the case about it.'" (emphasis, Court's own).[24] The Court also recognized "In the period since *Griffin* had been decided, cases in which authentication of social networking websites and postings at issue have proliferated."[25]

In *Sublet,* the Court of Appeals agreed with the lower court that it was proper to exclude testimony of a witness, who testified that other people had access to her account password so they could presumably access and change or insert information on the witness' page, thereby attributing the posted content to her. The Court reasoned, "when a witness denies having personal knowledge of the creation of the item to be authenticated, that denial necessarily undercuts the notion of authenticity." [26] However, after this analysis, the court then turned its lens in *Sublet* to another case, *Harris v. State,* to show when authentication (and therefore admissibility) can be proper when the creator of the social media page does not testify about the ownership of the page. The key is exigency and the ability to show proof of authorship. In *Harris*, petitioner defendant "TheyLovingTc" sent "direct messages" from his Twitter account on his phone about '[aveng]ing keon" to another Twitter user, OMGitsLOCO. The Court of Appeals agreed with the State that that there were "sufficient distinctive characteristics" for the trial judge to determine that a reasonable juror could find the "direct messages" and tweets authentic; to wit, [a witness] had identified "TheyLovingTc" as Defendant's Twitter name and that the photographs accompanying the TheyLovingTc messages were of the defendant. The State also argued that the content of the messages indicated that *Harris* was the author, including that they demonstrated that OMGitsLOCO and TheyLovingTc knew about the plan for a shooting."[27] The Court also noted "The substance of the conversation referenced a plan to "avenge keon" that had only just been created in response to events occurring that same day… That the plan subsequently came to fruition the following day also indicates that the "direct messages" were written by someone with knowledge of and involvement in the situation, which involved only a small pool of individuals."[28] Thus, the Court was satisfied that the Twitter handle, "TheyLovingTc" actually belonged to the defendant, and was therefore authentic and the evidence gathered from the page admissible.

The Texas Approach

Compared to Maryland, courts following the "Texas Approach" are more 'lenient' in determining what amount of evidence a "reasonable juror" would need to be persuaded that the alleged creator did create the evidence.[29] "This second approach is viewed as 'better reasoned' because it allows for proper interplay among the many rules that govern admissibility, including [FRE] 901."[30] The standard is best explained in the 2012 case, *Tienda v. State*,[31] where the defendant unsuccessfully

