Social Media and the First Amendment

Griffin v. State, 19 A.3d 415, (Md. Apr. 28, 2011)
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 of Appeals of Maryland, 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." Thus, in Maryland, under Griffin, the proponent must therefore affirmatively disprove the existence of a different creator for the evidence to be admissible.

State v. Sublet, 113 A.3d 697, 442 Md. 632 (2015)
Sublet established Maryland's standard that a "context-specific determination" whether the proof advanced is sufficient to support finding that the item in question (ownership of a social media page) is what its proponent claims it to be. 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). The Court also recognized "In the period since Griffin had been decided, cases in which authentication of social networking websites and postings has been addressed have proliferated." 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 other people could and had presumably accessed and changed or inserted information on the witness' page, thereby attributing it 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." 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 authenticity 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 Maryland 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 their author, including that they demonstrated that "OMGitsLOCO and TheyLovingTc knew about the plan for a shooting." 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.” 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.

Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012)

The defendant unsuccessfully appealed his murder conviction by alleging the state improperly admitted information gathered from the defendant’s MySpace account, through a subpoena. 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. 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.” 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 the 2) 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.” 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.” 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.”

U.S v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y., 2012).
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)." However, postings using 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." 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.

People v. Harris. 36 Misc. 3d 868, (N.Y. City Crim. Ct. 2012)
Defendant was charged with disorderly conduct after marching on roadway of 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. 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 newer information 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."

US v. Gatson, 2014 U.S. Dist. LEXIS 173588, (D.N.J. Dec. 15, 2014)
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 Gatson 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.

State v. Kolanowski, 2017 Wash. App. LEXIS 215 (Wash. Ct. App. Jan. 30, 2017)
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. 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."

Brown v. State, 796 S.E.2d 283 (Ga. Jan. 23, 2017)
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 victim. During the trial, city investigator and expert witness on 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— most 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 agreed with the trial court 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.

Bradley v. State, 359 S.W.3d 912, 2012 Tex. App. LEXIS 1076, 2012 WL 403279 (Tex. App. Houston 14th Dist. 2012)
Two defendant brothers robbed victim, taking various personal property from victim, including victim's own handgun. Defendant 1 pled guilty, and Defendant 2 was convicted at trial, despite Defendant 1 testifying his accomplice was another man. Throughout Defendant 2's trial, defense relied on the theory of mistaken identity. After the robbery, victim identified both defendants on two separate locations. Victim asked someone the names of the brothers, and located them on Facebook, where Defendant 2 posed with a gun like the one stolen from victim. Victim emailed these photos to detectives and then to positively identified both men at a lineup. One of the issues on appeal was whether the lineup was improper. However, the court upheld the conviction, stating, at 918, "Even if we assume, without deciding, the arrays were impermissibly suggestive, the in-court testimony is still admissible "as long as the record clearly reveals that the witness'[s] prior observation of the accused was sufficient to serve as an independent origin for the in-court identification." Citing Jackson v. State, 657 S.W.2d 123, 130 (Tex. Crim. App. 1983)."

U.S. v. Browne. (3rd Cir. 2016) (D.C. No. 3-13-cr-00037-001)
The case is available
at: http://www2.ca3.uscourts.gov/opinarch/141798p.pdf Defendant began messaging an 18 year old woman on Facebook messenger. They later met and exchanged sexually explicit photographs on Facebook Messenger. Defendant threatened victim he would release her explicit photos unless she engaged in oral sex with him. He said he would only delete the photos if she provided her password. Upon receiving her password, he logged in to her account and began messaging minors, from whom he received sexually explicit photographs. He repeated the same pattern with the minors as he did with the first victim. At trial, the Court allowed five Facebook-produced chat logs with certificates of authenticity into evidence per Federal Rules of Evidence 803(6), which the custodian certified ""were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook . . . [and] were made at or near the time the information was transmitted by the Facebook user." App. 403; see Fed. R. Evid. 803(6)." Defendant's appeal rested solely on the issue of the Facebook chat records not being properly authenticated and improperly introduced as evidence. In its decision to uphold the conviction, the court noted this was an issue of first impression. The court held that the records were not self-authenticating under an 803(6) analysis, but that there was sufficient extrinsic evidence to introduce them under a traditional 901 analysis (that the Government must produce sufficient evidence to support a finding the evidence is what the government claims it to be). Finally the court decided that although hearsay because the chats "at least in part to prove the truth of the matter asserted, that is, that [Defendant] sexually assaulted [a victim] and subsequently threatened her with video evidence, p. 26 , the records were admissible because erroneously admitting them "did not perceive grounds for reversal. Reversal is not warranted if it is "highly probable that the error did not contribute to the judgment."p. 28; and the record indicated more than sufficient extrinsic evidence to link defendant to the chats and satisfy the government's authentication burden under FRE 901.

