Acquiring, Preserving and Authenticating Social Media Evidence

Old Dominion Bar Assn., May 30, 2015

Presenters: Sharon D. Nelson, Esq. and John W. Simek
President and Vice President, Sensei Enterprises, Inc.
703-359-0700 www.senseient.com
snelson@senseient.com; jsimek@senseient.com
Discovery of Social Media

By Jennifer Ellis (2014, used by kind permission of the author)

Given the value of the information contained within social media accounts, it is no surprise that attorneys desire to obtain access to the information. It is not at all uncommon, for example, for an individual to say one thing in person to her attorney or a judge and to post completely contradictory information on Facebook. An individual might claim in court or interrogatories that she cannot leave her home due to emotional harm from an injury, but in turn post a video on Facebook showing her dancing at a party. In the past, it was necessary to hire a private investigator to prove someone was lying about his injury for a workers’ compensation claim; now the plaintiff frequently posts a picture of himself chopping wood or carrying a heavy couch, the exact evidence the defense attorney needs to prove her case.

Privacy Settings Are Important

Privacy settings control what an individual shares on social media sites. However, many users never change their privacy settings, or simply find the settings too complicated to alter. Many social media sites barely have any privacy settings at all. Twitter, for example, is either open or private. Facebook’s settings are extremely complicated and confusing. Blogs are meant to be open, and people frequently believe they are private when they are not. Since many people do not change their settings, attorneys should and do look through the social media sites in an ethical manner and view and preserve the information they can find. Keep in mind, if the attorney does the preservation, and authentication becomes an issue, the attorney could be forced to become a witness in her own case. It is best to have someone else in the firm do the preservation.

1 https://support.twitter.com/entries/14016#
2 Approximately 13 million US users never change their Facebook privacy settings. Of those that do, the majority are unaware that their privacy settings can be compromised by allowing additional applications access to their accounts and do not take the steps necessary to further protect their data. 13 million US Facebook users don’t change privacy settings, http://www.zdnet.com/blog/facebook/13-million-us-facebook-users-dont-change-privacy-settings/12398
3 Natalie Munroe was a teacher in Pennsylvania who blogged about her students. She believed her blog was only being read by a few people, apparently unaware that it could be widely read. http://tinyurl.com/8hx95c6. Munroe was suspended, brought back, and eventually fired. She claims she was fired due to the blog. The District claims she was fired for incompetence. Munroe has since brought a lawsuit against the district. Blogging Central Bucks Teacher is Fired, http://www.philly.com/philly/blogs/bucksinq/160413996.html
4 New York State Bar Association, Committee on Professional Ethics, Opinion 843, (September 10, 2010.)
The Client’s Social Media

The first step when a new client walks through the door is to ask if he uses any social media. The next step, in some cases, is to inform the client that he must stop posting immediately. Unfortunately, the addiction and use of social media can be so great that the client will be unwilling to stop. As a result, the attorney should also advise her client that if he does post, he should not post anything that deals with the case. The attorney must be clear about what “deals with the case” means, since many clients will simply think it means specifics about how the case is going, as opposed to comments about giving money to his mistress, lifting a heavy couch, attending a party, and so on. Make certain to ask the client not only about his own accounts, but his comments on other blogs and websites that might be relevant to the case. Social media and other online surprises can be very harmful. It is also important to remind the client that he may not delete any content from his account, even if it is potentially harmful to his case.

The first meeting with a client is also the time to speak with him about changing his privacy settings to make certain that his account is secure. Providing instructions on how to change privacy settings in written form or a video can be very helpful. It is also a good idea to have the client sign a document making it clear that he was told not to delete any content. This will protect the attorney from accusations of spoliation later on. In some cases it might be wise to ask for access to the account(s). Asking to friend the client is not enough, the password is necessary for a complete review of the client’s online conduct.

Also, if the client has a personal relationship with the opposing party, ask about the other side’s use of social media. In addition, ask the client if any potential witnesses are using social media. Find out if the client is friends and therefore has access to private areas of the accounts.

Opposing Party and Witnesses

Immediately view the opposing party’s accounts and witness accounts if they are freely accessible. It is permissible to view the accounts if the client has access. It is also permissible to ask witnesses to provide access to their accounts, though the attorney or other individual asking for access must be honest about her relationship to the case.