[1] *Infographic: Data Never Sleeps 2.0 DOMO. Accessed May 5, 2017 from: https://www.quora.com/How-many-images-are-uploaded-to Pinterest-every-day*
[2] *Social Media Update 2016. November 11, 2016. Accessed May 5, 2017 from: http://www.pewinternet.org/2016/11/11/social-media-update-2016/*
[3] *Smith, Craig. "How Many People Use the Top Social Media Apps and Services. February 2017. Accessed May 5, 2017 from: http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/*
[4] *United States Securities and Exchange Commission Form 10-Q. (Quarterly Report), page 33. Accessed May 5, 2017 from: https://s21.q4cdn.com/738564050/files/doc_financials/quarterly/2016/2016.09.30-10-Q-Project.pdf*
[5] *Kallas, Priit. "Top 15 Most Popular Social Networking Sites (and 10 Apps). DreamGrow. February 27, 2017. Accessed May 5, 2017 from: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/*
[6] *Kallas, Priit. "Top 15 Most Popular Social Networking Sites (and 10 Apps). DreamGrow. February 27, 2017. Accessed May 5, 2017 from: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/*
[7] *Nusca, Andrew. "Pinterest CEO Ben Silbermann: We're Not a Social Network." Fortune. July 13, 2015. Accessed May 5, 2017 from: http://fortune.com/2015/07/13/pinterest-ceo-ben-silbermann/*
[8] *Kallas, Priit. "Top 15 Most Popular Social Networking Sites (and 10 Apps). DreamGrow. February 27, 2017. Accessed May 5, 2017 from: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/*
[9] *People v Harris, 36 Misc. 3d 868, 878 (N.Y. City Crim. Ct. 2012)*
[10] *State v. Sublet, 113 A.3d 697, 702 (2015) and Griffin v. State, 19 A.3d 415, 2011 Md. LEXIS 226 (Md. Apr. 28, 2011)*
[11] *Wendy Angus-Anderson, Authenticity and Admissibility of Social Media Website Printouts, 14 Duke Law & Technology Review 33-47 (2015). Accessed May 8, 2017 from: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1282&context=dltr*
[12] *Id., page 11*
[13] *"How to Get Social Media Evidence Admitted to Court." The American Bar Association (ABA). November 16, 2016. Accessed May 9, 2017. Available at: http://www.americanbar.org/publications/youraba/2016/november-2016/how-to-get-social-media-evidence-admitted-to-court.html*
[14] *Id. citing Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro, Authentication of Social Media Evidence, 36 AM. J. TRIAL ADVOC. 433, 455 (2013).*
[15] *Griffin v. State, 19 A.3d 415, 2011 Md. LEXIS 226 (Md. Apr. 28, 2011)*
[16] *State v. Sublet, 113 A.3d 697, 442 Md. 632 (2015)*
[17] *The court found that having another person attempt to authenticate another user's social media account (in this case, the State's witness— a detective) would "[create the] potential for fabricating or tampering with electronically stored information on a social networking site, thus pos[ing] significant challenges from the standpoint of authentication of printouts of the site, as in the present case." Griffin v. State, 19 A.3d 415, 422.*
[18] *Griffin v. State, 19 A.3d 415, 427*
[19] *Id. at 428*
[20] *Griffin v. State, 19 A.3d 415, 2011 Md. LEXIS 226 (Md. Apr. 28, 2011)*
[21] *Griffin v. State, 19 A.3d 415, 423.*
[22] *State v. Sublet, 113 A.3d 697, 442 Md. 632 (2015)*
[23] *Id., at 715*
[24] *Id., at 709*
[25] *Id., at 709, 713*
[26] *Id., at 709, 718-719*
[27] *Id., at 720*
[28] *Id.*
[29] *Wendy Angus-Anderson, Authenticity and Admissibility of Social Media Website Printouts, 14 Duke Law & Technology Review 33-47 (2015). Referencing United States v. Vayner, 769 F.3d 125 (2d Cir. 2014); State v. Assi, No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. Ct. App. Aug. 21, 2012); People v. Valdez, 135 Cal. Rptr. 3d 628 (Ct. App. 2011); People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009); Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012); Manuel v. State, 357 S.W.3d 66 (Tex. Ct. App. 2011). Accessed May 8, 2017 from: http://scholarship.law.duke.edu/cgi/viewcontent cgi?article=1282&context=dltr*
[30] *Id. citing supra note 6, at 456.*
[31] *Tienda v. State, 358 S.W.3d 633, 2012 Tex. Crim. App. LEXIS 244, 2012 WL 385381 (Tex. Crim. App. 2012)*

appealed his murder conviction by alleging the state improperly admitted information gathered from the defendant's MySpace account through a subpoena.[32] The victim's sister then testified about the information posted on a MySpace account she believed the appellant defendant was responsible for registering and maintaining.[33]

On appeal, the defendant argued "that the State did not prove that he was responsible for creating and maintaining the content of the MySpace pages by merely presenting the photos and quotes from the website that tended to relate to him."[34] In response, the State argued that 1) "the contents of the social networking pages in this case contained sufficiently distinctive information to justify conditionally submitting them to the jury for its ultimate finding whether "the matter in question is what its proponent claims" and 2) the specificity of the content, an 'admission' by the appellant, was sufficient to tie him to this particular evidence and allow the jury to consider it for that purpose."[35] The Court of Criminal Appeals of Texas noted twenty-five identifying factors of Defendant's MySpace account that showed he was the owner of the account, including: his picture, email address, other demographic information, a link to a song played at the victim's funeral, pictures showing his gang tattoos, references to snitches, and conversations between him and other MySpace users about the ongoing investigation. "This combination of facts…is sufficient to support a finding by a rational jury that the MySpace pages that the State offered into evidence were created by the appellant. This is ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them."[36] The Court noted "It is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy… But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages."[37]

Briefly: After Showing Authenticity, Use Traditional Rules of Evidence to Prove the Case

Issues relating to weighing admissibility of social media evidence apply to jurisdictions whose evidence rules are patterned after the Federal Rules of Evidence ("FRE"). Therefore, regardless of whether a jurisdiction follows the Maryland or Texas approach, the most persuasive way of introducing social media evidence is to show as much "distinguishing" and circumstantial evidence as possible. This will help authenticate the evidence (FRE 901), and also show that the evidence is relevant and more probative than prejudicial (FRE 403). Prosecutors may also argue that a post, tweet, or social media conversation is being used as an admission under FRE 801(2). Postings can also be exceptions to hearsay (FRE 803) if they prove: present sense impressions, excited utterances, then existing mental, emotional, or physical condition of the declarant, etc. Of course, case law in each jurisdiction is precedent especially for proving authentication and ownership.

