ETHICAL ISSUES FACING ATTORNEYS IN THE AGE OF TECHNOLOGY

by

Cynthia N. Sass, Esquire

Hillsborough County Bar Association
Trial and Litigation Section CLE
May 2013

Available Courtesy of:
Law Offices of Cynthia N. Sass, P.A.
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
(813) 251-5599
www.EmploymentLawTampa.com

ETHICAL ISSUES FACING ATTORNEYS IN THE AGE OF TECHNOLOGY[1]

Cynthia N. Sass, Esquire
Law Offices of Cynthia N. Sass, P.A.
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
(813) 251-5599
www.employmentlawtampa.com

Hillsborough County Bar Association
Trial & Litigation Section
May 21, 2013

A. LAWYER OBLIGATIONS TO UNDERSTAND TECHNOLOGY

1. **Competence – Fla. Bar R. Prof. Conduct Rule 4-1.1 (2013):**

   A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

   - *Florida Ethics Opinion 10-2* (Sept. 24, 2010); *Florida Proposed Advisory Opinion 12-3* (Jan. 25, 2013). The comment to this rule provides: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject." The Professional Ethics Committee of the Florida Bar interprets this language to mean that a lawyer has an obligation to remain current in developments in technology that affect the practice of law.

   - In addition, in August 2012, the American Bar Association amended the comments to **Model Rule 1.1** on Competence to make it clear that a lawyer's obligation to keep up on changes in the law includes changes to technology. The comment now states that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study

[1] The following material is intended to provide information of a general nature concerning the broad topic of ethics and technology issues. The materials included in this paper are provided by the Law Offices of Cynthia N. Sass, P.A., and are for informal use only. This material should not be considered legal advice and should not be used as such. Thank you to Yvette D. Everhart, Esquire, of the Law Offices of Cynthia N. Sass, P.A. for her assistance in preparing these materials.

and education and comply with all continuing legal education requirements to which the lawyer is subject."

B. RESPONSIBILITIES OF LAWYERS TO PRESERVE ELECTRONIC DATA

1. Ethical Obligations to Ensure Preservation of Evidence

- Fairness to Opposing Party and Counsel – **Fla. Bar R. Prof. Conduct Rule 4-3.4 (2013)**:

  A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act.

2. Federal Law - When Does the Duty to Preserve Arise?

a. Florida federal courts have used the same standard as Florida state courts as to when a duty to preserve evidence arises.

- *Silhan v. Allstate Ins. Co.*, 236 F. Supp. 2d 1303, 1309 (N.D. Fla. 2002) (holding a duty to preserve evidence can arise by contract, by statute, or by a properly served discovery request (after lawsuit has already been filed)) (citing state law).

b. Party's obligation to retain documents, including e-mails, is only triggered when litigation is "reasonably anticipated."

- *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F. Supp. 2d 1317, 2010 WL 3368654, at *6 (S.D. Fla. Aug. 23, 2010).

c. When is litigation "reasonably anticipated?" The mere existence of a dispute does not necessarily mean that parties should reasonably anticipate litigation or that the duty to preserve arises.

- *Treppel v. Biovail Corp.*, 233 F.R.D. 363, 371 (S.D.N.Y. 2006).

- *Simon Prop. Group, Inc. v. Lauria*, 2012 U.S. LEXIS 184638 (M.D. Fla. Dec. 13, 2012) (court found that the sending of letters to the defendants that the plaintiff was auditing its agreements and that litigation might result was sufficient to put defendants on notice that litigation was reasonably anticipated).

- *Southeastern Mechanical Services, Inc. v. Brody*, 2009 WL 2242395 (M.D. Fla. 2009) (court found that litigation was reasonably anticipated upon the sending of a demand letter to defendants).

- *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F. Supp. 2d 1317, 1327 (S.D. Fla. 2010) (court found that upon defendant's letter to plaintiff stating defendant's position with respect to plaintiff's violation of an exclusivity provision in a professional services agreement, plaintiff was on notice that evidence related to its compliance would be relevant; yet plaintiff failed to impose a litigation hold on that evidence for another four months).

