Social Media Evidence and the Law: Obtaining Information and Admitting It Into Evidence
December 6, 2023

I. **Introduction**
    a. What is social media? Think outside of the box
        i. Networks
            1. Facebook/Meta, Instagram/Threads, Twitter/X, etc.
        ii. "Content hubs"
            1. Aggregators like Reddit
            2. Blogs, vlogs
            3. Tik tok
        iii. Forms of communication
            1. Text based
                a. Discord, Slack
            2. Messaging based
                a. What's App, Signal
            3. Video based
                a. Snapchat
        iv. Photo sharing
            1. Pinterest
        v. Video sharing
            1. Youtube
        vi. Location based
            1. Nextdoor, Meetup
        vii. Profession based
            1. LinkedIn
        viii. Fitness based
            1. Nike Run Club, Strava, Peloton
    b. Users in millions as of October 2021

Platform	Number of Active Users (in Millions)
Facebook	2895
YouTube	2291
WhatsApp	2000
Instagram	1393
Facebook Messenger	1300
Weixin/WeChat	1251
TikTok	1000
Douyin	600
QQ	591
Sina Weibo	566
Telegram	550
Snapchat	538
Kuishou	506
Pinterest	454
Twitter	436
Reddit	430

c. Demographics
    i. According to Pew Research, majorities of 18- to 29-year-olds say they use Instagram or Snapchat and about half say they use TikTok, with those on the younger end of this cohort – ages 18 to 24 – being especially likely to report using Instagram (76%), Snapchat (75%) or TikTok (55%).
    ii. These shares stand in stark contrast to those in older age groups. For instance, while 65% of adults ages 18 to 29 say they use Snapchat, just 2% of those 65 and older report using the app – a difference of 63 percentage points.
    iii. About half of Hispanic (52%) and Black Americans (49%) say they use the platform, compared with smaller shares of White Americans (35%) who say the same
    iv. Hispanic Americans (46%) are far more likely to say they use WhatsApp than Black (23%) or White Americans (16%).
    v. Those with higher levels of education are again more likely than those with lower levels of educational attainment to report being LinkedIn users. Roughly half of adults who have a bachelor's or advanced degree (51%) say they use LinkedIn, compared with smaller shares of those with some college experience (28%) and those with a high school diploma or less (10%)
    vi. Women continue to be far more likely than men to say they use Pinterest when compared with male counterparts, by a difference of 30 points (46% vs. 16%).
    vii. There are large differences in use of this platform by community type. Adults living in urban (17%) or suburban (14%) areas are more likely to say they use Nextdoor. Just 2% of rural Americans report using the site.

d. The decline of Facebook?
    i. Despite many articles heralding the end of Facebook and social media generally, Facebook continues to reign supreme
    ii. In 2023, only 31% of US adults say that they "never" use social media
    iii. 30% of US adults regularly get news on Facebook
    iv. In 2020, 3% of people surveyed by Pew Research said they regularly get news from TikTok. In 2023, that number had more than quadrupled to 14%
    v. People in the US have an average of 7/1 social media accounts. Globally, it's 8.4 accounts per person.
    vi. 84% of people aged 18 to 29 use at least one social media platform, and 81% of people between the ages of 30 to 49 use at least one platform
    vii. Most surprising? 45% of those in the 65+ age group use at least one platform
    viii. 39% of US online users agree with the statement, "I am addicted to social media."

e. Fitness apps and wearable devices
    i. Example devices
        1. Apple Watch/Samsung Watch/Google Pixel Watch
        2. Fitbit
        3. Garmin
        4. Amazfit
        5. Oura Ring
        6. Whoop recovery tracker
    ii. Cases
        1. *Hinostroza v. Denny's Inc.* 2018 U.S. Dist. LEXIS 109602, at *11–12 (D. Nev. June 29, 2018).
            a. A woman slipped and fell at a restaurant and allegedly sustained injuries resulting in a future back surgery
            b. Before the incident, she had two prior slip and falls and was involved in an auto accident
            c. Defendant restaurant requested data from a fitness activity tracker
            d. Plaintiff responded that she had nothing responsive in her custody or control
            e. The Court ordered that she respond and describe the search that she conducted for responsive documents
        2. Bartis v. Biomet, Inc., 2021 WL 2092785 [E.D. Mo. May 24, 2021]
            a. Multiple plaintiffs claimed that they sustained injuries including permanent mobility issues as a result of the implantation of an artificial hip made by Biomet
            b. One plaintiff responded in discovery that he continuously wore a Fitbit to track his number of steps, heart rate, and sleep
            c. Defendants requested "all data from the Fitbit and any other wearable device or other fitness tracker."
            d. Plaintiff objected that the data was "unreliable" because he began wearing the Fitbit after the revision surgery removing the Biomet device
            e. The Court ordered Plaintiff to produce the data. The Court noted specifically that Plaintiff had provided inconsistent responses as to whether he experienced difficulty or pain when walking and jogging
        3. A state court in Oregon granted a defendant's motion to compel discovery of the plaintiff's wearable technology information
            a. The request in that case was for production of: ""[a]ll documents, records, data, or information reflecting plaintiff's personal fitness, diet, or other lifestyle management. This includes, but is not limited to, data and information from hardware (including wearable technology), software, or personal

computing/telecommunication e-applications, e-logs, and e-diaries"

