The Importance of Understanding that "Computer Stuff"

by Erin W. Hapgood

The air is crisp, the sky is blue, football is in full swing and children are dreaming of bags of Halloween candy and a variety of treats, tricks, and scares. What scares some attorneys the most, however, is the ever-changing landscape of technology. Social media, e-mail and an individual's online presence can be a treasure trove for litigants, but can also tempt lawyers to bad behavior. The threat of a compromised e-mail system or online scam can make the best attorneys want to hide under the bed and cover their ears. Nonetheless, since the revision of the comment to Rule 1.6 of the Rules of Professional Responsibility, lawyers have an affirmative obligation to educate themselves about technology or, as difficult as it is for some attorneys, to seek the assistance of someone with such knowledge.

In honor of the month that sees witches, vampires, and zombies parading the streets, examples of the frightening ignorance and bad behavior of some attorneys can provide guidance to lawyers, at least of what *not* to do.

A dramatic example of which Virginia attorneys are probably familiar, *Lester v. Allied Concrete Co.*, 285 Va. 295 (2013), exemplifies such bad behavior. In the suit for the wrongful death of his client's wife, plaintiff's attorney advised his client (via a paralegal) to destroy potentially damaging posts from Facebook after defense counsel showed him a photograph from his client's account showing plaintiff "holding a beer can while wearing a T-shirt emblazoned with 'I <<heart>> hot moms.'" Compounding the misconduct, plaintiff then responded to discovery stating he had no Facebook account, testified in a deposition that he never deactivated his account, and made other false representations. The jury verdict stood, but plaintiff and his attorney suffered sanctions in the amount of $180,000 and $542,000 respectively.

In a federal case from Missouri,[1] the plaintiff initially denied the existence of her Facebook and other social media profiles, leading the court to grant defendant's request that plaintiff provide a "Download Your Info" report from Facebook, noting that this report will also include records of deleted material. In New York,[2] defendants moved for sanctions and an injunction because they believed the plaintiff had deleted some of her Facebook content. It turns out that the plaintiff had merely changed her privacy settings which, as most Facebook users know, limits who can see the posts but does not delete the content.

Technology can challenge attorneys outside the realm of social media and discovery. A recent settlement in an employment dispute in the Eastern District of Virginia shows just how vulnerable lawyers are to increasingly sophisticated hackers.[3] Plaintiff's counsel received an e-mail from an "aoi.com" address that was "visually similar" to his client's aol.com address, providing wiring instructions for the $65,000 settlement. Properly suspicious, plaintiff's counsel called his client who confirmed he did not send the e-mail; his counsel did not inform the defense that a third party was attempting to subvert the settlement proceeds. Plaintiff insisted on a strict payment deadline, in furtherance of which his counsel informed the defense that he would send wiring instructions. Shortly thereafter, defense counsel received an e-mail, from plaintiff's counsel's actual e-mail address, providing wiring instructions which turned out to be fraudulent.

In his opinion, Judge Payne determined the defendant substantially performed the settlement agreement and that plaintiff failed to take ordinary care. The court concluded that "[a]s technology evolves and fraudulent schemes evolve with it, the Court has no compunction in firmly stating a rule that: where an attorney has actual knowledge that a malicious third party is targeting one of his cases with fraudulent intent, the attorney must either alert opposing counsel or must bear the losses to which his failure substantially contributed."

The most frightening aspect of this situation is the level of detail known by the fraudsters: the plaintiff's name, the exact settlement figure, and the style of plaintiff's counsel's e-mails, including the use of a familiar salutation to defense counsel.

Other cautionary tales come from the experiences of a retired federal magistrate. In one case, the lawyer for a nursing home where one patient beat another to death learned *at the hearing on a motion to compel* that his client's cloud provider deleted data every thirty days; he had never asked his client about how and where they stored their data. In another case, an attorney representing a defendant in a child pornography case was cross examining the officer who had engaged with his client in a chat room. With each question he was, in the judge's words, "digging the hole his cli-

Technology *continued on page 48*

Technology *continued from page 46*

ent was in deeper and deeper." Finally the judge called him to the bench and asked what he was doing; the lawyer actually replied, "Your honor, I just don't understand this computer stuff."

Learning about technology can be daunting, but the frightening consequences of failing to make even the simplest inquiries about electronic data make such knowledge imperative. Lawyers can no longer pretend that these issues will not impact their personal practice. Some may find it difficult to admit their ignorance and ask for help, but this is precisely the obligation imposed by the revised comment to Rule 1.6. Do not wait until your case becomes an example; make the necessary inquiries before you are exposed as a lawyer who just does not understand "this computer stuff."

Endnotes:

1 *Rhone v. Schneider Nat'l Carriers, Inc.*, Case No. 4:15-cv-01096-NCC (E.D. Mo. April 21, 2016)

2 *Thurmond v. Bowman*, 6:14-CV-06465 EAW (W.D. N.Y. August 10, 2016) (the court also determined that three posting were inadvertently deleted; sanctions and injunction denied)

3 *Bile v. RREMC, LLC and Denny's Corporation*, Civil Action No. 3:15cv051 (E.D. Va. August 24, 2016)

Erin W. Hapgood is a member of the Technology and the Practice of Law Committee of the Virginia State Bar. Her practice on the Northern Neck of Virginia includes real estate and other civil litigation, criminal defense, and work as a guardian *ad litem*. She also has experience in electronic discovery in financial services litigation and has written and presented on ethics and technology.

Got an Ethics Question?

The VSB Ethics Hotline is a confidential consultation service for members of the Virginia State Bar. Non-lawyers may submit only unauthorized practice of law questions. Questions can be submitted to the hotline by calling (804) 775-0564 or by clicking on the blue "E-mail Your Ethics Question" box on the Ethics Questions and Opinions web page at www.vsb.org/site/regulation/ethics/.