Also send a Notice of Preservation to opposing Counsel. Fortunately, the amendments to the federal discovery rules from 2006 allow for discovery of electronic data to begin very early in the litigation process. Make it clear to opposing counsel that all data must be preserved. Do not just name specific social media sites, but be clear in the preservation that it means all sites and all accounts. Unfortunately, exactly what preservation is required is not yet clear. Does preservation mean keeping the privacy settings as is, so if an account was open it remains such?
Does it simply mean that data may not be deleted? Be clear about expectations and do not be surprised if the matter ends up before a judge.

Send out the Interrogatories relating to social media as quickly as possible and ask the right questions. Again, do not give the opposing client a chance to wiggle out by asking simply for Facebook when the client might have a Plaxo Account. Ask for everything. Ask for all email addresses as well, because the opposing party might have several accounts under various email addresses. Further, keep in mind that with strict privacy settings the opposing party can all but hide the existence of his account(s).

Trouble for Failure to Preserve

In the past, some have believed that it is acceptable to delete posts from social media accounts. A Virginia decision from 2011 puts the debate to rest. It is spoliation to delete relevant posts. In the case, the attorney instructed his client to “clean up’ his Facebook because we don’t want blowups of this stuff at trial.” The attorney further instructed the client to delete or deactivate the account, and then responded to discovery requests by informing opposing counsel that his client had no Facebook account. The client deactivated the account instead of deleting it. Upon reactivating the account, the client deleted 16 photographs, following his attorney’s instructions. Based on the spoliation, the court held that sanctions should be granted against both the attorney and the client. The sanctions amounted to $722,000 in legal fees, over $500,000 of which was payable by the attorney. In addition, the judge in the case reported the attorney to the Virginia State Bar. In the end, the attorney agreed to a five year suspension of his license.

A recent New Jersey case shows the serious consequences of deleting content from Facebook. In that case the plaintiff claimed that he deactivated his Facebook account and did not restore it quickly enough, resulting in deletion of his account. Leaving aside that this is not how Facebook deactivations and deletions actually work, the end result was that the court found that deletion of the account was spoliation of evidence and granted an adverse inference against. Given the cases and the trend, it seems to be straightforward that deleting posts, pictures or videos is unacceptable and likely to lead to serious sanctions.

---

6 “On July 17, 2013, the Virginia State Bar Disciplinary Board suspended Matthew B. Murray’s license to practice law for five years for violating professional rules that govern candor toward the tribunal, fairness to opposing party and counsel, and misconduct. This was an agreed disposition of misconduct charges.” VSB Docket Nos. 11-070-088405,11-070-0884222.
7 In the author’s experience, when a Facebook account is deactivated it is never deleted. When the owner logs into his account again, it is restored. In order for a Facebook account to be deleted, specific actions requesting deletion must be taken on the part of the account owner.
Ethical Pitfalls in Research and Discovery

There are a number of relevant guidance opinions from the New York City and State Bars,9 Philadelphia Bar10 and the San Diego County Bar11 Associations surrounding issues related to performing research utilizing social media.

General Research

First, as already noted, it is perfectly acceptable to search and access social media sites that are freely accessible. The New York Guidance Opinion states, “[an attorney] may access the public pages of another party's social networking website (such as Facebook or MySpace) for the purpose of obtaining possible impeachment material for use in the litigation.”12 On the other hand, the Philadelphia Opinion makes it clear that an effort to obtain access to the account through deception or illegal means is unacceptable.13

Friending a Witness

In the Philadelphia opinion, the attorney asked whether it would be acceptable for the attorney to have a third party request a witness to “friend”14 the opposing client. The third party did not intend to lie, but neither did he intend to reveal his relationship to the attorney.