4. But be careful!
    a. Spoljaric v. Savarese, 66 Misc. 3d 1220(A), 121 N.Y.S.3d 531 (N.Y. Sup. Ct. 2020)
        i. Plaintiff claimed to have sustained personal injuries in a motor vehicle accident
        ii. Defendant issued discovery for authorizations for all data pertaining to plaintiff's Fitbit device
        iii. Defendant moved to compel production when plaintiff refused
        iv. Defendant argued that the basis for the request was that the plaintiff had lost fifty pounds since the accident, and defendant was entitled to see how plaintiff did this despite his claim of lasting injury
        v. In deposition, Plaintiff testified that he very rarely checked his Fitbit and mostly used it as a watch to tell time
        vi. The court noted, "As diet, not just exercise, is a more important component of weight loss, this argument had little 'weight'" and characterized the request as a fishing expedition

iii. Widenor v. Patiala Express Inc., No. SA-21-CV-00962-FB, 2022 WL 3142621, at *3 (W.D. Tex. Aug. 4, 2022)

1. Defendant requested all fitness data, from any fitness tracker such as an Apple Watch, that Plaintiff had worn since the accident
2. Plaintiff testified in his deposition that he owns and wears an Apple Watch and wore it during the relevant time period
3. The Court took a skeptical approach and instructed the parties to confer as to what data Plaintiff had in his possession and whether it was in a form that could be produced to Defendant.
4. "If not, Defendant should subpoena the records from Apple."

II. <u>Acquiring Social Media Evidence</u>

a. Timing
    i. Begin your search as soon as you receive notice of the claim or lawsuit
    ii. Preservation letters
    iii. When you see something, save something
        1. Screenshots

2. Print to PDF
3. If all else fails, print to a printer and scan

iv. Recheck frequently, particularly if you have an avid sharer

b. Targets
   i. The parties
   ii. Family
   iii. Friends
   iv. Groups that the partis are a part of
   v. Party employers

c. Techniques
   i. Creative searches
      1. Do not only search a person's name in Google. Try adding terms that will help guarantee that you find *your* target like the city, state, or even family member names
   ii. Discovery requests
      1. Generally, courts will allow discovery of material posted to social media networking sites if it is relevant to the litigation and the discovery request is narrowly tailored
         a. *McCann v. Harleysville Ins. Co.*, 78 A.D.3d 1524, 1525, 910 N.Y.S.2d 614 (App. Div. 2010).
      2. "Narrowly tailored"
   iii. Subpoenas? Not usually…

III. <u>Discovery Requests</u>

a. Duty to preserve?
   i. How to preserve
      1. Some social media accounts have made this simple:
         a. Facebook: Go to Settings, Settings and Privacy, "Transfer a copy of your information"
   ii. Use of litigation preservation letters

b. Relevance
   i. Are you going fishing?
      1. In a personal injury case, "the fact that plaintiff had previously used Facebook to post pictures of herself or to send messages is insufficient to warrant discovery of this information." *Kelly Forman v. Mark Henkin*, 2015 N.Y. App. LEXIS 8353 (Dec. 17, 2015).
         a. Simply because the plaintiff's Facebook postings "might reveal daily activities that contradict claims of disability" is "nothing more than a request to conduct a fishing expedition." *Id.*
      2. But, other courts take a broader view:
         a. In a slip and fall case, the plaintiff took down hundreds of photographs from his Facebook page following the deposition. *Nucci v. Target Corp.*, 162 So.3d 136, 154 (Fla. 4th DCA 2015). The appellate court upheld the trial court order requiring production of photographs from two years prior to the incident.

Id. "We agree with those cases concluding that generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings that the user may have established." *Id.*

ii. *Rodriguez-Ruiz v. Microsoft Operations Puerto Rico, L.L.C.*, No. CV 18-1806 (PG), 2020 WL 1675708, at *1 (D.P.R. Mar. 5, 2020)
    1. Plaintiff alleged that he was wrongfully terminated by Microsoft in violation of the Americans with Disabilities Act
    2. He alleged that he suffers from cerebral palsy, headaches, and back pain
    3. Microsoft sent requests for production for the Plaintiff's Facebook or social media profiles
        a. How broad?
        b. "Complete copy of your profile, including, without limitation, all messages, posts, status updates, comments on your wall or page, causes and/or groups to which you have joined, which are in your account and which were published or posted between January 2010 and the present, related or referring to any emotions, feelings, mental status, or mood status"
        c. "Copy of all communications from you, whether through private messages in your profile or messages on your wall or page, which may provide context to the communication mentioned in the previous sub-section."
        d. " Any and all photos taken and/or uploaded to your account between January 2010 and the present."
        e. A request for the complete download of the entire Facebook account
    4. Plaintiff objected that the requests were not related in any way to the case, were overbroad, burdensome, offensive, and a violation of Plaintiff's right to privacy
    5. As always, start with Rule 26(b)(1)
        a. Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case ... Information within this scope of discovery need not be admissible in evidence to be discoverable
    6. "[i]nformation posted on a private individual's social media 'is generally not privileged, nor is it protected by common law or civil law notions of privacy"
    7. Relevant to what?
        a. "Several courts have found that the contents of a plaintiff-employee's social media profile, postings, or messages (including status updates, wall comments,

causes joined, groups joined, activity streams, blog entries during a relevant time period) are relevant and discoverable in employment cases which include claims of emotional distress, when they 'reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state.'"

b. Though courts have concluded that information posted or published on a party's social media page may be relevant, courts generally do not "endorse an extremely broad request for all social media site content."
c. "[A] party does not have 'a generalized right to rummage at will through information that [an opposing party] has limited from public view.' "
d. The fact that a plaintiff's mental or emotional state is at issue does not "automatically justify sweeping discovery of social media content."

