It was Abraham Lincoln who said “If we could first know where we are, and whither we are tending, we could then better judge what to do, and how to do it.”

We are now seven years into an era officially started in 2006 by changes to the Federal Rules of Civil Procedure, defining the manner and methods by which electronically stored information (ESI) could be discoverable. For the past decade, ESI has primarily meant emails. We have now begun a new phase of e-discovery characterized not only by emails, but also social media.

No part of e-discovery is moving more rapidly, or is in greater flux, than social media. This is so for several reasons, but three predominate:

- The widespread use, incredible volume, and transient nature of the data on social media (i.e. Facebook, MySpace, Twitter, LinkedIn, YouTube, etc.).
- The current immaturity of the technology and methods used to preserve, collect, authenticate and review social media data.
- The relative dearth and inconsistency of case law in federal and state courts to guide litigators.

This current state of instability raises certain risks (and provides some opportunities) in the practices of employment and personal injury attorneys where social media data has proven to be especially valuable, if not decisive, in litigation.

This article will address the manner and means by which counsel can gain access to social media evidence, providing a succinct summary and “lessons learned” from the limited case law. We will then investigate the areas where social media has been used successfully in employment and personal injury litigation. Finally, we will review several technological social media challenges faced by employment and personal injury litigators, provide some practical insights and advise on how to address them, and outline where to seek resources to assist, when necessary.

How Do You Gain Access to Social Media Evidence?

Until recently, requesting documents in e-discovery usually meant seeking emails from opposing counsel. While emails still comprise a large part of e-discovery requests, increasingly employment and personal injury cases have seen a growing number of e-discovery requests involving social media. If emails were thought to provide a less formal, “less likely to be considered official” means of communication when it became popular a decade or two ago, authors of social media posts have proven to be even more spontaneous and frank. Envisioned initially as a purely social communication media, there was a written, although not necessarily legal, expectation of privacy conveyed by the social media service providers in the privacy settings by which subscribers could categorize the material on their social media site. While perhaps not intended to do so, these privacy settings have led (and still lead) many participants to believe that their communications and posts are “private”.

Not surprisingly, privacy and confidentiality are usually cited as the primary reason for refusing discovery requests for social media. However, many courts have repeatedly ruled that discovery of potentially relevant evidence “trumps” privacy when it comes to social media for several reasons:

First, it is difficult to seriously argue that there is a legitimate expectation of privacy when the stated purpose of social media is to share information and experiences on the world-wide web, and at least a portion of the individual’s social media site has a public section available to the entire planet. Second, while site owners may restrict access to portions of the site through “privacy settings”, the designated “friends” who have access to this private information are not restricted from sharing it with others outside the circle of “friends” of the initial author. Finally, there are scores of social media provider employees who as “site operators” have access to all information on the social media site regardless of privacy settings.

However, as we know, there is not an absolute right to seek discoverable evidence in litigation. It must first be relevant to the issues and case for which it is being sought, or there must be a reasonable expectation that the discovery will lead to relevant evidence. In a number of cases, both federal and state, this burden has been met by information

Continued on Page 5
WHAT EMPLOYMENT … (Continued from page 4)

that was posted on the public portion of the social media site.

For example, in two federal employment law cases (EEOC v. Simply Storage Management, LLC\(^4\) and Held v. Ferrellgas Inc.\(^5\)), the courts permitted the requesting defendants access to social media sites. In the first case, the court limited the requested information by scope and timeframe, and in the second, the court limited the request to information that was reasonable and relevant (i.e., not requesting access to the entire sites). In the second case, a motion to compel was the means used to overcome the plaintiff’s refusal.

However, in Mailhoit v. Home Depot, U.S.A. Inc.,\(^6\) a recent California federal district court, under factual circumstances very similar to Simply Storage, the court refused to compel production of a party’s Facebook posts and photos. This court commented that the discovery requests seeking information regarding the emotional state of a former employee in a wrongful termination case were “too broad” and did not provide “sufficient notice….of what could be considered responsive material.” The Mailhoit court also stated that the Simply Storage court “failed to give proper weight to the parties’ ability to carry out the order.” It will be interesting to see which approach other federal district courts and federal appeals courts follow in the months and years ahead.

At the state level, five Common Pleas cases from Pennsylvania counties have addressed this issue in personal injury litigation. In three of the cases, McMillen v. Hummingbird Speedway, Inc.\(^7\), Zimmerman v. Weis Markets, Inc.\(^8\), and Largent v. Reed\(^9\), the courts each ruled that as a result of postings on the public portion of the social media sites, defendants were led to the reasonable belief that more relevant information might exist on the private portions of the sites. As a result, each court ordered the plaintiffs to provide their logon ID’s and passwords, after the plaintiffs had initially refused to do so.

