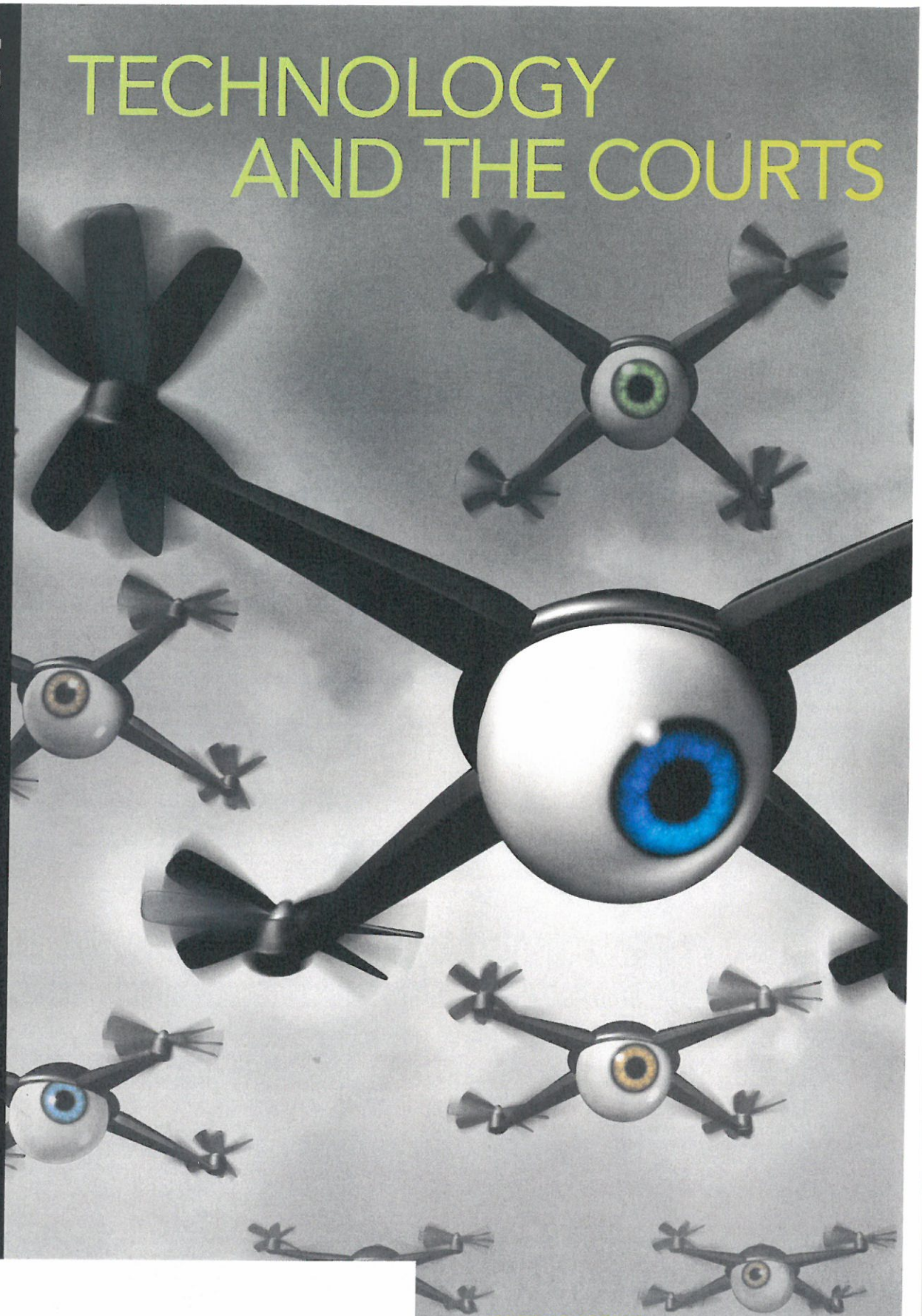
THE JUDGES' JOURNAL

A QUARTERLY PUBLICATION OF THE JUDICIAL DIVISION
FALL 2014 • VOL. 53 NO. 4 • AMERICAN BAR ASSOCIATION

TECHNOLOGY AND THE COURTS

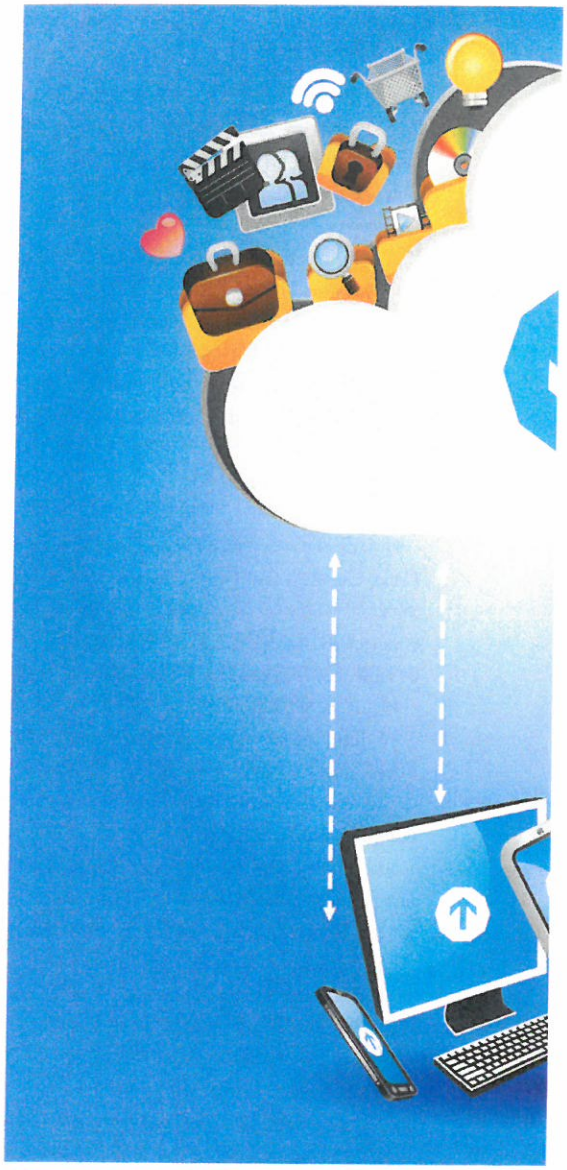


IN THIS ISSUE

- Interview with Chief Judge Eric Washington
- Judging in the Age of Technology
- Brave New World of Social Media
- Online Litigation
- Court Security Continued

Preserving, Harvesting, and Authenticating Social Media Evidence

By Sharon D. Nelson and John W. Simek



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. Seventy-four percent 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 that is actively on multiple social media platforms, you may need to archive all those 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 percent 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. While aggravated plaintiffs often 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 also was fired from his firm, was suspended by the Virginia State Bar for five years, and ultimately left the practice of law.[2]

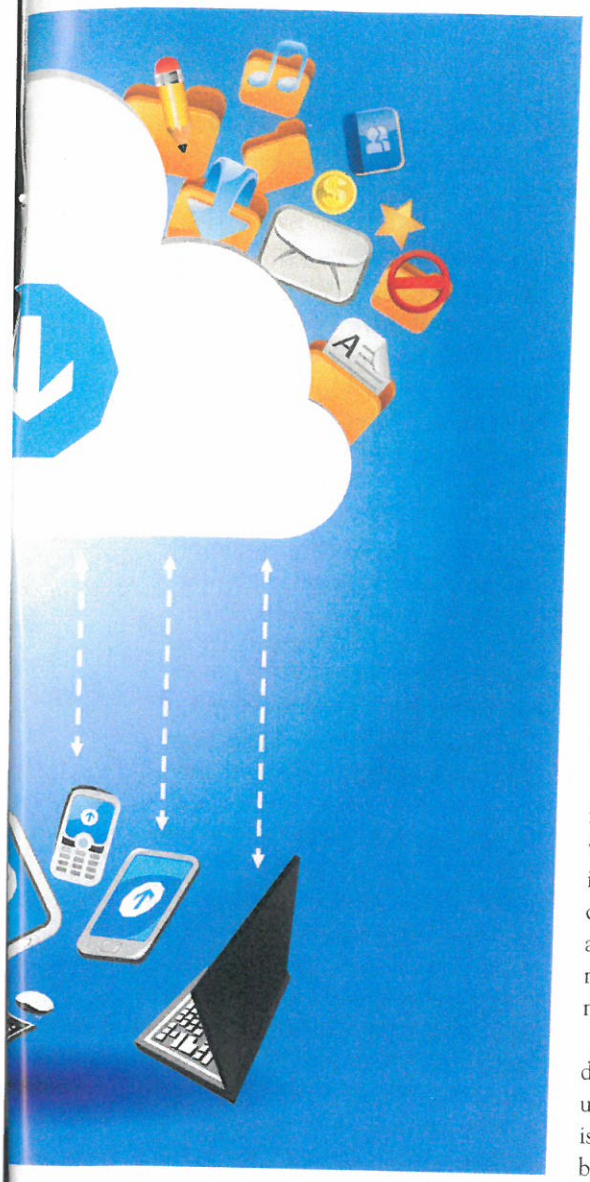
Many people have to preserve social media for compliance reasons. Obviously, you have to preserve it if you are under a litigation hold. You certainly will want an adversary's social media content preserved for use in litigation because so much of it seem to vanish with all sorts of imaginative explanations 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-day 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 that 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 that 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 copies of social media pages admitted by courts—slightly horrifying in most cases because there is no metadata to authenticate aspects that can very easily



be spoofed. Even taking a picture of the screen with your digital camera is a better solution becuase the date and time are embedded in the image file as metadata.

Lawyer and blogger Molly DiBianca wrote a comical post in July 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." This 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 because 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 nonpublic social media by going to the social media provider. Though they may get certain information—subscriber info, dates of connections, Internet Protocal (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 or 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. As a rule, broad requests are identified as "fishing" by the courts and generally denied. Judges tend to grant the most leeway in cases like personal injury suits, where a defendant's lifestyle is broadly in question.

A common misapprehension among attorneys making a discovery request is that all the social media content that 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 them over. If a judge is involved, it always works this way, but it is astonishing how many times we see the whole kit and caboodle turned over to the requesting attorney.

Sharon D. Nelson is the president of Sensei Enterprises, Inc., a digital forensics, information security, and information technology firm in Fairfax, Virginia. She may be reached at snelson@senseient.com.

John W. Simek is the vice president of Sensei Enterprises, Inc.; has a national reputation as a digital forensics technologist; and has testified as an expert witness throughout the United States. He may be reached at jsimek@senseient.com.