8. Social media content that is reflective of a person's emotional state is relevant and discoverable when the same has been placed at issue. For example:
    a. "[P]osts specifically referencing the emotional distress plaintiff claims to have suffered or treatment plaintiff received in connection with the incidents alleged in [his] complaint and posts referencing an alternative potential source of cause of plaintiff's emotional distress are discoverable. ... In addition, posts regarding plaintiff's social activities may be relevant to plaintiff's claims of emotional distress and loss of enjoyment of life."
9. The Court ordered Plaintiff's counsel to review all of Plaintiff's social media content from January 2010 through the present () and produce any and all content referencing Plaintiff's emotions, feelings, mental status, or mood status, including any photographs which may have accompanied such posts or comments
    a. The court also ordered the same consideration of every uploaded photo
    b. The court noted that Microsoft could challenge the production if it believed the production fell short

c. Narrow tailoring
    i. *Root v. Balfour Beatty Const. LLC*, 132 So. 3d 867 (Fla. 2d DCA 2014),
        1. Second District Court of Appeal considered the propriety of an order compelling the production of Facebook pages.
        2. The trial court required the plaintiff, who was claiming loss of consortium following injury to her three-year-old son, to produce electronically stored information relating to her

mental health, alcohol use, and relationships with friends and family members.
3. The appellate court considered whether the order was overly broad, and began by noting that "trial courts around the country have repeatedly determined that social media evidence is discoverable."
4. As the plaintiff's claim was premised upon loss of consortium, the court stated that discovery should have been limited to evidence related to the impact of the child's injury upon his mother.
5. As such, the compelled production was irrelevant and the discovery order was quashed.
6. The court did conclude with the following caveat: "Should further developments in the litigation suggest that the requested information may be discoverable, the trial court may have to review the material in camera and fashion appropriate limits and protections regarding the discovery."

ii. *Nucci v. Target Corp*., 162 So. 3d 146 (Fla. 4th DCA 2015),
1. Fourth District Court of Appeal conducted certiorari review of a lower court order compelling the discovery of photographs from a personal injury plaintiff's Facebook account
2. Plaintiff claimed she slipped and fell on a foreign substance on the floor of a Target store
3. Target sought production of photographs from the plaintiff's Facebook page, alleging that it was entitled to view her profile, as her lawsuit placed her physical and mental condition at issue
4. The plaintiff responded by asserting that disclosure violated her reasonable expectation of privacy and contended that Target's motion amounted to a fishing expedition
5. Target narrowed down its requests, and the plaintiff raised objections, including relevance.
6. The trial court ordered the plaintiff to provide copies or screenshots of all of the photographs associated with her social networking account for two years prior to the alleged fall.
7. The appellate court rejected the privacy claims, finding that social networking site content is neither privileged nor protected and found that the discovery order was narrowly tailored in scope, thus, reasonably calculated to lead to admissible evidence relating to the plaintiff's physical condition

IV. <u>Subpoenas</u>

a. Stored Communications Act (18 U.S.C. 121 §§ 2701-2713)
   i. Addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records"

ii. Enacted October 21, 1986
iii. Limits the ability of the *government* to compel third-party Internet service providers (ISPs) to turn over content information and non-content information (such as logs and other back-end information).
iv. Also limits the ability of the ISPs *themselves* to reveal content information to non-government entities

b. Section 2701
    i. Criminal penalties for anyone who intentionally accesses without authorization a facility through which an electronic communication service is provided and thereby obtains, alters, or prevents authorized access to a communication in storage

c. Section 2702
    i. 2702(b) describes conditions under which a provider can voluntarily disclose customer communications or records.
        1. Nine scenarios, including to the addressee/intended recipient, with the consent of the originator, or in emergency cases such as a missing child.
    ii. Targets two types of online service, "electronic communication services" and "remote computing services."
        1. The statute defines an electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications."
        2. A remote computing service is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."
        3. In general, ISPs are forbidden to "divulge to any person or entity the contents of any communication which is carried or maintained on that service."
        4. However, ISPs are allowed to share "non-content" information, such as log data and the name and email address of the recipient, with anyone other than a governmental entity.
        5. In addition, ISPs that do not offer services to the public, such as businesses and universities, can freely disclose content and non-content information

d. Section 2703
    i. When can the government compel an ISP to disclose customer or subscriber content and non-content information for electronic communication services and remote computing services
    ii. Important distinction
        1. Contents of electronic communications in <u>electronic storage</u>
        2. Contents of electronic communications in a <u>remote computing service</u>
    iii. What is "electronic storage"? See 18 U.S.C. 2510
        1. any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

2. any storage of such communication by an electronic communication service for purposes of backup protection of such communication

iv. Compelled disclosure of communications in electronic storage
    1. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant
    2. If it has been in storage for *more* than 180 days, then it is treated as a communication in a remote computing service
v. Compelled disclosure of communications in a remote computing service
    1. Government may require a provider of remote computing service to disclose the contents of any wire or electronic communication:
        a. without notice to the subscriber or customer if the government obtains a warrant; or
        b. with prior notice to the subscriber or customer if the government uses an administrative subpoena authorized by federal or state statute (or by federal or state grand jury or trial subpoena); or obtains a court order
            i. But, delayed notice can be given pursuant to Section 2705
vi. Why does the distinction matter?
    1. Communications held in electronic communications services require a warrant. Those in remote computing services require only a subpoena or court order with prior notice
    2. Constitutionality is in question
        a. In *United States v. Warshak* (2010), the Sixth Circuit found that email users have a Fourth Amendment-protected reasonable expectation of privacy in the contents of their email accounts and that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional

e. Section 2704
    i. Addresses backup preservation
f. Section 2705
    i. Provides for gag orders where a recipient of a Section 2703(d) order compelling production cannot disclose the existence of the order or the investigation
g. Section 2706
    i. Addresses cost reimbursement – the government entity pays the party providing the information in an amount mutually agreed upon