Notable Case Law from Smart Jurisdictions. (Most States use the Texas Approach)[38]

Similar to the Maryland and Texas Approaches, each jurisdiction's courts—state and federal— rule differently when it comes to authenticating evidence derived from social media. Make sure you know the case law in your jurisdiction. Here is a sampling of recent decisions from four Smart Prosecution jurisdictions.

New York: *U.S v. Meregildo.*[39] 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 "When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. See *Katz*, 389 U.S. at 351 (1967) (citations omitted)."[40] However, postings using

[32] *Tienda v. State, 358 S.W.3d 633*
[33] *Id., at 634*
[34] *Id., at 637*
[35] *Id., at 637*
[36] *Id., at 645*
[37] *Id., at 645-646.*
[38] *Id.*
[39] *U.S. v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y., 2012).*
[40] *Id., at 526*

Consider the following: a man walks to his window, opens the window, and screams down to a young lady, "I'm sorry I hit you, please come back upstairs." At trial, the People call a person who was walking across the street at the time this occurred. The prosecutor asks, "What did the defendant yell?" Clearly the answer is relevant and the witness could be compelled to testify. Well today, the street is an online, information superhighway, and the witnesses can be the third-party providers like Twitter, Facebook, Instagram, Pinterest, or the next hot social media application. ~ See,,People v. Harris

more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected. See *Katz*, 389 U.S. at 351-52 (citations omitted)." The court also stated, "Where 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."[41] 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.

New York: *People v. Harris.*[42] Defendant was charged with disorderly conduct after marching on roadway of the Brooklyn Bridge. 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 subsequently held that the defendant had no proprietary interest in the user information on his Twitter account, and he lacked standing to quash the subpoena.[43] 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 "If 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."[44]

New Jersey: *US v. Gatson*.[45] 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.[46] Defendant's Instagram account displayed photographs of himself with large amounts of cash and jewelry, which were possibly the proceeds from the underlying offense.[47] The court held that no search warrant is required for the consensual sharing of this type of information, and denied his motion to suppress.[48]

Washington: *State v. Kolanowski*.[49] Defendant appealed his conviction for rape and unlawful imprisonment. One issue on appeal was his argument that his counsel failed to authenticate a Facebook page of the victim— a photograph he argued showed she had access to her phone and was not with him during the time of the incident.[50] At trial, the victim testified that she did not have access to her phone at a certain time (later revealed to be when a Facebook picture of her was taken and uploaded). However, based on the record, the court ruled the introduction of the photo through proper identification "would not have advanced the defendant's case as authentication of the Facebook timestamp was at issue. Without proper authentication, the post was not relevant to the victim's credibility. But we simply cannot determine from this record what evidence the timestamp would have provided."[51]

Georgia: *Brown v. State.*[52] 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

[41] Id.
[42] People v Harris, 36 Misc. 3d 868, (N.Y. City Crim. Ct. 2012)
[43] Id., at 870
[44] Id., at 874
[45] US v. Gatson, 2014 U.S. Dist. LEXIS 173588, 2014 WL 7182275 (D.N.J. Dec. 15, 2014)
[46] Id., at *60
[47] Id., at *58
[48] Id., at *60 See generally U.S. v. Meregildo, 883 F. Supp. 2d 523 (S.D.N.Y. 2012).
[49] State v. Kolanowski, 2017 Wash. App. LEXIS 215 (Wash. Ct. App. Jan. 30, 2017)
[50] Id., at *5
[51] Id., at *13
[52] Brown v. State, 796 S.E.2d 283, 2017 Ga. LEXIS 29, 2017 WL 279532 (Ga. Jan. 23, 2017)

it at the homicide victim.[53] 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.[54] 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. The trial court further found that the admission of this evidence was harmless error that did not affect defendant's remaining convictions surrounding the murder, noting the testimony of the three eyewitnesses to the murder.

