Bench-Bar Conference

October 25, 2018

State and Federal Civil Practice

10:45 a.m. - 12:15 p.m.

"Social Media and the Law: Obtaining Information & Admitting It Into Evidence"

Panelists:

Hon. Tanya Bullock
Virginia Beach Juvenile & Domestic Relations District Court

Ryan T. Walker
Marks & Harrison

Laura Lee Miller
Harman Claytor Corrigan & Wellman, P.C.

Moderator:

Hon. John A. Gibney, Jr.
United States District Court for the Eastern District of Virginia, Richmond Division

Materials for Civil Breakout Session

10:45 a.m. - 12:15 p.m.

"Social Media and the Law: Obtaining Information & Admitting It Into Evidence"

"Social Media and the Law: Obtaining Information & Admitting it into Evidence"
prepared by
Hon. Tanya Bullock of the Virginia Beach Juvenile & Domestic Relations District Court, Ryan T. Walker of Marks & Harrison and Laura Lee Miller of Harman Claytor Corrigan & Wellman, P.C.
compiled by
Veronica Brown-Moseley of the Boleman Law Firm, P.C.

Social Media and the Law: Obtaining Information & Admitting it into Evidence

Hon. Tanya Bullock
Laura Lee Miller
Ryan T. Walker

I. Introduction

a. Various types of computers
   i. Cell phone, smart phone, Ipad, Tablet, GPS, Wii, Nintendo, DS, Xbox, Playstation, Fitness Tracker
b. Social Networking
   i. Commercial internet sites that provide subscribers server space to create a mini-website to which they control access
c. Social Media
   i. Forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content -- (Webster's Dictionary)
   ii. Social Networks- Facebook, Twitter, Foursquare, LinkedIn, Pinterest
   iii. Photo Sharing- Flickr, Instagram
   iv. U-Tube
d. Various texting Apps
   i. Text Now, Fake Text Message, Anonymous Text, What's App, Whisper, Snapchat, Cyber Dust, Kik, Text 4 Free, Many, many more
e. Video-Chat
   i. FaceTime, Skype, Tango, Text'em, Periscope
f. Digital Evidence
   i. Information that has probative value to an issue in the case, that is stored or transmitted in binary form (computer language) and may be relied on in court
   ii. Sometimes referred to as electronically stored information (ESI)
g. Two Types of Digital Evidence
   i. User-created digital evidence
   ii. Computer/Network-created digital evidence
h. User-created digital evidence
   i. Text (email, documents, chats), address books, bookmarks, databases, images, video and sound files, web pages
i. Computer/Network-created digital evidence includes
   i. Email headers, metadata, activity logs, browser cache, history, and cookies, backup registry files, configuration files, swap files
j. Inside the Box vs. Outside the Box
   i. Inside the Box- Computer owner has possession of the Information

1. Computer's hard drive and other memory, CDs and USB drives, iPods, Cell Phones, External Hard Drives

ii. Outside the Box- Computer owner does not have possession/not stored on owner's computer

1. Online email accounts (Gmail and Yahoo), internet shopping accounts, social networking accounts, backups of text messages, cell site location data, subscriber account records, contents of website

k. Computer Forensics

i. Process of acquiring, preserving, analyzing and presenting digital evidence for use in investigations and court proceedings

l. Acquisition Process

i. Make no changes to the media being examined during the process of collecting evidence

ii. Collection should be done in a manner that establishes a verifiable chain of custody, over the data, preserves data integrity and allows tracing of particular files or evidentiary items back to the original source

iii. Process should preserve the collected information and copies made of it, in it original form

II. Obtaining Information from Social Media

a. Begin searching as soon as you receive notice of the claim or lawsuit

i. Most websites have privacy settings that enable the user to limit access to "friends" only, but a surprising number of people maintain open or public pages

ii. Review and document websites early before a party realizes they need to "go private"

iii. Recheck websites frequently, as the content may change often

iv. Advise your client to not share information on social networking sites

v. Some sites, like LinkedIn, may tell the person that you have visited their page

b. Search not only the party involved, but their circle of social media "friends"

i. You may be able to "back door" your way into information regarding the party you are searching for

c. Discovery Requests

i. Generally, Courts will allow discovery of material posted on social networking sites if it is relevant to the litigation and the discovery request is narrowly tailored.

ii. Generally, to obtain access to private material, most courts require a threshold showing that the material is likely to contain information relevant to the lawsuit.