h. Section 2707
    i. Gives rise to civil action and addresses damages, defenses, statute of limitations (2 years after discovery or reasonable opportunity to discover the violation), and improper disclosure
i. Section 2708
    i. Exclusivity of remedies
j. Section 2709
    i. An electronic communication service provider has a duty to comply with a request for subscribing information, toll billing records, and electronic communication transactional records in its custody made by the Director of the FBI
k. Section 2710
    i. Deals with wrongful disclosure of videotape rental or sale records
l. Section 2711
    i. Definitions
    ii. Just four of them: "remote computing service," "court of competent jurisdiction," "and "government entity."
    iii. Note that it also refers you to the definitions given in 18 U.S.C. § 2510 which is where the bulk of the definitions needed are found
        1. Electronic communication
            a. Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce
        2. Electronic communications system
            a. Any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, <u>and</u> any computer facilities or related electronic equipment for the electronic storage of such communications
        3. Electronic communications service
            a. Any service which provides to users thereof the ability to send or receive wire or electronic communications
m. What does any of this have to do with social media?
    i. Social media did not exist in 1986 when this law was enacted
    ii. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 *(C.D. Cal. 2010)*
        1. Plaintiff alleged that he granted the defendants an oral license to use his works of art in a limited manner in connection with making garments. Plaintiff alleged that the defendants agreed to use his logo on the apparel, but failed to do so. Plaintiff also alleged that at times they attributed the artwork to others, or at times to one of the defendants. He sued for breach of contract, copyright infringement, and other claims
        2. In February 2010, defendants served supoenaes on Facebook, Myspace, and two other businesses. The

subpoenas to the social media companies sought the plaintiff's basic subscriber information, along with all communications that referred or related to the defendants or the Ed Hardy brand. Defendants argued that the information was relevant in determining the nature and terms of the agreement, if any.

3. Plaintiff moved to quash the subpoenas, arguing that the social media companies were prohibited from disclosing electronic communications as ISPs under 18 U.S.C. Section 2701
4. First, the magistrate judge ruled that the social media companies were not electronic communications service providers and that the materials sought were not in electronic storage
5. On motion for reconsideration, the court took a new turn
6. The court noted that the Act defines an electronic communications service provider as "any service which provides to users thereof the ability to send or receive wire or electronic communications."
7. An ECS provider cannot knowingly divulge the contents of a communication while in electronic storage by that service (see Section 2702(a)(1)(b))
8. Note – none of the social media companies themselves moved to quash the subpoena
    a. The court found that Plaintiff had standing
9. The court reasoned that there is no provision in the statute for disclosure of communications to a third party by subpoena
10. The court noted that an ECS provider includes "*any* service" which provides the ability to send or receive electronic communications
11. The court observed that both Facebook and Myspace allowed for private messaging. Also important for the court was the fact that "wall postings" were not strictly public. Instead, the user can choose who can access the wall, making it difficult to distinguish from an online bulletin board
12. The court therefore held that Facebook and Myspace were ECS providers
13. That does not end the inquiry. The court then had to determine if the information sought was in electronic storage
    a. The court held that the wall postings were "stored for backup purposes" under the statute (and are therefore in electronic storage).
    b. The court also held "in the alternative" that Facebook and Myspace were RCS providers.
14. The court quashed the subpoenas as to private messages stored by Facebook and Myspace

15. As to the wall postings, the court concluded that it did not have sufficient evidence in the record as to whether Plaintiff's "wall" was fully accessible to the public or in some manner restricted

iii. *Crispin* is the first district court case to apply the SCA to social media

iv. Takeaways

1. The SCA only applies to communications that are not readily accessible to the general public.
    a. *Facebook v. Superior Court (Hunter)*, the Supreme Court of California held that social media posts that were configured to be public fell within § 2702(b)(3)'s lawful consent exception, which allows ISPs to disclose a user's content with the user's consent
    b.

n. Recent examples

i. Homicide defendant denied access to the records of harassing online messages and death threats that he claimed had kept him in "constant fear for his life" in connection with self-defense argument

1. Opposition to Non-party Instagram Motion to Quash Subpoena Duces Tecum at 5, People v.[Redacted], No. [Redacted] (Cal. Super. Ct. Nov. 13, 2018) (on file with the Harvard Law School Library)

ii. Jewell v. Aaron's Inc.

1. 1700+ FLSA collective action in the Northern District of Georgia where class plaintiffs claimed that they were not paid for their 30-minute meal periods.

2. Aaron's asked a limited set of plaintiffs to produce: "All documents, statements, or any activity available that you posted on any internet Web site or Web page, including, but not limited to Facebook, MySpace, LinkedIn, Twitter, or a blog from 2009 to the present during your working hours at an Aaron's store."

3. To support its argument that the requested information was relevant, Aaron's produced a Facebook post from the named plaintiff ("Plaintiff Jewell") that stated that Plaintiff Jewell was taking a lunch break: "At workkkk…on lunch….ready to go home… work two hrs in am then offffff for the day." The date and time of the post was illegible on the printout Aaron's received, and Aaron's argued the date/time stamp should be legible "if provided by Plaintiff."

4. Aaron's also argued that other postings showed employees making personal posts on social media, i.e., taking breaks from work

5. Plaintiffs argued that it would be unduly burdensome

6. The court sided with the plaintiffs

a. "Defendant has not made a sufficient predicate showing that the broad nature of material it seeks is reasonably calculated to lead to the discovery of admissible evidence….The court finds that the burden imposed on a class of plaintiffs to produce such an overly broad swath of documents, while technologically feasible, is far outweighed by the remote relevance of the information."

iii. Murder defendant in Washington, D.C. was denied access to impeachment material from a key prosecution witness's social media accounts, despite the trial judge's finding that the evidence was relevant, material, and necessary to vindicate his "fundamental constitutional rights."
   1. Brief for the United States at 3, *Facebook, Inc. v. Wint*, 199 A.3d 625 (D.C. 2019) (No. 18-SS-958)

iv. Iraqi refugee accused of terrorism denied access to Facebook and Twitter posts that he argued may have helped exonerate him
   1. Ben Taub, The Fight to Save an Innocent Refugee from Almost Certain Death, New Yorker (Jan. 20, 2020), https://www.newyorker.com/magazine/2020/01/27/the-fight-to-save-an-innocent-refugee-from-almost-certain-death [https://perma.cc/53Y7-WVHN].