The opinion noted that such behavior would violate several rules of ethical conduct. The lawyer would be “procuring conduct [and be] responsible for [that] conduct” in violation of Pennsylvania Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants.) Also, the lawyer

---

9 New York State Bar Association Guidance Opinion 843  
http://www.nysba.org/CustomTemplates/Content.aspx?id=5162  
10 Philadelphia Bar Association Guidance Opinion 2009-02  
12 New York State Bar Association Guidance Opinion 843  
13 Philadelphia Bar Association Guidance Opinion 2009-02  
14 Friend is Facebook's term for two people who are connected to each other on the service. Different social media providers use different terms. For example, LinkedIn uses “contact” and “connection.” Friending someone requires the affirmative action of a request on the part of the individual seeking the connection and an affirmative action on the part of the individual accepting the connection. See Facebook, “How do I add a Friend?”  
would be violating rule 8.4 (Misconduct) by engaging in “deceptive” conduct. In addition, the attorney would be encouraging a third party to violate Rule 4.1 (Truthfulness in Statements to Others) by having the third party “omit a highly material fact.”\textsuperscript{15} Based upon the Philadelphia Bar Association’s Guidance Opinion, it is very clear that having a third party (or the attorney herself) friend a witness without revealing her relationship to the case would be highly inappropriate.

*Communicating with a Represented Party*

The San Diego County Bar Association took on the issue of communicating with a represented party. In short, as is the case off line, it is inappropriate to communicate with a represented party online. In the instant case, the attorney did not identify himself as the attorney, which made the effort to communicate all the more grievous. An additional issue, of concern for those involved in employee cases, includes an analysis of whether the contacted employees serve as represented parties.\textsuperscript{16}

In 2012, the issue of friending represented parties came up in New Jersey where two attorneys are likely to face sanctions due to their paralegal friending the opposing party in a case.\textsuperscript{17} The issue came to light during a deposition when it became clear that the attorneys had access to the private areas of the plaintiff’s Facebook account. The attorneys denied responsibility because they asked the paralegal simply to perform a general search of the web. The issue with this defense is that attorneys are responsible for the behavior of their staff. The attorneys are charged with violating New Jersey rules 4.2 (communications with represented parties,) 5.3(a), (b), and (c) (failure to supervise a nonlawyer assistant,) 8.4(c) (conduct involving dishonesty and violation of ethics rules through someone else’s actions or inducing those violations,) and 8.4(d) (conduct prejudicial to the administration of justice.) In addition, the more senior of the two attorneys is charged with RPC 5.1(b) and (c) (ethical obligation in relation to supervising another attorney.) These are all very serious charges, and regardless of the outcome, the publicity, which will spread rapidly through social media, will no doubt be very harmful to the two attorneys in question.

At this point it seems well-settled that the action of friending someone or seeking to access their accounts through some form of communication, is contact. Therefore attorneys should never seek to friend or obtain access to the account of an opposing party through any form of communication with a represented party. If seeking to friend a witness, the attorney or individual assisting the attorney must be clear of her relationship to the case.

\textsuperscript{15} Philadelphia Bar Association Guidance Opinion 2009-02
\textsuperscript{16} SDCBA Ethics Opinion 2011-2, May 24, 2011
\textsuperscript{17} http://www.lexisnexis.com/community/labor-employment-law/blogs/labor-employment-commentary/archive/2012/09/13/ethics-charges-for-two-lawyers-over-facebook-friending-a-litigant.aspx
**How to Obtain Access**

If an attorney believes that there is useful information contained within a social media account, she should seek to obtain access to the information hidden therein. There are a number of ethical ways to do so, aside from just looking to see what is freely available.

*See if the Client or a Friendly Witness has Access*

In family law cases especially, the parties or witnesses might have access to each other’s accounts. It is perfectly acceptable to view and use any information that is freely available through this method. Be cautious in any case though where it looks like a witness might be sharing the information under duress. For example, in an employer/employee case, if another employee is friends with a plaintiff on Facebook, he might feel he has no choice but to share the information. If that employee complains later and says he was forced to share the access, it is uncertain how a court will look upon it.

*Ask for Access to the Account*

During the discovery process, unless there is a reason not to do so, ask for access to any and all social media accounts. In terms of Facebook, it is possible to download an entire account, so request that the opposing party do so and provide a copy.\(^18\) Be sure to ask for continuing access as well. The opposing party will likely refuse this request, and wisely so. Social media postings can provide a plethora of private information, some of which may be harmful to a case. It is possible to simply ask the opposing party to adjust privacy settings so the account is viewable, but again, it is likely this request will be refused. It is always best to ask though because during the discovery process the judge will certainly ask if the request was made.