1. *James v. Edwards*, 85 Va. Cir. 139, 142, 2012 Va. Cir. LEXIS 183 (Greensville Cir. Ct., 2012) (party seeking discovery of plaintiff's social networking or social media activity that is not readily available to public access "must establish a 'factual predicate' with respect to the relevancy of the evidence," citing and applying *McCann v. Harleysville Ins. Co.*, 78 A.D.3d 1524, 1525, 910 N.Y.S.2d 614 (App. Div. 2010).

iii. It is suggested that your discovery request be narrowly tailored, so that the request is more likely to be granted

1. *Crabtree v. Angie's List, Inc.*, 2017 U.S. Dist. LEXIS 12927 *12 (S.D. Ind. 2017) (in seeking discovery of plaintiff's social media posts, e-mails, text messages, blog or website posts "prepared, created, obtained, or used by" plaintiff for a one year period, "[d]efendant cats too wide a net as it does not sufficiently justify the breadth of the request" and it "has not shown how e-mails, text messages or social media posts from this one year time period may be more probative as to these issues than other less intrusive data already within its control.")
2. *Thompson v.* Autoliv ASP, Inc., 2012 U.S. Dist. LEXIS 85143 at *13 (D. Nev. June 20, 2012) (limiting defendant's discovery requests regarding plaintiff's social network sites to material relevant to the litigation about her injuries and ordering in camera inspection of information produced, along with an index of redacted material, the court recognizing that "litigation does not permit a complete and open public display of Plaintiff's life.")
3. *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012) (denying motion to compel entire contents and access to plaintiff's Facebook account, the court noting that "the Defendant does not have a generalized right to rummage at will through information that Plaintiff has limited from public view. Rather, . . . there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence. Otherwise, the Defendant would be allowed to engage in the proverbial fishing expedition, in the hope that there might be something of relevance in Plaintiff's Facebook account."
4. *Scott v. United States Postal Service*, 2016 U.S. Dist. LEXIS 178702 at *13-14 (M.D. La. 2016) ("[t]he Court also finds that the Request for Production is overly broad to the extent that it seeks all social media postings 'related to any type of physical or athletic

activities from June 6, 2014, to present. . .' The Court will therefore limit the Request for Production to all of Plaintiff's social media postings, including photographs, since the June 6, 2014 accident that: (1) refer or relate to the physical injuries Plaintiff alleges she sustained as a result of the accident and any treatment she received therefore; or (2) reflect physical capabilities that are inconsistent with the injuries that Plaintiff allegedly suffered as a result of the accident."

iv. Davenport v. State Farm, 2012 U.S. Dist. LEXIS 20944 (M.D. FL. 2012) (ordered plaintiff to produce any photographs of her taken since the date of the accident and posted to social networking site).

v. Chauvin v. State Farm, 2011 U.S. Dist. LEXIS 121600 (E.D. Mich. 2011) (denying request for production of plaintiff's Facebook account because there was "no indication that granting access . . . would be reasonably calculated to lead to the discovery of admissible information.").

vi. Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018 (D. Colo. 2009) (denying the plaintiff's request for a protective order regarding social media content).

vii. Barnes v. CUS Nashville, LLC, 2010 WL 2265668, *1 (M.D. Tenn. 2010) (magistrate judge offered to create a Facebook account to "friend" plaintiffs in order to review subpoenaed material).

d. Social Networking Sites' Position on Account Information Requests
   i. Google – "it's all content", "we only accept process from local Superior Court (Santa Clara County California) or federal courts."
   ii. Facebook – "it's all content and we don't comply with subpoenas in civil cases"
   iii. Twitter – only respond to law enforcement requests with a valid search warrant or court order, and they notify the user of the request before they turn over the information.

e. Privacy Rights
   i. ECPA – Electronic Communications Privacy Act (1986)
   ii. HIPPA
   iii. FERPA – Family Education Rights and Privacy Act
   iv. Stored Communications Act
   v. Wiretap Act
   vi. Many, many more.....

f. Expectation of Privacy
   i. There is no expectation of privacy on social networking sites.
   ii. There are disclaimers contained in the sites' "Terms of Use" Agreements

1. Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010) (ordered production of the plaintiff's entire Facebook and MySpace profiles, finding there was no expectation of privacy).

iii. But see, *Appler v. Mead Johnson & Co., LLC*, 2015 U.S. Dist. LEXIS 133769 (S.D. Ind., 2015) (the defendant requested the plaintiff's entire Facebook Profile and the court noted that "discovery of an entire Facebook Profile pits two competing ideas of privacy and discovery rights against each other.")