V. <u>Getting Evidence In – Relevant and Authenticated</u>

a. Fed. R. Evid. 402
   i. Relevant evidence is admissible unless otherwise provided and irrelevant evidence is not admissible

b. Fed. R. Evid. 401(a)
   i. Does the evidence have any tendency to make a fact more or less probable than it would be without the evidence?

c. Fed. R. Evid. 901(a)
   i. the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

d. A court needs to find that sufficient evidence is present for the jury to conclude that the evidence is what the proponent of the evidence claims. *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) (citations omitted)

e. Two step process
   i. Satisfactory foundation
   ii. Jury determines if the evidence is authentic

f. Two approaches have developed
   i. The Maryland Approach
      1. Courts are skeptical of social media evidence, finding the odds too great that someone other than the alleged author was the actual creator
      2. Proponent must either
         a. Ask the purported creator if he or she created the profile or post,

b. Search the internet history or hard drive of the purported creator's computer to determine whether that computer was used to originate the profile/post, or
c. Obtain information directly from the social networking website 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

3. Exemplified by Maryland Court of Appeals decision in *Griffin v. State*. 19 A.3d 415 (Md. App. 2011)
    a. Defendant was charged with 2nd degree murder, first degree assault, and use of a handgun in the commission of a felony
    b. The State offered printouts from a Myspace profile belonging to the defendant's girlfriend to demonstrate that the defendant had allegedly threatened one of the state's witnesses
        i. The page contained the statement "FREE BOOZY [the nickname for the defendant]!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"
        ii. The printout described details of the profile owner's life such as a birthday of October 2, 1983 and the location of Port Deposit. A photo of the defendant and his girlfriend was included
    c. Rather than using the defendant to authenticate the pages, the State attempted to use an investigator's testimony
    d. The lead investigator for the case downloaded the information from Myspace.
    e. He testified that he knew it was the defendant's girlfriend's profile due to the photograph of defendant and her, a reference to their children, and her date of birth listed on the printout.
    f. Defense counsel objected that the state could not establish a "connection" between the girlfriend and the social media page.
    g. The printouts were admitted and the defendant was convicted
    h. The defendant appealed, asserting that the printouts were not properly authenticated
    i. The Maryland Court of Special Appeals upheld the
    j. After another appeal request, the Maryland Court of Appeals accepted the case
    k. The court stated that the potential for "fabricating or tampering with electronically stored information on a

social networking site" posed "significant challenges" for authentication

l. The court confirmed that Rule 901 governed and noted that "distinctive characteristics" can be offered as circumstantial evidence for authentication
m. But, the court reversed and remanded, holding that the birthdate, location, reference to the defendant's nickname, and a photograph of the couple were not sufficiently distinctive characteristics to authenticate the printout.
    i. The court specifically noted its concern that someone other than the alleged author may have accessed the account and posted the message in question

4. *State v. Eleck*, 23 A.3d 818, 819 (Conn. App. Ct. 2011)
    a. Defendant appealed a conviction of first degree assault by means of a dangerous instrument
    b. Defendant claimed on appeal that the trial court improperly excluded evidence that had been properly authenticated
    c. Defendant had offered printouts of Facebook messages allegedly received from a State witness who was at the party where the altercation occurred.
    d. The defendant personally testified as to the authenticity of the printouts, stating that the username belonged to the witness, the profile had photos of the witness, and that he had downloaded and printed the messages himself
    e. The State's witness admitted that the profile was hers, but claimed that her account had been hacked and she had not sent the messages at issue
    f. The appellate court affirmed the trial court's decision not to admit the evidence, holding that even unique usernames and passwords are not enough to eliminate the possibility of hackers.
    g. The court reasoned that the messages themselves did not reflect distinct information that only the witness would have possessed regarding the defendant or the character of their relationship

ii. The Texas Approach
    1. More lenient in determining the amount of evidence that a reasonable juror would need to be persuaded that the alleged creator did in fact create the evidence
    2. The burden of production transfers to the objecting party to demonstrate that the evidence was created or manipulated by a third party
    3. *Tienda v. State*, 358 S.W.3d at 634

a. After being convicted of murder, defendant appealed and claimed that the trial court should not have admitted evidence from Myspace pages alleged to be managed by the defendant.
b. The Fifth Circuit upheld the conviction
c. The victim was traveling home from a nightclub when his car came under gunfire from a caravan of three or four cars on the same road
d. The defendant was a passenger in one of the caravan's cars
e. The Court admitted several Myspace accounts into evidence that allegedly belonged to the defendant.
f. Each account was linked to emails addresses including the defendant's name or nickname, had a profile name matching either Tienda's name or nickname, listed the defendant's hometown as the location, and contained photographs of a person who resembled the defendant
g. The accounts had posts with statements including "You aint BLASTIN You aint Lastin" and "EVERYONE WUZ BUSTIN AND THEY ONLY TOLD ON ME."
h. The Court considered *Griffin* (the Maryland approach) and determined that the evidence here had more indicia of authenticity as a whole
i. The court deemed the evidence sufficient for a reasonable jury to believe that the defendant created and maintained the profiles