Sublet v. State, 113 A.3d 695, 442 Md. 632, 2015 Md. LEXIS 289, 2015 WL 2226252 (Md. 2015)
Petitioner Defendant was charged with assault after a fight broke out between himself and his girlfriend's mother. During cross-examination of the mother, Defendant sought to introduce four pages of printed Facebook chat conversations she had with seven different people. Photo icons (profile pictures) of each person appeared next to the chat, along with the time of the chat and the date. The witness stated she did not write the entries on the fourth page and did not know where they came from, but she did admit to writing the exchanges appearing on the first three pages. The judge did not allow the evidence after the witness explained she gave her password to other people and could therefore not authenticate the contents. This was affirmed, as the hight court notes that to authenticate social networking evidence pursuant to Md. R. 5-901, the trial judge had to determine there was proof from which a reasonable juror could find that the evidence was what the proponent claimed. Here, because the witnesses denied making some of

the exchanges, and testified she gave her Facebook password to other people, the exhibit could not be properly authenticated to be admissible.

People v. Valdez, 201 Cal. App. 4th 1429, 1434–37 (Cal. App. 4th Dist. 2011).
Defendant was convicted of various charges stemming from a drive-by shooting incident. Defendant challenged introducing printouts of his social media accounts that the State's police expert presented at trial, containing pictures and other biographical information showing purported gang affiliation. The expert explained that although the profile is accessible to the public, only the individual who created the profile, or one who has access to that person's login ID and password, can upload or manipulate content on the page. The page icon displayed a photograph of defendant's face, and the page included greetings addressed to him by name and by relation. The page owner's stated interests, including an interest in gangs, matched what the police otherwise knew of defendant's interests from their field contacts with him. A photograph on the page of defendant forming a gang signal with his right hand met the threshold required for the jury to determine its authenticity. The page was password-protected for posting and deleting content. Defendant's hearsay challenge lacked merit because the trial court did not admit the material for the truth of any assertion on the page. The gang evidence was relevant and probative. Therefore, the court held that a reasonable trier of fact could conclude from the information posted— including personal photographs, communications, and other details—that the social media profile belonged to the defendant.

Elonis v. U.S., 575 U.S._(2015)
Petitioner was indicted for five counts of making threats to injure various individuals including his estranged wife, co-workers and law enforcement in violation of 18 U.S.C. s. 875(c), after posting threats about his wife and co-worker on his Facebook account. His wife testified at trial that she feared the posts as serious threats, prompting her to obtain a three-year restraining order. Elonis claimed the posts were fabricated and not intended to resemble an actual individual. After the Court of Appeals confirmed his conviction, the Supreme Court reversed the conviction and remanded the case. The Court held the statute, 18 U.S.C. s.875(c) not only requires proof that a communication was transmitted and that it contains a threat, it also requires proof of the offender's mental state. Further, the lower court's jury instruction regarding a reasonable person's view of the communication is consistent with civil liability in tort law and not sufficient to meet the legal requirement for criminal conduct. In light of the Opinion, the Supreme Court stated it is unnecessary to consider any First Amendment issue.

Bradley v. State, 359 S.W.3d 912, 2012 Tex. App. LEXIS 1076, 2012 WL 403279 (Tex. App. Houston 14th Dist. 2012).
Two defendant brothers robbed victim, taking various personal property from victim, including victim's own handgun. Defendant 1 pled guilty, and Defendant 2 was convicted at trial, despite Defendant 1 testifying his accomplice was another man. Throughout Defendant 2's trial, defense relied on the theory of mistaken identity. After the robbery, victim identified both defendants on two separate locations. Victim asked someone the names of the brothers, and located them on Facebook, where Defendant

2 posed with a gun like the one stolen from victim. Victim emailed these photos to detectives and then to positively identified both men at a lineup. One of the issues on appeal was whether the lineup was improper. However, the court upheld the conviction, stating, at 918, “Even if we assume, without deciding, the arrays were impermissibly suggestive, the in-court testimony is still admissible "as long as the record clearly reveals that the witness'[s] prior observation of the accused was sufficient to serve as an independent origin for the in-court identification." Citing Jackson v. State, 657 S.W.2d 123, 130 (Tex. Crim. App. 1983).”

