

**SOCIAL MEDIA EVIDENCE  
IDENTIFICATION, RETRIEVAL, AUTHENTICATION AND  
PRESENTATION**

*Christina S. Tillinger  
Krieger & Tillinger, P.C.  
Christina@krieger-tillinger.com*

I. Identification - Variations of Social Media Commonly Used

- A. Facebook
- B. Instagram
- C. Snapchat
- D. Twitter
- E. WhatsApp

II. Discoverability

- A. What is Discoverable? TRCP 192.3 - Discovery is permissible if it pertains to relevant evidence or may lead to the discovery of admissible evidence. This rule has been interpreted to include electronic evidence. *In Re Weekly Homes, L.P.*, 295 S.W. 3d 309, 322 (Tex. 2009). Like with all discovery, the TRCP prohibit litigants from going on “fishing expeditions”, and find that discovery requests, including those for social media, must be reasonably tailored to include matters relevant to the case at hand.

II. General Methods of Obtaining Social Media Information, Posts, and Messages

There are several general ways to retrieve social media information, posts and messages.

- A. Public Domain - Often the attorney, the client, or the attorney’s staff can simply go on to social media and gather information (posts, pictures, videos, etc.) Often times, this is a good starting point for gathering evidence, and will give the attorney a guideline on what deeper digging needs to be done. The attorney can Google the subject’s name to see a list of which social media sites are being used by the subject, or go to each individual site - Facebook, Snapchat, Instagram - to find a specific subject’s profile. Social media postings and communications are freely discoverable without court order when the subject’s account is public. *Fawcett v. Altieri*, 38 Misc. 3d 1022, 960 N.Y.S.2d 592,290 Ed. Law Rep. 227 (Sup 2013).

- B. Traditional Discovery Tools and Procedures - If the subject's social media page is not public, then traditional discovery may be the way to go. Interrogatories can be used to request the identification of any screen names, identities, passwords, etc. to "any social media site" or to "Facebook, Instagram, etc.". It is a good idea to have a standard social media injunction interrogatory or interrogatories to include in your discovery requests in cases where such information would be helpful - i.e. most family law cases.

Here is an example of a discovery requests used to obtain social media information and content:

Request for Production No. 1: A copy of your social media (e.g., Facebook, Instagram, Snapchat, etc.) data that depicts, discusses, or references any of the following: the child; your relationship with the other parent; your relationship with your child; your possession or access to the child; conservatorship of the child; the parties' ability to care for the child; the parties' parenting styles; child support or health insurance for the child; this lawsuit; your consumption of alcohol; your consumption of controlled substances; or your nightlife activities.

- C. Forensic Examination- A third way of retrieving social media information is through forensic examination. In rare circumstances, a court can order a forensic exam of a party's computer to search for hidden and/or deleted data. However, this is rarely granted, and usually comes only after a court has determined that the attorney has tried less invasive and far-reaching means to obtain the desired data.
- D. Subpoena - This is probably the least productive means to obtain content from social media. Besides the problem of figuring out to whom exactly to send the subpoena, and whether or not that can even be done (distance, etc.), sites such as Facebook and Twitter have their own policies and procedures for obtaining data from their sites. For example, Facebook cites the "Stored Communication Act" on their site, which prohibits any disclosure by Facebook of user content. Facebook directs litigants and counsel to produce and authenticate the site content of their own accounts by downloading the information themselves.

### III. "How-To's" In Collecting Social Media Material for Production and Use

Unlike collecting email and text messages, social media content usually includes text, pictures, memes, videos, and a variety of other mediums. This information is usually stored in "the cloud".

How to's:

A. Facebook - The Facebook user can take the following steps:

1. Click the down arrow at the top right of the Facebook page and select "Settings".
2. Click "Download a Copy of your Facebook Data" below your "General Account Settings".
3. Click "Start My Archive".

B. Twitter - The Twitter user can take the following steps:

1. Go to "Account Settings" by clicking on the profile icon at the top right of the page, and select "Settings and Privacy" from the drop-down.
2. Click the "Request Your Archive" tab next to "Your Twitter Archive".
3. Once the download is ready, Twitter will send a notice through a push notification. The user shall then go to "Settings" and click "Download Archive" under "Download Your Data".
4. Twitter will send an email to the user with a download link to the Twitter user's email account.
5. When the user gets the email, the user can click the "Download" button while logged in to his/her Twitter account and download a zip file of the Twitter archive.