*Send a Subpoena to the Site*

Though generally the social media sites will not cooperate with a civil subpoena, from time to time they will be surprisingly helpful\(^19\). As a result, it never hurts to send the subpoena. Even if the site won’t provide content, citing the Stored Communications Act, it will normally provide assistance in connecting an account with an email address. This can be helpful if ownership of the account will be in issue. For example, in a criminal case the prosecution’s verdict was

\(^{18}\) Facebook’s “Download your information” tool is located under Account Settings.

\(^{19}\) See Won’t the Social Media Provider Help, *infra*. 
overturned when it was shown that prosecution had failed to tie the account in question to the defendant’s girlfriend.\textsuperscript{20} Proof of ownership could have been shown with MySpace’s assistance.

\textit{Compel Discovery}

This is where things get tricky. Different judges tend to have different responses to the request to compel discovery of a social media account. The best approach, and the one that has shown the most results, is to capture what is already viewable (through appropriate ethical means) and to show it to the judge. If the judge can see that the account has relevant and contradictory information, she is likely to provide access to the account. If the judge has concerns about the privacy of those other than the account holder, request that the court review the data first to help resolve the issue. Some judges do not feel that there are any privacy rights in social media content.\textsuperscript{21}

\textit{Case Law}

There are a number of opinions related to discovery of social media when the account itself is not a part of the case, in other words when opposing counsel believes that she might find useful data in the account but the online behavior is not at the center of the dispute. At this point the trend in such cases is to provide access to social media accounts only when the opposing party can show that there is relevant and/or contradictory information contained therein. For example, in \textit{McMillen v. Hummingbird Speedway, Inc.}\textsuperscript{22} a review of the public areas of McMillen’s Facebook page revealed information contradictory to what he was claiming in terms of his injuries. The judge provided access noting specifically that the Facebook information was not privileged.

Another case is simply the paragraph long \textit{Piccolo v. Paterson}.\textsuperscript{23} The judge denied access to the Facebook pages the defense desired. The judge noted that the defense already had many pictures, and that no pictures or other data were freely available that showed contradictory information to what the plaintiff was claiming. In is interesting to note that the plaintiff actually changed her privacy settings early in the case, to preclude anyone other than a friend viewing her pictures.

\begin{itemize}
\item \textsuperscript{20}Bad MySpace Detective Work Results In Overturned Murder Conviction
\item \textsuperscript{21} NY v. Harris, 2012 NY Slip Op 22175, June 30, 2012.
23 http://tinyurl.com/3jhmk2e
http://www.theemployerhandbook.com/piccolo.PDF
\end{itemize}
In *Zimmerman v. Weis Markets Inc.*

24, the judge granted discovery due to the public availability of pictures that contradicted the plaintiff’s claim that he did not wear shorts due to his embarrassment about a scar. The plaintiff posted pictures on his MySpace profile which clearly showed him wearing shorts after his injury (the scar was visible.) Due to the public availability of this contradictory information the judge found that there was clearly relevant data to be found within the MySpace account and therefore access to the account was properly compelled.

Another important case comes from Judge R. Stanton Wetick. Judge Wetick is known as a discovery judge in Pennsylvania, so his view on the discovery of social media was quite welcome. Judge Wetick denied mutual requests for access to Facebook accounts in the case of *Trail v Lesko* because he was not going to allow a fishing expedition when there was no evidence that contradictory or useful information could be found in either Facebook account.

Therefore Judge Wetick used the same reasoning as in many of the other cases on this issue.

In a recent Florida case, the Judge granted in part and denied in part the request by defense in a personal injury case for complete access to the plaintiff’s social media network. He held that the plaintiff must provide copies of all pictures depicting her since her injury, rather than provide access to the entire social media account in question. He further held that in requesting that the plaintiff provide every device on which she accessed her social media accounts, the defense had overreached. In reaching his decision the judge noted that social media sites are “neither privileged nor protected by any right of privacy.” He also noted though that the discovery request must be properly tailored, and to support both assertions, he cited the decision in *Tompkins v. Detroit Metropolitan Airport.*

In *Tompkins*27 the court found that while social media is discoverable, and “generally not privileged,” the opposing party still may not, “have a generalized right to rummage through information that Plaintiff has limited from public view.” The court required a “threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence.” As in the other cited cases, the court wanted to see some evidence that justified the defendant, “delving into the non-public section of [plaintiff’s] account.” The court noted specifically that if the public segment of plaintiff’s account had “contained pictures of her playing golf or riding horseback,” that the defendant would have had a better case to access the private portions of her account.