In the fourth case, Trail v. Lesko\(^10\), complete access to Facebook by ordering logon ID’s and passwords was denied, when the court ruled that neither party had established that Facebook might contain relevant evidence.

In the fifth case, Arcq v. Field\(^11\), where no information was found on the public site to permit the defendants to reasonably believe that relevant information existed in other portions of the site, the court denied access. The court reasoned that while it was not an “absolute necessity” that material appear on the public portion of the site to warrant access to the entire site, it was necessary for the defendant to have some “good faith belief” that the private portion may contain relevant information.

These cases raise at least two important issues: 1) will some clarity develop as more federal district courts and federal appeals courts, as well as state appeals courts address these issues, and 2) under Arcq v. Field, what additional information might a party need to reach a “good faith belief” regarding the evidence on a social media site? The obvious answer seems to be the testimony received in interrogatories or depositions. If so, will this approach be adopted by federal courts as well?

What Are The “Lessons Learned” From These Cases?

First, always ask opposing counsel for access to social media sites. Perhaps they’ll grant it, precluding your need for any of the following steps.

Second, based upon strategic considerations, your request can be for complete access by seeking the ID # and password to the site(s), or a discovery request limited to the issues of the case and a reasonable timeframe, allowing the client and opposing counsel to perform the search. The relevance and egregiousness of the evidence found on the public portion of the site will probably help determine which approach should be taken.

Third, if no relevant evidence can be found on the public portion of the sites, consider sworn responses to interrogatories or testimony in depositions to support your “good faith belief” that relevant evidence exists on the social media sites. The key here will be if such testimony exists.

Fourth, in all instances, make your discovery requests as specific as possible relative to scope and timeframe, and based upon Mailhoit, consider opposing counsel’s ability to carry out the request.

Fifth, it is almost always unproductive to seek social media site information from social media providers, as they have perfected the use of the Stored Communications Act (SCA) to shield them from such requests.\(^12\) To their credit, Facebook has developed a procedure to download site content, the utility of which we will discuss later in this article. Hopefully, other social media sites will follow Facebook offering similar services.

Gaining access to the social media evidence for use at trial in the manner prescribed above goes a long way to providing the


\(^7\) McMillen v. Hummingbird Speedway, Inc., 113-2010 CD (C.P. Jefferson, Sept. 9, 2010)


\(^9\) Largent v. Reed, 2009-1823 (Pa. Ct. of Common Pleas; Nov. 8, 2011)


Continued on Page 6
WHAT EMPLOYMENT … (Continued from page 5)

evidence that you need to win your employment or personal injury case. But there are still several tricky technical hurdles that must be overcome to have your evidence preserved, collected and admitted in court. Before we address these technical issues, let’s review how social media, once obtained, can be successfully used to win your employment or personal injury case.

Using Social Media Successfully in Your Employment and Personal Injury Case

Pre-Employment

Let’s say you represent a plaintiff who is filing a discrimination in-hiring suit who claims that he was discriminated against in the hiring process on the basis of race. Since recent studies have shown that pre-screening the social media sites of potential hiring applicants by companies is a widespread corporate practice, it might be worthwhile to investigate the social media screening practices of your defendant. Did they visit social media sites in advance of the hiring interview? Did they visit the public portion of these sites, or request the ID and passcodes from the applicant to access the entire sites? If so, did they inform the applicant of this practice?

Once access to the social media sites was gained, did the hiring manager do these searches, or did someone else do the searches and provide a report to the hiring manager? If the searches were not done by the hiring manager, did the report mention the race of the applicant? The answers to any of these questions may provide the factual basis to support your claim.

That’s not to say that corporations may not screen prospective hiring candidates to select interviewees or determine to whom to extend offers. What it does mean is that certain steps must be taken to ensure that the screening is lawful and not used as a means of discrimination.

For example, a lawful screening of social media will ensure that:

- Someone other than the hiring decision-maker performs the social media site reviews and prepares a report for the hiring manager with only appropriate information included in it.
- A record of the process used to create the report should be completed to include: the person performing the searches and the social media sites visited; the date the report was created and by whom.
- Disclosure is made to the applicant that the public portion of their social media sites may be visited as part of the hiring process. Based upon recent developments, seeking ID’s and passwords from applicants to gain full access to the entire sites should be avoided.
- Applicants are notified of adverse action taken as a result of the social media report (as so ruled by the FTC).