4. *People v. Clevenstine*, 891 N.Y.D.2d 511 (N.Y. App. Div. 2009)
    a. Defendant was convicted on multiple sexual charges
    b. The victims testified that the defendant had messaged them through social media sites
    c. The legal compliance offer from Facebook testified that the messages originated from the purported accounts belonging to the defendant
    d. The defendant's wife testified that she had seen the same sexually explicit messages on her husband's Myspace account on their home computer
    e. The Court recognized the possibility that someone else had accessed the social media accounts, but said that the likelihood of such a scenario was a factual issue for the jury to consider

iii. Comparing the approaches
1. The textual difference is almost nonexistent
    a. Maryland Rule of Evid 5-901(a): "The requirement of authentication…is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

b. Texas Rule of Evid. 901(a): "To satisfy the requirement of authenticating…the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."
2. Both states agree on a "reasonable juror" test
3. But, the Maryland approach has a heightened burden – preponderance of the evidence
    a. And, it specifies three authentication approaches with their own challenges
4. Neither the heightened burden or specific paths to authentication are included in the Texas approach

g. Rule 901(b) – a non-exhaustive list that satisfies 901(a)
    i. For authenticating social media evidence, Rule 901(b)(1) and Rule 901(b)(4) are the most helpful.
    ii. Rule 901(b)(1) permits authentication through the "testimony [of a witness with knowledge] that [the evidence] is what it is claimed to be."
        1. For electronic evidence, the witness testifying may be the person who created the electronic document or maintains the evidence in its electronic form
        2. *See e.g. United States v. Barlow*, 568 F.3d 215, 220 (5th Cir. 2009) (holding that a chat log was properly authenticated by the testimony of a witness who participated in, and thus created, the chat).
        3. Recipients can also authenticate via testimony
            a. *See Talada v. City of Martinez*, 656 F. Supp. 2d 1147, 1158 (N.D. Cal. 2009) (holding that emails received were properly authenticated when the recipient provided a declaration asserting that the emails were true and correct copies).
            b. Example - an instant message was properly authenticated when "[t]he accomplice witness . . . testified to defendant's [instant messenger] screen name. People v. Pierre, 838 N.Y.S.2d 546, 548-49 (2007). "[Another witness] testified that she sent an instant message to that same screen name, and received a reply, the content of which made no sense unless it was sent by defendant [and] there was no evidence that anyone had a motive, or opportunity, to impersonate defendant by using his screen name." *Id.* at 549.

h. Rule 901(b)(4) – circumstantial evidence
    i. Permits a party to authenticate evidence using circumstantial evidence with "the appearance, contents, substance, internal patterns, or other distinctive characteristics of the [evidence], taken together with all the circumstances

i. *United States v. Vazquez-Soto*, 939 F.3d 365, 372 (1st Cir. 2019)

i. A USPS mail carrier with a history of back problems is found to be totally disabled and requiring retirement. For over a decade, Vazquez-Soto filed annual disability claims with supporting documents. In 2012, the USPS begins investigating him for possible fraud. Surveillance showed Vazquez-Soto carrying a large picture frame, riding a motorcycle and carrying a satchel, and generally walking around with ease.
ii. One of the investigating agents testified about photos he had downloaded from a Facebook page bearing the name of Vazquez-Soto's ex-wife Carmen Janica.
    1. The photos showed Vazquez-Soto traveling in Colombia, standing in a group of motorcycle riders next to a bike, seated on a motorcycle, entering a paddle boat, and dancing
    2. Janica did *not* testify at trial
iii. Defense counsel objected to the Facebook photos as not properly authenticated. On appeal, they argued that without Janica's testimony, the government failed to make a prima facie case that the social media evidence was in fact a posting on her Facebook page
iv. The First Circuit disagreed
    1. The account ownership is not relevant
        a. It did not matter whether it was actually Janica's page
    2. The authenticity of *the photographs* themselves is what matters
    3. Ordinary authentication rules apply
        a. Was there sufficient evidence for a reasonable factfinder to conclude that the photos were of Vazquez-Soto?
    4. The government's offer of testimony from the agent who downloaded the photos because he recognized Vazquez-Soto was enough for a reasonable fact-finder to conclude, along with their own examination of the photos compared to the man in the courtroom, that the photos showed Vazquez-Soto

j. *Parker v. State*, 85 A.3d 682 (Del. 2014)
    i.

VI. <u>Spoliation</u>

a. Standard
- **i.** Federal Rule of Civil Procedure 37(e)
    - **1.** 2015 amendment: ESI must be preserved in the anticipation or conduct of litigation
- **ii.** State
    - **1.** *Est. of Lester v. Allied Concrete Co.*, 736 S.E.2d 699 (2013), 285 Va. 295

a. Lester was driving his wife to work when the driver of a loaded concrete truck lost control of his vehicle. The wife ultimately passed away
b. Lester filed suit against the driver and his employer
c. After the lawsuit was filed, Lester sent an email to the attorney for Allied Concrete, which allowed the attorney to know which page was Lester's
d. Allied Concrete sent a discovery request for all pages of Lester's Facebook page, including all photos, messages, etc.
    i. Attached to the discovery request was a copy of a photograph the attorney downloaded off of Lester's Facebook account depicting Lester accompanied by other individuals, holding a beer can while wearing a T-shirt emblazoned with "I ♥ hot moms."
e. The next morning, counsel for Lester instructed his paralegal by email to tell Lester to "clean up" his Facebook page because "[w]e don't want any blow-ups of this stuff at trial."
f. Lester told the paralegal a short time later that he had deleted his Facebook page
g. Counsel responded to the pending discovery request with the answer, "I do not have a Facebook page on the date this is signed, April 15, 2009."
h. Allied filed a motion to compel
i. Lester eventually reactivated his Facebook page and his counsel was able to print copies of the page.
j. After that, Lester deleted 16 photos from his Facebook page.
k. In deposition, Lester testified that he never deactivated his Facebook page
l. Allied Concrete then sent a subpoena to Facebook to verify Lester's testimony
m. Allied hired an expert to determine how many pictures Lester deleted
n. The jury received an adverse-inference instruction, allowing them to conclude that the Facebook content that Lester deleted would have been damaging to his case
o. The trial court determined that Allied was entitled to sanctions and sanctioned Lester's attorney $542,000 and Lester for $180,000 for violating 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.