---

25 Trail v. Lesko, No GD-10-017249.
27 Tompkins v. Detroit Metropolitan Airport, Case No. 10-10413, 2012 WL 179320 (E.D. MI. 2012)
The conclusion to be drawn thus far about the majority of social media discovery decisions is that, while courts are willing to provide access to private sections of social media accounts, they are not willing to allow fishing expeditions simply based on the view that the accounts might have useful information. Some evidence showing that relevant information can be found in the account must be offered before discovery will be granted.

*Won’t the Social Media Provider Help?*

Social media providers will not provide content from a social media account in civil cases. As recently as 2007 some providers did respond to civil subpoenas with content, but now the providers state unequivocally that due to the Stored Communications Act, 18 U.S.C. § 2701 et seq, they may not provide content. The providers will respond to a subpoena only with information about who owns the account. This means the only way to get the data is to have the owner of the account cooperate. In criminal cases, most social media providers will assist when provided with an appropriate subpoena or warrant. On occasion a social media site will be surprising, go against its stated rules, and provide the evidence. Therefore, it never hurts to ask with a subpoena in a civil case. Just be prepared for a no.

The various social media sites generally have details on the subpoena process, and what they will provide. Review each site to learn the appropriate steps.

*What Happens if the Owner of the Account Deletes the Data?*

Most social media providers claim that when a user deletes information from his account, it is gone forever. Facebook, for example, explains that its deletion system works much like a recycling bin. In essence, when a user deletes data, that data is stored on Facebook’s server briefly until the system writes over it; this means, unfortunately, if someone is savvy and starts deleting harmful data, there is nothing that can be done to bring it back, once it is overwritten. Facebook does state, “[i]f a user cannot access content because he or she disables or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account’s content. Facebook preserves user content only in response to a valid law enforcement request.” Of course, if there is nothing to find because it has been deleted and destroyed, than the site cannot restore the data. And outside of criminal cases, it must be the account’s owner who requests the data be restored.

---

28 Facebook states, “Federal law prohibits Facebook from disclosing user content (such as messages, wall posts, photos, etc.) in response to a civil subpoena.” http://www.facebook.com/help/?faq=17158

29 For Facebook this requires the email address that the attorney desires to connect to the account. https://www.facebook.com/help/?page=211462112226850

30 See Send a Subpoena to the Site supra.

Authentication

Authentication is another troubling issue when it comes to social media. Facebook states that the owner or someone familiar with the account can authenticate it. The issue however is that it is impossible to know whether the user deleted something in the account, leaving only helpful items. This is why it is extremely important to perform research early in the process, and to take screen shots of any evidence discovered immediately. Be certain to keep records as to how the evidence was preserved.

In terms of proving who owns the account, remember, it is very easy to create a fake social media account. Just because an account looks like it belongs to someone does not mean that it does. That is why it might be important to at least subpoena the account identifying information from the social media site, if there is any question as to ability to prove ownership of an account.

The case law on authentication and admissibility of social media sites is contradictory. In State v. Bell the court found that the level of admissibility is low and accepted as good enough testimony from a witness familiar with the MySpace account and e-mail address of the party the information was to be used against. Also the evidence showed that the defendant used certain code words and that those words were contained within the account. The court also noted that the witness agreed that the provided print-outs seemed to be an accurate reflection of the MySpace account in question.32

On the other side, in Griffin v State, the court was concerned about how easy it is to create a fake account and noted that information such as birthdate, picture, and residence were not enough to prove ownership.33

The Other Side – Responding to Social Media Requests

It is important to be prepared to respond appropriately to requests for social media content. All businesses (including law firms) should have a social media policy that controls who may (and may not) speak on behalf of the company. The policy should also consider addressing whether supervisors may be connected to employees on the more social sites (as opposed to professional sites like LinkedIn,) and remind employees about the fact that policies online are the same as policies off line; specifically in relation to sexual harassment and other such issues. Employees should also be reminded not to discuss private information and/or litigation on their social media accounts. Employers might consider training employees on social media privacy

32 State v. Bell, 882 N.E.2e (2008.)
settings to assist in security. As already explained, individuals should be warned not to post anything that can be harmful to their cases on social media.