Anticipating Defense Arguments for Admitting Evidence Derived from Social Media

Defense counsel may successfully argue (in addition to authenticity) the following to preclude evidence gathered from social media.

Reliability: "Since photographs can be doctored and written posts can be edited and backdated, it can be difficult for judges to determine reliability of social media posts."[55] To address this concern, Law enforcement officers may sometimes obtain, confirm, or collaborate information gathered from social media through their own investigations including surveillance and witness affirmation. Subpoenas to the social media site may include metadata that confirms the date of the post or other indicia of reliability. See *People v Harris,* 36 Misc. 3d 868.

Relevancy and Prejudice: "Users often post playful images of themselves that are intended as jokes. These might be along the lines of flashing gang symbols."[56] Prepare to conduct a FRE 403 prejudicial v. probative balancing test. Probative evidence will be bolstered by contemporaneous investigations from law enforcement, including surveillance and witness testimony. If the judge rules to allow the evidence or testimony, be prepared with appropriate jury instructions.

How to Properly Investigate Social Media Cases Without Misconduct: Guidance from Bar Associations

Bar Associations across the country are beginning to pay close attention to what legal professionals are doing with social media, how they are doing it, and why they are doing it.[57] In 2009, the Philadelphia Bar Association was the first to delve into the ethical issue of using social media for legal investigations. Bar Associations agree that viewing a witness' public online profile is permissible because it is not a communication, but friending a represented witness to request otherwise restricted information amounts to impermissible communication with a represented party. Jurisdictions are split regarding friending unrepresented witnesses to gather information. The following chart summarizes ethical guidance from seven jurisdictions. Philadelphia, Pennsylvania's rules are the most restrictive when collecting evidence from social media, while New York's are the most liberal.

[53] Id., at 285
[54] Id., at 285-286
[55] Winterton, Danielle. "Social Media and Criminal Law." LegalMatch. Accessed May 9, 2017, available at: http://www.legalmatch.com/law-library/article/social-media-and-criminal-law.html
[56] Id.
[57] Harvey, Christina Vassiliou Harvey, Mac R. McCoy and Brook Sneath. "10 Tips for Avoiding Ethical Lapses When Using Social Media." Business Law Today. Accessed May 10 2017 from: http://www.americanbar.org/publications/blt/2014/01/03_harvey.html

Jurisdiction	Can attorney access a represented or unrepresented witness' **public** social media profile?[58]	Can attorney/agent[59] friend request to follow a **represented** witness with a **private** profile?	Can attorney/agent friend request or follow an **unrepresented** witness with a **private** profile?	Can attorney/agent create a fictional profile to friend a represented or unrepresented witness?[60]
Pennsylvania (Philadelphia)[61]	Yes	No	No[62]	No
New York[63] (NYC)[64]	Yes	No	No[65]	No
California (San Diego)[66]	Yes	No[67]	No, unless the requestor discloses affiliation to opposing party and the purpose of the request	No
New Hampshire[68]	Yes	No	No, unless the request identifies the lawyer by name and also identifies the client and matter in litigation	No
Oregon[69]	Yes	No	Yes, but the requesting attorney cannot state or imply she is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role, the lawyer shall make reasonable efforts to correct the misunderstanding.	No
Kentucky[70]	Yes	No	Unclear[71]	No
Washington, DC[72]	Yes	No	No, unless the lawyer identifies himself, state that he is a lawyer, and identify who he represents and the matter	No