C. Instagram - The Instagram user can take the following steps:

1. Log into Instagram and go to "Account Settings". Choose "Privacy and Security".
2. User enters his/her email address into the box that pops up with the title "Get a Copy of What You've Shared on Instagram".
3. Instagram will email a link to download a file with the comments, photos, profile information, and more. This can take up to forty-eight hours.

#### IV. Presentation and Admissibility of Social Media Information and Documentation in Court

The same standards that govern other forms of evidence govern social media evidence, meaning that the evidence must be relevant, authenticated, and cannot be hearsay.

A. Relevance - As with other types of evidence, the social media content sought to be used must make the existence of any material fact more or less probable than it would be without the evidence, and the probative value must outweigh the prejudicial effect.

B. Authentication -

1. Produced by Opposing Party/Social Media User. Texas Rule of Civil Procedure 193.7 applies to social media content, and provides that the easiest way to authenticate information from social media sites is to receive the content from the opposing party through discovery - the opposing party being the social media participant, obviously. TRCP 193.7 provides that “a party’s production of a document in response to written discovery authenticates the document for the use against that party in any pretrial proceeding or trial, unless.....” (withdrawal language). Therefore, if you request the social media content in discovery, and it is produced, it is authenticated and usable.
2. Authentication Through Witness or Party. First, an attorney can send Requests for Admissions and Interrogatories to authenticate social media evidence. Second, a party can be deposed and asked to authenticate the social media discovery. Third, the attorney can “prove up” the evidence in trial just as he/she would do a picture or a letter or an email, by laying a foundation that the information accurately reflects the actual information obtained. This works as to individual bits of social media evidence, such as a posting in the user’s words, or a picture the user posted.
3. Caselaw Regarding Authentication. Most of the law covering authentication fo social media comes from criminal cases. In *Derring v. State*, the Court stated, “Facebook presents a (sic) authentication concern that is twofold. First, because anyone can establish a fictitious profile under any name, the person viewing the profile has no way of knowing whether the profile is legitimate. Second, because a person may gain access to another person’s account by obtaining the user’s name and password, the person viewing the profile cannot be certain that the author is in fact the profile owner. Thus the fact that an electronic communication on its face purports to originate from a certain person’s social networking account is generally insufficient, standing alone, to authenticate that person as the author of the communication. *Derring v. State S.W. 3d 668, 671 (Tex. App. - Eastland 2018)*.”

Some Texas courts have allowed circumstantial evidence to be used where the alleged author does not testify. See *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012), where the trial court admitted posts from what was purported to be Defendant's MySpace page. The court of criminal appeals held that there was sufficient circumstantial evidence of authenticity to admit the posts - the page was registered to a person with Defendant's nickname, photographs on the profile were of Defendant, the profile referenced Defendant's arrest, the murder allegedly committed by the Defendant, and even the Defendant's ankle monitor.

- C. Hearsay. Exceptions to the general hearsay rule may also apply to social media. Concepts such as present sense impression, excited utterance, recorded recollection, public records and certain regular records could be relevant considerations. For example, a party could introduce his/her own prior social media posts as proof of prior consistent statements against interest, or admissions by party opponents. Social media posts can also be used to refresh a witness' memory.

Of course, just as with all hearsay, if the statement from social media that is being offered is not being offered to prove the truth of the matter asserted, it is not hearsay. Therefore, the attorney must clearly articulate the purpose of the content offered and the evidentiary basis for admissibility.

It goes without saying, then, that just like the hearsay rules must be reviewed to get social media posts are, they need to be reviewed by the other side to keep them out.

## V. Ethical Considerations in Social Media Evidence

- A. False Friending - Many social media users maintain privacy settings that block strangers from viewing their posts and pictures, and require that the potential "friend" be accepted by the owner of the social media account. Texas courts have found that it is a violation of Rule 4.02 of the Texas Disciplinary Rules of Professional Conduct for an attorney to send a "friend" or "follow" request to an opposing party when the attorney knows that the opposing party is represented by counsel. If the opposing party is not represented by counsel, there is no prohibition against the attorney "friending" the opposing party; however TDRPC 4.01(a) prohibits attorneys from making a "false statement of fact or law" to a third person. Therefore, attorneys are prevented from pretending to be someone other than who they are to "friend" this opposing party. These same rules, of course, apply to the attorney's friends, family, and staff.