1. *Holly v. Dollar Tree Stores, Inc.*, 2013 U.S. Dist. LEXIS 38795 (M.D. TN., 2013) (court concluded that the defendant had not made the requisite showing for full access to plaintiff's *private* Facebook or other social media pages).

g. Sample Authorization to Release Electronic Communications

i. Pursuant to the Stored Communication Act, 18 U.S.C § 2701(c)(2), you are hereby authorized and directed to produce to [ATTORNEY NAME, FIRM, AND ADDRESS], or to any of his or her agents or representatives, any and all information in your possession regarding any [WEBSITE NAME] account(s) registered to [PLAINTIFF'S NAME] and/or [USERNAME AND URL], including but not limited to: any and all emails, messages, screenshots, Wall postings, Timeline postings, photographs, videos, notes or other electronic data or material, including attachments, sent to or from, or posted and displayed publicly or privately, from [DATE] to present.

h. Subpoenas

i. Facebook will generally deny subpoena requests, citing the Stored Communication Act ("SCA"), 18 U.S.C. § 2701 et seq.

ii. The SCA generally prohibits a "person or entity providing an electronic communication service to the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

iii. The SCA further prohibits a "person or entity providing remote computing service to the public" from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service." 18 U.S.C. § 2702(a)(2).

iv. Disclosure in violation of the SCA can expose the record holder to civil liability. Theofel v Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), cert denied, 125 S. Ct. 48 (2004).

v. Authorized disclosures under the SCA:

1. Incidental to the provision of the intended service;

2. Incidental to the protection of the rights or property of the service provider (Made with the consent of a party to the communication or, in some cases, the consent of the subscriber;
3. Related to child abuse;
4. Made to public agents or entities under certain conditions;
5. Related to wiretaps; and
6. Made in compliance with certain criminal or administrative subpoenas issued in compliance with federal procedures;

vi. The SCA does not include an exception for civil subpoenas

vii. Facebook's position is that the user, not Facebook, is obligated to produce his or her own content, citing Suzion Energy Ltd. v. Microsoft, 2011 WL 4537843 at *5 (9th Cir. 2011) ; Offenback v. L.M. Bowman, Inc., 2011 WL 2491371 at *3 m. 3 (M.D. Pa. 2011).

1. Facebook will not product any content (posts, photos, etc.). It is only required to provide basic subscriber information to a party in a civil matter if the information is indispensable to the case and not within the party's possession.
2. Facebook will not comply with out-of-state subpoenas.
3. Facebook will not produce the requested information even if you have a signed release from the plaintiff.
4. If the user cannot access the account because he or she is disabled or deleted the account, Facebook will, to the extent possible, provide "reasonably available data" to the user.
    a. Facebook will charge a fee ($150 - $500) for retrieval of a user's records.

III. Preserving Information

a. Send opposing counsel a preservation letter to prevent information from being deleted from social networking sites
b. In federal court, preservation issues can be addressed at Rule 26(f) meeting
c. Facebook Deactivation vs. Delete
    i. Facebook profiles are not usually "deleted," only deactivated. Even if a plaintiff elects to deactivate his or her profile, Facebook saves all profile information including friend lists, photographs, interests, etc. The user may reactivate the account at any time.
    ii. To permanently delete a Facebook account, the user must submit an official request to Facebook. Once this request is processed, the page is deleted with no option for recovery. (Use of Social Media in Litigation)
d. Telephone Service Provider Records
    i. Each provider keeps call detail records (CDR) of cell phone activity
        1. Detailed records of each call

2. Tower location information and call duration
3. Data transfer sizes and rates
4. GPS information
5. Need warrant or court order to obtain information

IV. Admitting Information into Evidence

a. Admissibility
   i. Lorraine v. Markel American Ins. Co., 241 F..R.D. 534 (D. Md. 2007)
   ii. In order for ESI to be admissible, the proponent admitting the digital evidence must
      1. Show the ESI is relevant
      2. Establish admissible facts to show that the item is authentic
      3. Deal with any hearsay
      4. Determine if the best evidence rule applies or meets and exception
      5. Argue that the probative value outweighs its prejudicial effect

b. Authenticity
   i. Social networking sites are NOT self-authenticating. They do not verify that you are you who say you are. You can create a fake account or manipulate a screenshot using Photoshop.
   ii. Forensic Examiner - Expert Witness
      1. They generally can rule out if the digital evidence has been altered, changed or deleted
      2. Note: Many devices will allow you to delete parts of a text message and leave the rest.
   iii. Witness personal knowledge
   iv. Distinctive characteristics
   v. Rules of Evidence[1]
      1. Federal Rule of Evidence 901(a) – "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."
      2. Federal Rule of Evidence 901(b)(4) – Use of distinctive characteristics – "The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances."
      3. Federal Rule of Evidence 104(b) – "When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist.

---

[1] For a comprehensive discussion regarding authentication of ESI and the Federal Rules of Evidence, please see Hon. Paul W. Grimm, et al., "Authentication of Social Media Evidence," *American Journal of Trial Advocacy*, 36 Am. J. Trial Advoc. 433 (2013).