During Employment

Most courts have agreed that company monitoring of the social media sites of their employees is appropriate, if the monitoring is in compliance with a clearly defined corporate social media policy, and if the monitoring is performed to ensure that the use of social media sites does not interfere with work.

These social media policies must provide clear guidance on the use of social media during working hours, include obvious prohibitions against discrimination and harassment, and ensure confidentiality of corporate information. Furthermore, employers must clearly indicate that they intend to monitor computers and social network sites during working hours. Companies are advised to have employees acknowledge that they have read these policies, and they should review and update them periodically.

It should be noted that even when taking all the above precautions, some companies have had trouble with the NLRB over their interpretation of what is considered “inappropriate behavior” when using social media. Gripping about a boss or using profanity may be permitted, if these complaints are made as part of what is considered “concerted activity” that is done on behalf of, or in conjunction with other employees.

Interestingly, company attempts to coerce employees into providing their ID’s and passcodes to their social media sites to provide this employee monitoring have failed under a growing trend by a number of states to pass privacy legislation prohibiting this practice.

After Employment

After employment issues relative to social media usually involve ownership. Who owns the contacts gained through the use of the social media sites? Do employees own this information and have a right to take it when they leave the company, or is the information owned by the company and attempts by employees to take it upon departure a misappropriation of trade secrets? How much effort was taken in advance by the company to safeguard the information seems to be the determining factor used by most courts in deciding the ownership


14 See http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre36.shtm


For example, factual determinations like: if the data in question could have been easily acquired by other means (i.e. a Google search); was the data password protected; were employees required to sign a confidential or non-solicitation agreement relative to this information at the time of employment; was the data restricted to use by only employees and business partners; are all factors in making the ownership of the data determination.

To the extent and degree that employers have sought protection of this type, their claims of misrepresentation of trade secrets by departing employees have generally been supported by the courts.

Social Media in Personal Injury Cases

Most personal injury lawyers are now aware of the incriminating admissions made on social media sites that have torpedoed scores of personal injury claims. Some examples:

- The plaintiff claiming an inability to work as a result of an injury, engaged in dancing, swinging on a swing and enjoying various water sports in pictures posted on her social media site.
- The employee who injured his leg in a forklift accident who testifies that he never wore shorts because he was embarrassed by the scar on his leg from the accident, who is seen in photos on his public portion of MySpace with shorts and the scar visible.
- Or the particularly crass plaintiff who has lost his wife in a terrible accident in the wrongful death suit wearing a t-shirt saying “I love hot Moms” on Facebook.

These, and other careless social media posts, have caused many personal injury lawyers to advise clients that:

- Prior to filing a lawsuit they need to remove any objectionable posts to their social media sites that could hurt their case, reminding the potential client that social media material is usually discoverable.
- They ought to refrain from any posts regarding the people or issues in the trial throughout its duration.
- They need to refrain from “friending” anyone they don’t know, because insurance adjusters, investigators and others may try to get incriminating information off their social media sites through fraud and deception.
- They need to be aware of what information “friends” may posting about them and request that no posts be made regarding them for the duration of the trial.

Privacy and confidentiality are usually cited as the primary reason for refusing discovery requests for social media. However, many courts have repeatedly ruled that discovery of potentially relevant evidence “trumps” privacy when it comes to social media.

Overcoming Technological Challenges Involving Social Media

As mentioned earlier, social media provides several tricky technological hurdles (different from email and other sources of ESI), that can present unique problems, for the litigator in employment and personal injury cases.

Preservation

One of the landmines of social media e-discovery is preservation. If it is difficult to preserve millions of emails in even a small employment case, imagine how difficult it is to preserve emails, pictures and video on multiple social media sites whose servers may be controlled by a social media service provider.

The good news is that although the data resides on servers that may not be controlled by the individual
WHAT EMPLOYMENT … (Continued from page 7)

or their company, the account and therefore the data, for the most part, is controlled by the person who has control of the account profile. Therefore, when a preservation letter goes out at the beginning of litigation, it is sent to opposing counsel and their client with instructions to preserve and not delete social media content. In the best of circumstances, this is no small task given the transient nature of social media data.

Facebook recently made this preservation effort less ominous by the creation of the Download Your Information (DYI) function, which permits an account owner to download the entire site content at that moment in time by executing four easy commands that take about a minute. It then takes Facebook approximately 10-20 minutes to perform the function and return the site contents to the account owner in a zip file attached to an email. As convenient as this sounds, this approach is not without shortcomings. First, the file will not copy any information that has been deleted prior to the copy being made, nor does it provide a means by which any deletions can be detected in the received file. Second, the procedure does not capture the application program interfaces (API’s) required to capture the metadata or the hash values that can be so important to proper authentication.