Social media evidence needs to be preserved appropriately. For a business with a great deal of social media evidence to preserve, it is wise to involve a company that can help in the preservation process during litigation. An individual can simply print out the pages or download the account. If the account is large (and is not on Facebook where it can be downloaded) and it is likely the history of the account will enter into the lawsuit, it might be wise to arrange for preservation of the account through a third party, to avoid any accusations of spoliation later on.

In the end, it is crucial for clients, indeed for everyone, to remember that any content posted on a social media site, even back in 2004 when Facebook was first created and the client might have been in college, could come up later during litigation. Therefore everyone needs to be careful to think before they post. This does not mean that people should go back and clean up their accounts just because some day they might, by chance, be sued. But it does mean they might want to give some thought to their online reputations due to their past and current postings.
How 2 Collect Social Media 4 E-Discovery

By Sharon D. Nelson, Esq. and John W. Simek
© 2014 Sensei Enterprises, Inc.

It is somewhat mind-boggling to realize that Facebook is only a decade old. Yet here we are, with more social media platforms than we can count – and an enormous problem. In fact, several enormous problems.

If you are running a business or law firm which is actively on multiple social media platforms, you may need to archive all that data for compliance reasons. And it goes without saying that your data will be subject to discovery.

Or perhaps you have a case in which social media (a snippet of it or a large volume) is involved. How do you properly collect that kind of evidence? Maintain the chain of custody? And authenticate it in court?

As to the value of the evidence, it cannot be overstated. Some experts estimate that Facebook postings emerge as evidence in as much as 60% of divorce cases. Personal injury law is probably a close second.

We’ve all seen some of the legendary cases in which someone makes a legal claim that they are wholly disabled only to put (usually on Facebook, the big kahuna of social media evidence) a photo showing them skiing, dancing, chopping down trees, etc. Our favorite is the guy operating the chain saw who bursts into a spontaneous Irish jig. According to his court pleadings, he was pretty much confined to his bed by his various disabilities. We are assuming the case did not go well for him.

It is useful to underscore that both parties have the duty to preserve relevant evidence, including social media evidence. Often, plaintiffs feeling aggrieved overlook that. Spoliation is not tolerated – and in one Virginia wrongful death
case where an attorney advised a client to “clean up his Facebook,” he paid for it dearly. Though the case was won, the victory was Pyrrhic, especially for the attorney, who had to pay significant sanctions of $500,000, including defense counsel’s fees and costs. He was also fired from his firm, suspended by the Virginia State Bar and he left the practice of law.

So how do you capture the evidence from social media?

Sometimes, if you just need a few social media postings preserved, you don’t need one of the larger companies. Small digital forensics firms are accustomed to this sort of preservation, using tools like SnagIt or Adobe Acrobat - and the costs are minimal, generally several hundred dollars. The files are stored, generally, on their servers and any transfer of the files involves a chain of custody document. This is not necessary if your consultant uses products such as Reed Tech’s Web Preserver, since it logs the user and the data and time of preservation, as well as hashing the file at the time of preservation. The software of some of the other vendors will do exactly the same thing.

But why not do it yourself? We have become a DIY nation, but it really doesn’t make sense to do itself yourself or have an employee do it. You really don’t want to put anyone from your firm on the stand to authenticate the evidence, particularly since your firm and your client have a vested income in the outcome of the case. The evidence may seem suspect. Respected third party experts constitute the avenue of choice – and remember, experts live and die by their reputations, so their credibility is life’s blood to them.

Authentication is usually simple if a third party expert has been used or if self-authenticating software has been employed. And how wonderful if the parties stipulate to the authenticity of the data – the failure, so often, to do this baffles us, especially where there is no credible challenge to the authenticity.