U.S. v. Browne. (3rd Cir. 2016) (D.C. No. 3-13-cr-00037-001).
The case is available at: http://www2.ca3.uscourts.gov/opinarch/141798p.pdf Defendant began messaging an 18 year old woman on Facebook messenger. They later met and exchanged sexually explicit photographs on Facebook Messenger. Defendant threatened victim he would release her explicit photos unless she engaged in oral sex with him. He said he would only delete the photos if she provided her password. Upon receiving her password, he logged in to her account and began messaging minors, from whom he received sexually explicit photographs. He repeated the same pattern with the minors as he did with the first victim. At trial, the Court allowed five Facebook-produced chat logs with certificates of authenticity into evidence per Federal Rules of Evidence 803(6), which the custodian certified ““were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook . . . [and] were made at or near the time the information was transmitted by the Facebook user.” App. 403; see Fed. R. Evid. 803(6).” Defendant’s appeal rested solely on the issue of the Facebook chat records not being properly authenticated and improperly introduced as evidence. In its decision to uphold the conviction, the court noted this was an issue of first impression. The court held that the records were not self-authenticating under an 803(6) analysis, but that there was sufficient extrinsic evidence to introduce them under a traditional 901 analysis (that the Government must produce sufficient evidence to support a finding the evidence is what the government claims it to be). Finally the court decided that although hearsay because the chats “at least in part to prove the truth of the matter asserted, that is, that [Defendant] sexually assaulted [a victim] and subsequently threatened her with video evidence, p. 26 , the records were admissible because erroneously admitting them “did not perceive grounds for reversal. Reversal is not warranted if it is “highly probable that the error did not contribute to the judgment.”p. 28; and the record indicated more than sufficient extrinsic evidence to link defendant to the chats and satisfy the government’s authentication burden under FRE 901.

Sublet v. State, 113 A.3d 695, 442 Md. 632, 2015 Md. LEXIS 289, 2015 WL 2226252 (Md. 2015).
Petitioner Defendant was charged with assault after a fight broke out between himself and his girlfriend’s mother. During cross-examination of the mother, Defendant sought to introduce four pages of printed Facebook chat conversations she had with seven different people. Photo icons (profile pictures) of each person appeared next to the chat, along with the time of the chat and the date. The witness stated she did not write the entries on the fourth page and did not know where they came from, but she did admit to

writing the exchanges appearing on the first three pages. The judge did not allow the evidence after the witness explained she gave her password to other people and could therefore not authenticate the contents. This was affirmed, as the hight court notes that to authenticate social networking evidence pursuant to Md. R. 5-901, the trial judge had to determine there was proof from which a reasonable juror could find that the evidence was what the proponent claimed. Here, because the witnesses denied making some of the exchanges, and testified she gave her Facebook password to other people, the exhibit could not be properly authenticated to be admissible.

People v. Valdez, 201 Cal. App. 4th 1429, 1434–37 (Cal. App. 4th Dist. 2011). Defendant was convicted of various charges stemming from a drive-by shooting incident. Defendant challenged introducing printouts of his social media accounts that the State's police expert presented at trial, containing pictures and other biographical information showing purported gang affiliation. The expert explained that although the profile is accessible to the public, only the individual who created the profile, or one who has access to that person's login ID and password, can upload or manipulate content on the page. The page icon displayed a photograph of defendant's face, and the page included greetings addressed to him by name and by relation. The page owner's stated interests, including an interest in gangs, matched what the police otherwise knew of defendant's interests from their field contacts with him. A photograph on the page of defendant forming a gang signal with his right hand met the threshold required for the jury to determine its authenticity. The page was password-protected for posting and deleting content. Defendant's hearsay challenge lacked merit because the trial court did not admit the material for the truth of any assertion on the page. The gang evidence was relevant and probative. Therefore, the court held that a reasonable trier of fact could conclude from the information posted— including personal photographs, communications, and other details—that the social media profile belonged to the defendant.

Packingham v. North Carolina U.S.____ (2017)
The Supreme Court held that a North Carolina law (N.C. Gen. Stat. § 14-202.5) that made it a felony for prohibited convicted sex offenders to use social media violated the first amendment (the North Carolina legislature reasoned that convicted sex offenders knew children could make accounts on social media). Defendant, a convicted sex offender, was charged under this law after he posted information on a social media account about an unrelated traffic case. The Supreme Court held North Carolina's statute unconstitutional, and that social media (including Facebook, Amazon, etc.) is a protected space under the First Amendment. The Supreme Court explained that the State had not met its burden to show that "this sweeping law is necessary or legitimate to serve its purpose of keeping convicted sex offenders away from vulnerable victims." The Court explained that North Carolina could protect children through less restrictive means, such as prohibiting "conduct that often presages a sexual crime, like contacting a minor or using a website to gather information about a minor."