Even with these limitations, requesting that opposing counsel and his client use this capability from Facebook and other social media providers that develop a similar capability, may provide valuable data that might be otherwise lost, if a forensic collection cannot be made.

To stress the importance of timely and accurate preservation of social media content, your request to preserve social media content in your preservation letter to opposing counsel and their client might include a reference to a recent Virginia state case21 where counsel instructed a paralegal to tell their plaintiff client to “clean up” his Facebook profile that had some potential damaging pictures and posts on it after the case had been filed. Later the client was told by counsel to de-activate his profile. Based upon this spoliation of evidence, the attorney was ordered to pay over $542,000, and the plaintiff $188,000 to the defendant. If, after a lawsuit has been filed, counsel or his client has any thoughts of altering Facebook, or other social media content prior to downloading, this should dissuade them.

A good preservation letter places opposing counsel and their clients on notice to preserve and not alter or delete information on all their social media sites, pending the court’s decision on access to them in response to your discovery requests.

Collection

Using the proper method of collection of social media data is critical because unlike email, where securing metadata is determined by the selection of the format in which the emails are produced (i.e. Native format that includes metadata, as opposed to PDF or TIFF formats where metadata is not included unless specifically requested as separate load files), metadata for social media is captured during the collection process. By capturing the application program interfaces (API’s) of the social media at the time of collection, the metadata is also captured.

If other methods of collection for social media are used (i.e. “screen shots” or data collected from 1st generation web crawlers), the metadata is not collected and authentication becomes more difficult, especially if there is insufficient testimony and limited circumstantial evidence.22

As with other forms of electronic documents, metadata in social media data can include create time, unique ID # of the person making the post, the device from which the post (or entry) was made, and a log report indicating every time a page was touched.23 This information can be pivotal in authenticating whether a particular person is the author of a post. Therefore, if any of the metadata items above are important to your case, a decision to pay for a forensic collection that will include the social media metadata and hash values, as opposed to a do-it-yourself “screen shot” collection that does not collect the metadata, is probably worth the additional expense.24

To illustrate this point, metadata used to identify the device from which a post was made could be relevant in a personal injury case where a person has commandeered the ID and passcode of your client and “spoofs” or prefabricates a damaging post. Metadata might be the only way in which your client might be shown not to have made that post.

Authentication

As with other areas of evolving e-discovery law related to social media, there is currently no established standard in federal or state court regarding the authentication of social media. However, to date, the rules of evidence for admissibility for paper documents have proven to be applicable to the special demands of electronic evidence and social media.

In the landmark federal case, Lorraine v. Markel American Insurance Company,25 Magistrate Judge Grimm from the Maryland Federal Court indicated that authentication of electronic evidence is a two-step process:

24 For an excellent discussion involving preservation, collection and other evolving legal and technical issues associated with social media in e-discovery, please see “Primer on Social Media”, The Sedona Conference, 10/2012
WHAT EMPLOYMENT  … (Continued from page 8)

1. Sufficient foundation must be laid to indicate that the evidence is what it purports to be
2. A jury must then determine if the electronic evidence had been fabricated or tampered with

Underlying this approach is whether or not the specter of fabrication is a bar to authentication to be decided by the court, or a factual question to be decided by the jury.

A good preservation letter places opposing counsel and their clients on notice to preserve and not alter or delete information on all their social media sites, pending the court’s decision on access to them in response to your discovery requests.

How much evidence is enough to satisfy the foundational requirement that the evidence was sent from the person who owns the social media profile and has not been prefabricated? In Lorraine, referenced above, both metadata and file level hash values were deemed sufficient circumstantial evidence to establish authenticity.

In another federal case, United States v. Lanzon26 (a criminal case), the 11th Circuit Court of Appeals in 2011, using the rule of evidence that the “proponent need only present enough evidence to make out a prima facie case that the proffered evidence is what it purports to be”, the court allowed authentication of social media evidence on the testimony of a single participant. In other federal and state cases, additional evidence has been required to authenticate social media evidence.27

In People v. Clevenstine28 (N.Y. Superior Court, 2009) (another criminal case), testimony from several people was required to overcome a presumption that social media evidence may have been tampered with. In that case, circumstantial foundational evidence was provided by:

- Testimony from two victims who had exchanged messages with the defendant
- An investigator who testified that he had retrieved messages from the hard drive of the victims
- Testimony from the legal compliance officer at MySpace, stating that the accounts created by the victims and the defendant had exchanged messages

Ideally, testimony from the purported creator of the social media under oath regarding whether he/she created the site profile and added the post in question is the best authentication.