The court may admit the proposed evidence on the condition that the proof be introduced later."

4. Virginia Rule of Evidence 901 - "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the thing in question is what its proponent claims

vi. Case Law
    1. Griffin v. State, 419 Md. 545 (2011) – Court of Appeals
        a. Holding: The proper means to authenticate printouts of postings on social media sites is as follows:
            i. Ask the purported creator if she indeed created the profile and also if she added the posting in question;
            ii. Search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question; and
            iii. 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.
            iv. See also: Commonwealth v. Wallick, Commonwealth v. Williams, People v. Beckley and State v. Eleck
    2. Tienda v. State, 358 S.W. 3d 633 (2012) – Texas Court of Appeals
        a. Holding: There were far more circumstantial indicia of authenticity in Tienda than in Griffin. There was 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.

vii. Questions to address when confronted with digital evidence
    1. How was the evidence collected?
    2. Where was the evidence collected?
    3. What types of evidence was collected?
    4. Who handled the evidence before it was collected?
    5. When was the evidence collected?

viii. Steps to Authenticate

1. Take a Screen Shot
    a. Hit "Print Screen" button, open a Word document or email, and then press CTRL-V to paste the screen image into the document or email
    b. Need time and date stamp
    c. May need someone to testify how and when the material was discovered and stored
2. Save a copy of the website using tools like HTTrack Website Copier – creates a local copy of the website that permits offline browsing
3. Have the party confirm the page or profile is his in a deposition
4. Have "friends" who interact with the page confirm that it is the party's page or profile
5. Identify any content or other factors that are unique to the person you believe authored the material
6. Send Requests for Admission before trial to confirm the authenticity
7. Consider the use of a computer forensic expert
8. Use of metadata – information showing how and when the material was created, accessed or modified

c. Best Evidence Rule
    i. To prove the content of a writing, the original writing is required, except as otherwise provided in these Rules, Rules of the Supreme Court of Virginia, or in a Virginia statute. (Va. Supreme Court Rule 2:1002)
    ii. Exceptions
        1. Originals lost or destroyed
        2. Original not obtainable
        3. Original in possession of opponent
        4. Collateral matters
    iii. Text Messages
        1. Dalton v. Commonwealth, 64 Va. App. 512 (2015)
            a. Holding: Text messages constitute writings which are subject to the best evidence rule.
    iv. Still Images and Video Recordings
        1. Midkiff v. Commonwealth, 280 Va. 216 (2010)
        2. The Virginia Supreme Court held that the Best Evidence Rule does NOT apply to still images and video recordings. So pictures are not subject to the rule or other digital evidence, only writings.

d. Hearsay

i. Computer generated data is generally NOT hearsay because hearsay is a statement offered by a "declarant". A declarant is defined as a person. - Virginia Rules of Evidence 2:801

V. Important Ethical Considerations

a. Rule 4.2 of the Rules of Professional Conduct:
   i. In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized by law to do so.
      1. Do not send a Facebook friend request to an adverse party. This constitutes an indirect ex parte communication with a represented party.
      2. Do not create a "fake" account to send the party a friend request. Do not use any deceptive practices in obtaining information through social networking sites.
      3. Do not direct someone else to submit a Facebook friend request to the plaintiff for you.
         a. You may obtain information concerning the plaintiff's Facebook page through an existing Facebook friend.
         b. You cannot friend someone that is a "friend" of the party under false pretenses.

b. Rule 3.4(a) of the Rules of Professional Conduct:
   i. A lawyer shall not: (a) obstruct another party's access to evidence or alter, destroy or conceal a document or other material having potential evidentiary value for the purpose of obstructing a party's access to evidence. A lawyer shall not counsel or assist another person to do any such act.
      1. Do not direct your client to delete incriminating posts or photos. You may suggest that your client activate the privacy settings his or her account, but you and your client still have an obligation to preserve and produce the material if it is relevant or reasonably calculated to lead to the discovery of admissible evidence.
      2. Lester v. Allied Concrete Co., Case No. CL09-223 (Va. Cir. Ct. Sep. 1, 2011), Lester v. Allied Concrete Co., Case Nos. CL08-150, CL09-223 (Va. Cir. Ct. Oct. 21, 2011) (sanctioning plaintiff and his attorney for knowingly deleting potentially incriminating photographs on Facebook).

c. Rule 1.1 of the Rules of Professional Conduct

i. A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
ii. Requires attorneys to be knowledgeable regarding social media.

Thank you to Danielle D. Giroux and Jon A. Nichols, of Harman, Clayton, Corrigan & Wellman, PC, for their contributions to the written materials.