Social Media:

Preservation, Harvesting and Authentication

By Sharon D. Nelson, Esq. and John W. Simek

The Rapid Rise of Social Media

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. One sixth of the world's population was on Facebook as of 2014. 74% of all online American adults use it.[1] And yet, we have had very little concrete history in the courts – what opinions we have are often contradictory. Unless you've dealt with a particular judge, you may have no idea what kind of a ruling you are likely to get with respect to social media evidence.

For those 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. In real life, many companies are not archiving, regulations notwithstanding. And few firms understand that their social media postings are subject to discovery until they receive a discovery request.

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 is probably a close second, most likely followed by employment cases.

This is by no means a scholarly article. These are observations and musings of two e-discovery and digital forensics experts, who see a lot of things happen in preliminary hearings that will never be reported in a court opinion.

So, as Bette Davis once famously said, "Fasten your seat belts – it's going to be a bumpy ride."

Preservation – DIY or Outsource?

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 duty. 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 he won the underlying wrongful death case, the victory was Pyrrhic. He had to pay significant sanctions, including defense counsel's fees and costs. He was also fired from his firm, suspended by the Virginia State Bar for five years and he ultimately left the practice of law.[2]

Many people have to preserve social media for compliance reasons. Obviously, you have to preserve it if you are under a litigation hold. You certainly will want to preserve an adversary's social media content for use in litigation as so much of it seems to disappear with all sorts of imaginative explanations given for the disappearance.

One void we've tried to fill with this article is HOW to preserve social media data, whether it is for compliance or e-discovery reasons. Strangely, as we watched a number of CLEs in this area, none of the speakers were able to describe the specifics of social media preservation – nor did they mention a single vendor.

Companies that provide social media archiving and related e-discovery services include ArchiveSocial (http://archivesocial.com), X1 Social Discovery ™ (http://www.x1.com/products/x1_social_discovery/) and Hanzo (http://www.hanzoarchives.com/). Most such companies will cheerfully give you a tour or a free 30 trial. These companies are best used for larger efforts. Many e-discovery or digital forensics companies can easily (and more cheaply) handle the smaller efforts.

Sometimes, if you just need a few social media postings preserved, you can save money by using small digital forensics firms which are accustomed to this sort of preservation, using tools like SnagIt, Camtasia or Adobe Acrobat - and the costs are minimal, generally several hundred dollars. The files are stored on their servers and any transfer of the files involves a chain of custody document. Some consultants will use products which log the user and the data and time of preservation, as well as hashing the file at the time of preservation.

But why not do it yourself? This is a constant question. Lawyers could certainly use any of the products we've cited above. They can take screen shots too - we've also seen that. We have even seen printed out copies of social media pages admitted by courts – slightly horrifying in most cases since there is no metadata to authenticate something which can very easily be spoofed. Even taking a picture of the screen with your digital camera is a better solution since the date and time is embedded in the image file as metadata.

Lawyer and blogger Molly DiBianca wrote a comical post in July of 2014 about a case in South Carolina entitled, *"How NOT to Produce Facebook Evidence."*[3] In Wellin v. Wellin, Defendants moved to compel production in native format after the plaintiffs "printed out responsive emails and provided photocopies of certain portions of those emails to defendants. Additionally, [one plaintiff] provided the content of several text message exchanges and Facebook posts by transcribing those messages on loose-leaf paper." That certainly elicited a "Yikes!" from us.

The judge granted the motion.

We have become a DIY nation, but it really doesn't make sense to preserve social media 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 interest 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. And, as mentioned previously, the costs of preservation are small – and cases rarely go to trial so the costs of testifying are generally avoided.

Harvesting Social Media Evidence

Many lawyers still make the mistake of thinking they can get non-public social media by going to the social media provider. Though they may get certain information – subscriber info, dates of connections, IP addresses, etc. – they will not get social media content because the Stored Communications Act forbids it.[4]

They will generally have to get the data from the user or from a friend of the user who is willing to share it, assuming it is not public. And clearly, no deceit can be involved in procuring the evidence.

Judges often think it is hard for a user to get his/her own data, so we often advise lawyers to write out the steps to illustrate their simplicity. It takes only a few moments to request your Facebook data – author Nelson has done this several times. The response generally comes back within three hours. It comes in the form of a link to download a .zip file – expand the file, and you have all the posts and photos that the user put online. Note that it will not return what others may have posted on the user's account because they are "friends."

In cases where the social media site provides no mechanism for a user download, we have often seen user consent forms used – once filled out, they can then be sent to the provider, who will produce the content to the user.

We have seen instances where judges have required log-in information for social media sites so that the other side could cruise for evidence, but it seems to us that these cases are rapidly going out of favor. In the paper world, you wouldn't give one side the keys to the other side's office so they could rummage through all the file cabinets. Likewise, they should have no right to do so in the digital world.

The more narrowly a request is tailored, the happier judges seem to be. They tend to grant the most leeway in cases like personal injury suits, where a defendant's lifestyle is broadly in question. As a rule, broad requests are identified as "fishing" by the courts and generally denied.

A common misapprehension among attorneys making a discovery request is that all the social media content which may exist will be turned over to them. In practice, the data **should** go to the producing party's attorney to screen for relevance and privilege before turning it over. If a judge is involved, it always works this way, but it astonishes how many times we see the whole kit and caboodle turned over to the requesting attorney.

Authentication

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 frequent failure to do this baffles us, especially where there is no credible challenge to the authenticity. You can also use requests for admissions – or perhaps lock the authenticity down in a deposition.

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. Starting in 2012, Twitter also made it possible to download your Twitter archive so you can get all your Tweets (including Retweets) from the point at which you started using Twitter.

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.

Sometimes, the expert testimony of third parties who have preserved the data is required. If data was deleted and then recovered, digital forensics experts may be required to authenticate whatever artifacts they recovered.

In a perfect world, the collection of social media will have timestamps and header metadata, the data will be stored unchanged and played back so that it is viewed as it originally existed. And of course there should be an audit trail to the original content.

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 Federal 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 Patzakis 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 the proponent offers evidence of authenticity (called the Maryland Standard). Another line of cases (called the Texas Standard) looks to whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic.[5]

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 posts, etc. that the "duck" approach often works.

We have heard from our local state judges in Virginia that, unless someone objects to the authenticity of the social media 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.

We are roughly a decade into the social media world. Our heads spin when we try to imagine the kind of social media (or mutant children) evidence we may be dealing with a decade hence.

One thing we have certainly learned in our many preliminary court skirmishes on behalf of clients is that counsel would be wise to resolve any issues without resort to the courts.

Therefore, our parting words belong to Judge Gerald Bruce Lee, from the Eastern District of Virginia, who recently told an audience bluntly: "Don't bring me e-discovery disputes. I don't like them." Many of his colleagues seem to share that sentiment.

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

[1] http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/
[2] http://www.abajournal.com/news/article/lawyer_agrees_to_five-year_suspension_for_advising_client_to_clean_up_his_f/
[3] http://www.delawareemploymentlawblog.com/2014/07/how-not-to-produce-facebook-evidence.html
[4] http://www.law.cornell.edu/uscode/text/18/part-I/chapter-121
[5] http://www.delawareemploymentlawblog.com/2014/02/delaware-supreme-court-rules-on-admissibility-of-facebook-evidence.html