Remember that the problem of authentication goes away if the other party provides his or her own social media postings. Facebook has for several years made it easy to download all that you have ever posted – and it is to the user you will have to look if the postings are not public because social media companies
will generally be protected from revealing the data by the Stored Communications Act, except in criminal matters.

Still, we have seen many cases where data is public because there are no privacy settings. In the case of businesses, they would defeat the purpose of social media if their posts were not public, but you often see an employee allowed to post on the social media who goes “rogue” in their postings. This is the perfect example of when it critical to get the social media posts preserved before wiser heads can prevail and the postings are taken down.

One very good but blessedly short white paper on the subject of “Overcoming Potential Legal Challenges to the Authentication of Social Media Evidence by John Patzakis of X1 Discovery may be downloaded here: http://www.x1.com/products/x1_social_discovery/whitepapers.html.

As Patzakis points out:

“Under US Federal Rule of Evidence 901(a), a proponent of evidence at trial must offer “evidence sufficient to support a finding that the matter in question is what its proponent claims.” Unless uncontroverted and cooperative witness testimony is available, the proponent must rely on other means to establish a proper foundation. A party can authenticate electronically stored information (“ESI”) per Rule 901(b)(4) with circumstantial evidence that reflects the “contents, substance, internal patterns, or other distinctive characteristics” of the evidence. Many courts have applied Rule 901(b)(4) by ruling that metadata and file level hash values associated with ESI can be sufficient circumstantial evidence to establish its authenticity.”

Once again, we must tip our hat to Patzakis for a blog post he wrote on Federate District Court Judge Paul Grimm’s 2013 law review article (co-authored with two of his law clerks), entitled “Authentication of Social Media Evidence.”

Judge Grimm is something of a rock star in the e-discovery community and summarizes his excellent 29-page article as follows:
“Given the ubiquitous use of digital devices to communicate on social media sites, there is little chance that such evidence will cease to be highly relevant in either criminal or civil cases...Hopefully, this Article can shed some light on the nature of the confusion and offer useful suggestions on how to approach the authentication of social media evidence. It is a near certainty that the public appetite for use of social media sites is unlikely to abate, and it is essential for courts and lawyers to do a better job in offering and admitting this evidence. We hope that reading this Article will be their first step toward this goal.”

No doubt much of what it is written in this article will be taken as sound guidance by lawyers and judges alike. The article is available to subscribers to LexisNexis and Westlaw but non-subscribers may purchase the article for $15 at https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=36+Am.+J.+Trial+Advoc.+433&srctype=smi&srcid=3B15&key(fc4221105d6e3043005602dcb471862d

The article includes a “checklist for authentication” and a discussion of the perils of relying on screen printouts of social media, documenting the many cases where such printouts were disallowed or otherwise subject to serious challenges by the courts. Additionally, Judge Grimm highlights Federal Rule of Evidence 901(b)(4), (authenticating evidence through internal patterns and other “distinctive characteristics”) noting that it is “one of the most successful methods used to authenticate all evidence, including social media evidence.” Judge Grimm advises the collection of “all of the circumstances and characteristics that apply to the social media exhibit that add up to a showing that, more likely than not, it was authored by the person that you contend authored it.”

Judge Grimm is certainly correct that the case law in this area is “clear as mud,” with courts frequently coming down on all sides of the issues involved in authentication. One set of cases will not admit the evidence unless the court conclusively determines that the evidence is authentic. Another line of cases looks to whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic.
Our presentation will go through some of the cases on both sides of the fence, but it is worth noting that we have seen an uptick in the number of courts that adhere to the “duck” rule: “If it looks like duck and quacks like a duck, it must be a duck.” There are so many distinctive circumstances of characteristics in social media evidence, including content, use of nicknames, dates, Internet addresses, abbreviations, slang, knowledge of specific facts, replies to another post, etc. that the “duck” approach often works.

We have heard from our local state judges that, unless someone objects to the authenticity of the evidence (or its relevance), it will come in – that’s just common sense. As they candidly say, their system works and they are loathe to make things more complicated than they need to be.

Though there are still cloudy issues involved in the preservation and authentication of social media evidence, one thing is clear. In a single decade, we’ve come a heck of a long way in the preservation of this new form of evidence.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com