i. Lester's attorney was suspended from practicing law for five years for instructing Lester to obstruct access to evidence

p. The Supreme Court of Virginia affirmed

VII. Evidentiary Hurdles

a. Is it really being used as character evidence?
   i. Fed R. Evid. Rule 404
      1. Can get around it via a Rule 404(b) exception such as motive, intent, or identity
      2. But even then, be wary of Rule 403's prohibition on unduly prejudicial evidence
b. Hearsay
   i. Fed R. Evid. Rule 801(c)
   ii. Photographs and silent video mined from a social media account are generally not statements
      1. Though, consider that they *could* contain a statement
   iii. Social media statements are plainly out of court statements
   iv. Possible avenues around this:
      1. Not offered for their truth
         a. A statement may be offered to show that it was viewed to demonstrate notice or motive
      2. Admission by a party opponent
         a. Polk County School Board v. Coe, 2013 WL 3367400 (Fla. Div. Admin. Hrgs. 2013)
            i. Involved the termination of a Polk County School Board employee
            ii. The ALJ analyzed whether Facebook posts were properly admitted as admissions of a party opponent under Florida's Evidence Code
            iii. A witness testified that he did a public search of the employee on Facebook, identified the employee from photographs on the social media account, and viewed comments between the employee and another school employee
            iv. This circumstantial evidence was sufficient to establish that the employee posted the comments
            v. Accordingly, the postings fell under the admission of a party opponent exception to the hearsay rule
      3. Present sense impression (particularly for "live" tweeting, vloging, streaming, etc.)
      4. Excited utterance
      5. Then-existing mental, emotional, or physical condition
      6. Recorded recollection
c. Whatever happened to the best evidence rule?

i. Federal Rule of Evidence 1002, provides that an original writing, recording, or photograph is required to prove the contents of the document.
ii. FRE 1001(d) was drafted to provide clarification for how ESI was to be treated under the Best Evidence Rule: "For electronically stored information, 'original' means any printout — or other output readable by sight — if it accurately reflects the information."
    1. For most forms of ESI, including electronic documents, emails, digital photos, and video files, an exact copy of those items will suffice under the Best Evidence Rule
iii. But what about your screenshot of a party's social media post?
    1. A screenshot is necessarily a truncated image of a full native social media page
iv. *Edwards v. Junior State of America Foundation* (E.D. Texas April 23, 2021)
    1. Plaintiff had deleted his Facebook account, resulting in evidence being lost
    2. An eDiscovery expert submitted an affidavit stating that a tool was used to determine that evidence had been deleted
    3. The court imposed severe evidentiary sanctions on Plaintiff, including exclusion of evidence and adverse instructions
    4. Plaintiff had sought to offer screenshots as evidence of the Facebook content, instead of the deleted native files.
    5. The court held that the metadata and full content of the native files were essential to satisfy the best evidence rule
    6. The court ruled that the screenshots were not enough to accurately reflect the substance and context of the native file, because they couldn't show that the Facebook messages were authentic, nor could they be used to prove who had sent the messages in the screenshots
        a. "Here, the screenshots will not suffice as an "original" because the screenshots are not an "output" that "accurately" reflect the information. Only native files can ensure authenticity. Additionally, although the Best Evidence Rule allows for an original "photograph" to prove the contents of the photograph, this does not mean that the screenshot here can be used to prove that Harper sent the Facebook Messages contained in the screenshots."

VIII. <u>Ethical considerations</u>

a. ABA Model Rule 3.4
    i. a "lawyer shall not unlawfully obstruct another party's access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value."
    ii. But…
        1. Florida Bar Ethics Opinion 14-1 (June 25, 2015)

a. A lawyer may advise a client to use the highest level of privacy settings on the client's social media page. A lawyer may also advise the client pre-litigation to remove relevant information from the client's social media page so long as the removal does not violate any substantive law regarding preservation and/or spoliation and the information is preserved.

2. New York Ethics Opinion 745 (July 2, 2013)
    a. But provided that such removal does not violate substantive law regarding destruction or spoliation of evidence, there is no ethical bar to "taking down" such material from social media publications, or prohibiting the client's attorney from advising the client to do so, particularly inasmuch as the substance of the posting is generally preserved in cyberspace or on the user's computer.

b. ABA Model Rule 4.2
    i. attorneys and attorneys' agents are prohibited from requesting a connection to a represented party through social media networks. Accordingly, attorneys should avoid communicating with or contacting a represented party to access social media information.
    ii. Some social media platforms, such as LinkedIn, send an automatic message to accountholders informing them that their profile was viewed and by whom. Certain jurisdictions, such as New York, view such automatic messages as contacting the accountholder
c. ABA Model Rule 8.4
    i. an attorney violates ethical obligations when using deceptive tactics to gain access to a private account. An attorney may request permission to review an unrepresented person's private social media information, but cannot engage in dishonest or deceptive conduct to do so.