Other ways to provide circumstantial foundational evidence to authenticate social media can include:

- Metadata and hash values resulting from a forensic collection can provide key circumstantial data to authenticate a social media item.29
- Identification of distinctive characteristics of the post, like regularly misspelled words, punctuation, appearance (font style) and other unique print, taken in conjunction with the circumstances.

As the People v. Clevenstine court stated, even with all the circumstantial evidence that was presented, it was still possible that someone else accessed the defendant’s social media account and sent the messages under his name. What most of the cases acknowledge is that while this will always be the case, the more circumstantial evidence provided makes a positive factual jury determination more likely.

Review

Review of social media that has been collected in sequential, lineal form, and includes text, photos and videos, can be very difficult and time consuming to review. Professional e-discovery suppliers can organize this collected social media data to maximize efficiency of review, saving review time and money.

Conclusion

The law related to social media is complex and evolving rapidly. The pervasiveness of social media during all stages of employment and personal injury litigation, as well as its widespread use, incredible volume and transient nature, have ushered in a new phase of e-discovery, where the evidence gained from social media can be the decisive factor in employment and personal injury litigation.

We learned that gaining access to social media is possible if the data is relevant. Asking for the data is the first step. If denied, the courts have ruled that searching for data on the public portion of the social media sites often provides a “good faith belief” that relevant data will be found on the other portion of the site and have subsequently permitted access to the entire site on that basis. Testimony received in interrogatories and/or depositions has also been used to provide the “good faith belief” required for the court to grant access.

26 United States v. Lanzon, 639 F.3d 1293, 1298–99 (11th Cir. 2011)
29 John Patzakis, supra fn 19

Continued on Page 10
We also learned that social media data is pervasive before, during and after employment and personal injury litigation. It is used to screen potential applicants, monitor employee behavior once hired, and determine ownership of data when employees depart. It is also being used to counsel clients before litigation, select jurors, and impeach witnesses.

Finally, we learned that to take full advantage of the decisive nature of this potential evidence, tricky technical issues must be overcome to ensure authenticity and admissibility. Although legal standards are not yet established for social media, a handful of federal and state cases are providing valuable guidance on key issues for practitioners.

The technical challenges require that lawyers get the help they need in this new phase of e-discovery, especially in the preservation, collection, authentication and review of social media. This means that large firms will probably rely more heavily on their in-house, e-discovery practices that they have created over the past several years, to counsel and advise them; and that mid-to-small firms will retain E-Discovery Counsel on an “as-needed” basis to offset the large firm ESI “skill gap” that has developed over the past several years and continues to grow.

If there is any good that we can expect from this next phase of e-discovery involving social media, it may be the opportunity and impetus that it provides to mid-to-small firms as they attempt to close the ESI “skill gap” with larger firms and establish ESI parity.


WPTLA has partnered with PayPal!

You can now make your payments for membership, dinner meetings, sponsorships, etc., with your credit card, via PayPal.

Look for the “Pay Now” buttons on our website.

What Employment … (Continued from page 9)

P I C T U R E S

& PROFILES

Q U E S T I O N N A I R E

Name: James J. Ross
Firm: Bowers, Ross & Fawcett, LLC, Ambridge, PA
Law School: Ohio Northern University
Year Graduated: 1980

Special area of practice/interest, if any: Plaintiff’s personal injury and criminal defense

Most memorable court moment: $3.2 million award in a premises liability action in the Court of Common Pleas of Allegheny County in 2007, with Western PA Trial Lawyers’ member Dave Zimmaro as co-counsel

Most embarrassing (but printable) court moment: Too many to mention

Most memorable WPTLA moment: All of our Comeback Award Dinners

Happiest/Proudest moment as a lawyer: Swearing-in ceremony as Assistant United States Attorney for the Western District of Pennsylvania in 1984

Best Virtue: Hard work

Secret Vice: Blowing off steam with a cold beer or glass of good wine

People might be surprised to know that: I am full-blooded Italian

Favorite movie (non-legal): Remember the Titans

Favorite movie (legal): The Verdict

Last book read for pleasure, not as research for a brief or opening/closing: The Killer Angels

My refrigerator always contains: Prosciutto ham and good cheese

My favorite beverage is: Moosehead or Peroni beer

My favorite restaurant is: Aviva Brick Oven, Wexford, PA

If I wasn’t a lawyer, I’d be: The most interesting man in the world and drink Dos Equis (stay thirsty my friends)