- B. Privacy Right Expectations - What expectation of privacy does a person on social media have? Courts have recognized that social media sites are not privileged, and that they are not protected by any right to privacy. Courts are pointing out the difference between “private” and “not public”. Following this thought, when a person posts content on social media, whether to a large group or a smaller, restricted group, the poster has no reasonable expectation of privacy. Even content posted to a small group can be copied, shared, and reposted from that point forward - there is nothing the original poster can do to prevent that; hence, there is no reasonable expectation of privacy. Clients should be advised that regardless of their personal expectation of privacy as determined by their privacy settings, the content of their social media accounts may be fair game to the other side. It is good practice to advise your client to use the highest of privacy settings; however, they should still be instructed that this may not fully protect them.

A few cases pertaining to Social Media and privacy:

1. *McMillen v. Hummingbird Speedway, Inc.*, 2010 WL 4403285 (Pa. C.P. 2010) - Users of Facebook are put on notice by Facebook’s terms and privacy policies that regardless of the user’s subject intentions when sharing information, their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook itself.
2. *EEOC v. Simply Storage Management, LLC*, 270 F.R.D. 430, 110 Fair Empl. Prac. Cas. (BNA) 49 (S.D.Ind. 2010) - Content from a social media site is not protected from discovery simply because the social media account is “locked”, or “private”, or that the social media site user has “decided” that only other users who has obtained his/her permission may view the profile or site or content.
3. *R.S. ex. rel. S.S. c. Minnewaska Area School District No. 2149*, 894 F. Supp. 2<sup>nd</sup> 1128, 290 Ed. Law Rep 711 (D Minn. 2012) - Here, the court did rule that “private messages” sent through Facebook operate as email does, in that they are sent from one user to another directly, and not open to perusal even by “friends” of either party. Therefore, there is a reasonable expectation of privacy to private messages.
4. *Largent v. Reed*, No. 2009-1823 (Pa.C.C.P. Nov 8, 2011) - The court ordered the Plaintiff to turn over her Facebook login information to counsel for Defendant within 14 days, and gave counsel for Defendant 21 days to “inspect Plaintiff’s profile”. With that login information, counsel for Defendant could view Plaintiff’s posting, settings, friend list, groups to which she belongs, and even “private” messages.

5. *In re Indeco Sales, Inc. No. 09-14-00405-CV.2-14, WI. 5490943 at \*4 (Tex.App.-Beaumont Oct. 30, 2014, orig. proceeding) (mem. op.)* Court of appeals held that the trial court did not abuse its discretion by granting a Plaintiff's motion for protection as to discovery requests seeking "all posts or messages Plaintiff sent or received on her Facebook page, regardless of topic, all information, data, posts, and conversations from her Facebook page, and every photograph posted since the accident, regardless of when the photograph was taken."

## VI. Random Additional Thoughts

- A. Statistics - Here are some helpful statistics regarding social media use:

- \*1.52 billion people log in to Facebook daily and are considered to be active Facebook users.

- \*Ages 25-34 represent almost 30% of all Facebook users

- \*5 new Facebook profiles are created every second

- \*76% of Facebook users are female

- B. Advertising

- \*Facebook pages

- \*Local interest groups

- C. Lawyer Groups

- \*TFL - Texas Family Lawyers

- \*Texas Family Lawyers

- \*Texas Lawyers

- \*Galveston, Harris and Montgomery County Lawyers

- \*Texas Paralegals

- \*Houston Lawyers

- \*Houston Mediation Connection

## VII. Additional Resources

- A. Melinda Barlow, *Social Media and Your Case: From Pleadings to Closing*, State Bar of Texas: Texas Perspective on E-Discovery, (2013).
- B. John G. Browning and Kendyl Hanks, *Social Media, Discovery, and Ethics*, 35<sup>th</sup> Annual Litigation Update Institute, (January 2019).
- C. Michael Cowen, *Social Media: How to Get Information and Get it Into Evidence*, 31<sup>st</sup> Annual Advanced Evidence and Discovery (2018).
- D. Shawn Thompson, *Social Media Discovery and Admissibility*, State Bar of Texas: Advanced Evidence and Discovery (April 2019).

- E. Joseph Indelicato, Jr. And Katherine Hamilton and Nina Indelicato, Of Counsel, Underutilized Discovery Methods and Discovery to Third Parties, State Bar of Texas: 43<sup>rd</sup> Annual Advanced Family Law Course (2017).
- F. Hon. Emily A. Miskel and Britney Elaine Harrison, *E-Discovery: Spinning ESI Straw into Discovery Gold*, State Bar of Texas: 44<sup>th</sup> Annual Advanced Family Law Course (2018).