[58]"As with represented parties, publicly viewable social media content is generally fair game. If, however, the information sought is safely nestled behind the [witness] third party's privacy settings, ethical contraints may limit the lawyers options for obtaining it." Harvey, Christina Vassiliou Harvey, Mac R. McCoy and Brook Sneath. "10 Tips for Avoiding Ethical Lapses When Using Social Media." Business Law Today. Accessed May 10 2017 from: http://www.americanbar.org/publications/blt/2014/01/03_harvey.html. The New York State Bar Association reasons, "Obtaining information about a party available in the Facebook or MySpace profile is similar to obtaining information that is available in publicly accessible online or print media..." See New York State Bar Association's Committee on Professional Ethics. Opinion # 843. (September 10, 2010). Accessed May 11, 2017 from: http://www.nysba.org/CustomTemplates/Content.aspx?id=5162 [59]Jurisdictions have rules (patterned by the ABA) about non-attorney assistants acting as agents for the attorney. The agent acts as an arm of the attorney. For example, the Pennsylvania Rules of Professional Conduct state the attorney is responsible for the actions of the agent. "a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if: the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved;..."See Pennsylvania Rules of Professional Conduct 5.3 (c)(1). "Responsibilities Regarding Nonlawyer Assistants." Available at: http://www.pacode.com/secure/data/204/chapter81/s5.3.html [60]The jurisdictions unanimously agree that creating a fictional profile to gain information from the witness violates multiple ABA rules by making a false or misleading statement. Applicable rules include: RPC 4.1 (Truthfulness in Statements to Others), 4.3 (Dealing with Unrepresented Person), 4.4 (Respect for Rights of Third Persons), 7.1 (Communication Concerning a Lawyer's Services), 7.4 (Communication of Fields of Practice and Specialization), and 8.4 (Misconduct). The New York City Bar Association explained, "We believe these rules are violated whenever an attorney 'friends' an individual under false pretenses to obtain information from a social networking site." The Association of the Bar of the City of New York Committee on Professional Ethics. Formal Opinion 2010-2. "Obtaining Evidence From Social Networking Websites." Page 3. Accessed May 11, 2017 from: http://www.nysba.org/CustomTemplates/Content.aspx?id=5162 [61]The Philadelphia Bar Association's Professional Guidance Committee. Opinion 2009-02. (March 2009). Accessed May 11, 2017 from: https://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf [62]The Philadelphia Bar Association's reasoning for the complete restriction of friending an unrepresented witness is based on an analysis of attorney misconduct from Pennsylvania's Rules of Professional Conduct, Rule 8.4(c), which is derived from ABA's RPC Rule 8.4: "Misconduct" "it is professional misconduct for a lawyer to... engage in conduct involving dishonesty, fraud, deceit, or misrepresentation." the friend request to access a private profile or page] omits a highly material fact, namely, that the third party who asks to be allowed access to the witness' pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness." The Philadelphia Bar Association's Professional Guidance Committee. Opinion 2009-02. (March 2009) at page 3. [63]New York State Bar Association's Committee on Professional Ethics. Opinion # 843. (September 10, 2010). Accessed May 11, 2017 from: http://www.nysba.org/CustomTemplates/Content.aspx?id=5162 [64]The Association of the Bar of the City of New York Committee on Professional Ethics. Formal Opinion 2010-2. "Obtaining Evidence From Social Networking Websites." Accessed May 11, 2017 from: http://www.nysba.org/CustomTemplates/Content.aspx?id=5162 [65]Unlike other jurisdictions that allow friending of an unrepresented party, New York does not pose any limitations (such as immediately telling the witness the attorney is representing an opposing party). "...We conclude that an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information about an unrepresented person's social networking website without also disclosing the reasons for making the request."(emphasis added)..."Rather than engage in 'trickery' [such as creating a fake account and friending the witness), lawyers can—and should—seek information maintained on social networking sites, such as Facebook, by availing themselves of informal discovery, such as the truthful 'friending' of unrepresented parties..." The Association of the Bar of the City of New York Committee on Professional Ethics. Formal Opinion 2010-2. (pages 2, 4) "Obtaining Evidence From Social Networking Websites." [66]The San Diego County Bar Association Legal Ethics Opinion 2011-2 (adopted by the San Diego County Bar Legal Ethics Committee May 24, 2011). Accessed May 11, 2017 from: https://www.sdcba.org/?pg=LEC2011-2 [67]SDCBA's opinion includes explains why sending a friend request amounts to communication, even when no actual discussion takes place. "An attorney's ex parte communication to a represented party intended to elicit information about the subject matter of the representation is impermissible no matter that words are used in the communication and no matter how that communication is transmitted to the represented party." Id. [68]The New Hampshire Bar Association. Ethics Committee Advisory Opinion #2012-13/05. "Social Media Contact with Witnesses in the Course of Litigation." Accessed May 11, 2017 from: https://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_05.asp [69]The Oregon Bar Association. Formal Opinion 2013-189 (2016 Revision). "Accessing Information about Third Parties through a Social Networking Website." Accessed May 11, 2017 from: http://www.osbar.org/_docs/ethics/2013-189.pdf [70]The Kentucky Bar Association. Ethics Opinion KBA E-434. November 17, 2012. Accessed May 11, 2017 from: http://c.ymcdn.com/sites/kybar.site-ym.com/resource/resmgr/Ethics_Opinions_(Part_2)_/kba_e-434.pdf [71]The Bar Association does not explicitly answer the question, but implores its members that the Rules of Professional Conduct require truthfulness and honesty when dealing with others, prohibit an attorney from maing false statements, and prohibit a lawyer from engaging in dishonest conduct. [72]The District of Columbia Bar Association. Ethics Opinion 371. "Social Media II: Use of Social Media in Providing Legal Services." Accessed May 11, 2017 from: https://www.dcbar.org/bar-resources/legal-ethics/opinions/Ethics-Opinion-371.cfm