IX. **<u>Privacy Implications</u>**
a. Where do you have a reasonable expectation of privacy on the internet?
    i. Fourth Amendment
        1. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…
        2. "Reasonable expectation of privacy" test
            a. *Katz v. United States*, 389 U.S. 347
                i. Convicted for transmitting gambling information over the phone
                ii. Government attached an eavesdropping device outside the public phone booth
                iii. Court ruled that the use of the device without a warrant violated the Fourth Amendment

iv. The Fourth Amendment "protects people, not places"
    1. Marked a dramatic shift from previous rulings that had focused on the concepts of property and trespass
    2. Katz had plainly sought to keep the conversation private – as demonstrated by shutting the door behind him
v. "Reasonable expectation of privacy" – from Justice Harlan's concurrence
    1. First, that a person has exhibited an actual (subjective) expectation of privacy, and second
    2. That the expectation be one that society is prepared to recognize as reasonable

3. *United States v. Jones*, 565 U.S. 400 (2012)
    a. The Court stepped away from the *Katz* standard
    b. Authorities obtained a warrant allowing them to place a GPS tracking device underneath Jones' vehicle, as he was under suspicion of narcotics trafficking
    c. But, they did the installation after the deadline stated on the warrant
    d. Using the data, the government obtained an indictment against the accused
    e. The Supreme Court held that the installation qualified as a search, but the Court used the trespass doctrine from the 1928 case *Olmstead v. United States*

ii. The Electronic Communications Privacy Act
    1. Governs prohibits on the interception of electronic communications
    2. Prohibitions relate to "any wire, radio, electromagnetic, photo-optical, or photo-electronic facilities for the transmission of wire or electronic communications."
    3. Granted protection to previously unprotected communications, but probably still leaves a lot to be desired in society today

iii. *United States v. Meregildo*, 883 F. Supp. 2d 523 (S.D.N.Y. 2012)
    1. Defendant wanted to suppress evidence that the government obtained from his Facebook account as violating his Fourth Amendment rights
    2. The government accessed this information from his Facebook friend, who cooperated with law enforcement
    3. The court denied the defendant's motion to suppress
    4. The court emphasized the privacy settings used by the defendant on the account, which allowed the Facebook

friend to see the messages that the defendant posted to his account
5. Accordingly, there was no expectation of privacy in the posts

iv. *Sines v. Kessler*, 2020 U.S. Dist. LEXIS 223168 (W.D.Va Nov. 30, 2020)
1. Federal district court examined the scope of permissible social media discovery
2. Arose of the violence that occurred at rallies in Charlottesville, Virginia in August 2017.
3. Court had ordered each of the defendants to produce "complete and accurate credentials or consent to access any social media accounts within the [d]efendant's control that might contain any discoverable information."

v. Florida's courts have held that "Facebook itself does not guarantee privacy. By creating a Facebook account, a user acknowledges that her personal information would be shared with others. 'Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist.'" *Nucci v. Target Corp*., 162 So. 3d 146, 154 (Fla. 4th DCA 2015) (*quoting Romano v. Steelcase, Inc*., 30 Misc. 3d 426, 907 N.Y.S.2d 650, 656-7 (N.Y. Sup. Ct. 2010)).

b. In September 2023, the U.S. Supreme Court agreed to decide whether Florida and Texas may prohibit large social media companies from removing posts based on the views they express
i. *Moody v. NetChoice*, No 22-277
ii. *NetChoice v. Paxton*, No. 22-555
iii. Not only important for the First Amendment, but also for access to social media evidence
iv. Consider: If we view social media platforms as treasure troves of evidence regarding a person's physical health, mental well-being, location, activity in their communities, how that information is regulated is an important consideration for us as litigators
v.

X. **<u>Deepfakes</u>**

a. Combining concerns over privacy, social media authentication, and the reality that our current legislative and judicial frameworks are probably not equipped for the world ahead
b. What is a deepfake?
i. Media that has been digitally manipulated to replace a person's likeness with that of another, or to make it appear that a person is doing something or saying something that they did not actually do or say
ii. While altering videos and images is not new, deepfakes take it an additional step further by using machine learning and artificial intelligence to create the content
c. Video, images, and even audio
i. In 2019, a UK-based energy firm's CEO was scammed by phone when he was ordered to transfer a large sum of money into a

Hungarian bank account by deepfaked audio made to sound like the voice of the firm's parent company's chief executive (https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=3d34ad4e2241)

XI. **Practical tips**

a. Send the preservation letter ASAP, even if you don't believe that social media evidence will come into play in your case
    i. The odds are, someone in your case is using a social media platform regularly. You never know who it is, or what they're posting, unless you work to get that preserved and find out
    ii. Address preservation issues at your Rule 26(f) meetings
b. Search yourself, early and often
    i. Save what you can with as much indicia of reliability as you can grab, including date of the post, account name, account photos (even beyond the profile photo)
c. Draft a memo to your file about where you find the information, when you printed it, what URL you used, what search terms did you use, and whether you clicked through any groups or other accounts to get to where you found useful information
d. If you've got it, use it
    i. You can get ahead on getting your evidence admitted at trial by locking someone into authenticating their account information or the posts themselves at deposition
        1. And if they try to say it isn't their post or their page, you've then got time to investigate that before trial
e. Subpoenas are unlikely to be a powerful tool in your arsenal, so think creatively
f. Narrowly tailor all discovery requests
    i. For a personal injury case, ask for copies of any posts or statements made about the incident, the treatment, the injuries, etc.
    ii. Ask for posts/statements/photos/etc. that show the party's mental state, physical activity, travel, exercise, etc. Be specific.
    iii. Limit the time period.
        1. Don't ask for all posts, photos or videos showing plaintiff competing in a running race
        2. Ask for any social media posts, comments, photos from the day after the accident to the present that show Plaintiff engaging in running races
g. Use an internet archive page to see if you can uncover evidence that plaintiff has "cleaned up"
    i. The Wayback Machine – The Internet Archive is a website that provides access to a digital library of archived web pages
        1. Florida courts appear reluctant to introduce Wayback Machine documentary evidence without proper testimony explaining how the machine works. For example, in St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, 2006 WL 1320242 (M.D. Fla. May 12, 2006), the plaintiff attempted to offer

printouts from the Internet Archive website to prove how two other websites looked at various times in the past.29 The U.S. District Court for the Middle District of Florida ruled that the plaintiff would need to present evidence from an Internet Archive official with personal knowledge of how the archive worked.

h.