In Summary: How to avoid misconduct during criminal investigations

1. Gather evidence from public pages or feeds where no potential for misrepresentation exists. "There is no reasonable expectation of privacy for tweets that the user has made public." [73]

2. See if a cooperating witness has access to the witness' social media page. Here there is no misrepresentation made by the attorney, and also no direct contact made to the witness. [74] See also *Meregildo*: "Where 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." [75]

3. Rely on law enforcement investigations. Courts generally have not questioned law enforcement for using false accounts or cooperating witnesses to gain access to social media sites. "Courts generally have not questioned law enforcement for using false accounts or cooperating witnesses to gain access to social media sites." [76]

4. Ask (or subpoena) opposing counsel for access to download the Facebook user's entire account (Facebook's "Download your information" tool is located under Account Settings.)

5. Subpoena the social media provider to access a user's account. See *U.S. v. Harris,*[77] where the Court held that pursuant to the State's subpoena, Twitter must provide information relevant to the dates of the investigation.

Conclusion

Social media provides prosecutors and law enforcement critical information and evidence to develop and prosecute cases. However, prosecutors must be aware of ethical considerations in their respective jurisdictions and adhere to ethical boundaries to guide them while prosecuting a case. In this vast and ever-evolving field, prosecutors should keep abreast of relevant case law and Bar Association opinions to aid them in the pursuit of justice.

BJA STAFF

Tammy Brown, *Senior Policy Advisor, Bureau of Justice Assistance*

APA STAFF

Beth Merachnik, *Project Director, Association of Prosecuting Attorneys*
Margo Badawy, *Project Attorney, Association of Prosecuting Attorneys*
Kristi Barksdale, *Project Associate, Association of Prosecuting Attorneys*
Angel Tucker, *Director of Communications, Association of Prosecuting Attorneys*
Rashaund Savage, *Senior Graphic Designer, Association of Prosecuting Attorneys*

This article was supported by Grant No. 2014-YX-BX-K001 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

SmartProsecution.APAInc.org | APAInc.org

ASSOCIATION OF PROSECUTING ATTORNEYS

[73] People v Harris, 36 Misc. 3d 868, 875.
[74] The New Hampshire Bar Association explains that unlike a situation where an attorney asks someone to friend a witness, the a situation where a person, not acting as an agent at the behest of the lawyer, obtains information from the witnesses social media account is permissible. "The difference in the latter context is there is no deception by the lawyer. The witness chose to reveal information to someone who was not acting on behalf of the lawyer. The witness took the risk that the third party might repeat the information to others." The New Hampshire Bar Association. Ethics Committee Advisory Opinion #2012-13/05. "Social Media Contact with Witnesses in the Course of Litigation."
[78] U.S. v. Meregildo, 883 F. Supp. 2d 523, 526
[79] "The Legal Ethics of Social Media." The New Jersey Attorney General's Advocacy Institute. September 13, 2016. Page 10. Accessed May 11, 2017 from: (http://www.njadvocacyinstitute.com/course-materials/njagai--legal-ethics-of-social-media--class-materials.pdf)
[80] People v Harris, 36 Misc. 3d 868