- *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (duty to preserve electronic evidence was triggered when plaintiff filed an EEOC charge).

- *Goodman v. Praxair Services, Inc.*, 632 F. Supp. 2d 494, 510 (D. Md. 2009) (duty to preserve arose upon defendant receiving letter from plaintiff stating plaintiff had consulted two attorneys in the matter and made reference to plaintiff being "forced to litigate").

- *But see Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 622 (D. Colo. 2007) (no duty to preserve arose upon defendant receiving demand letter to determine "whether this situation can be resolved without litigation").

3. **State Law - When is There a Duty to Preserve Evidence?**

   a. In Florida, "[a] duty to preserve evidence can arise by contract, by statute, or by a properly served discovery request after a lawsuit has already been filed."

      - *Royal & Sunalliance v. Lauderdale Marine Ctr.*, 877 So. 2d 843, 845 (Fla. 4th DCA 2004).

   b. Most Florida courts have held that there is no common law duty to preserve evidence before litigation has commenced. *Id*.

      - *Gayer v. Fine Line Contr. & Electric Inc.*, 970 So. 2d 424, 426 (Fla. 4th DCA 2007) (holding that "[b]ecause a duty to preserve evidence does not exist at common law, the duty must originate either in a contract, a statute, or a discovery request").

      - *But see, Pen Lumberman's Mutual Inc. v. Fla. Power & Light Co.*, 724 So. 2d 629, 630 (Fla. 3d DCA 1999) (neither rejecting nor accepting the argument that there might be "some type of common law duty to preserve [evidence] after being notified of possible legal action").

   c. However, the Second District Court of Appeal of Florida recently recognized that a party may have a duty to preserve evidence prior to litigation commencing if a claim is reasonably foreseeable or where there was a written request to preserve evidence by the injured party prior to the information or evidence being lost or destroyed in the normal course of operations.

- *See Osmulski v. Oldsmar Fine Wine, Inc.*, 93 So. 3d 389 (Fla. 2d DCA 2012), *rev. denied*, 2012 Fla. LEXIS 140 (Fla. Jan. 31, 2013).

4. **Litigation Holds**

   a. Issuing a litigation hold is to occur "once a party reasonably anticipates litigation, then it 'must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents.'"

      - *Point Blank Solutions, Inc. v. Toyobo America, Inc.*, 2011 WL 1448137, at *11 (S.D. Fla. April 5, 2011), *citing Pension Committee v. Banc of America Securities, LLC*, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010).

   b. It is the duty of legal counsel to ensure that the proper people receive and abide by the litigation hold.

      - *Swofford v. Eslinger*, 671 F. Supp. 2d 1274, 1282 (M.D. Fla. 2009).

5. **Preservation of Social Media**

   a. Duty to Preserve. A few courts have implied that there is a duty to preserve social media and awarded sanctions when the parties failed to preserve such evidence:

      - *Lester v. Allied Concrete Co., supra*, pg. 15 (awarding significant sanctions for lawyer misconduct and spoliation of Facebook® evidence).

      - *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535 (Pa. Ct. Com. Pl. May 19, 2011) (the court ordered the "Plaintiff shall not take steps to delete or alter existing information and posts of his MySpace or Facebook accounts").

      - *Howell v. Buckeye Ranch, Inc.*, 2012 U.S. Dist. LEXIS 141368 (S.D. Ohio Oct. 1, 2012) (stating that the plaintiff was on notice that the opposing party was seeking the private information of the plaintiff's social media account once the defendant served discovery requests and the plaintiff has a continuing obligation to preserve the private sections of the plaintiff's social media account).

   b. Preservation Required. Certain federal agencies that require the preservation of social media, such as FINRA, the SEC and the FDA.[2]

      - *FINRA Regulatory Notice 10-06 (January 2010).* With the rise in use of social media networks, FINRA issued this notice with the primary goal to ensure that investors are protected from false or misleading information and that firms are able to effectively supervise staff in the involvement of these sites. The guidance

[2] Financial Industry Regulatory Authority ("FINRA"), U.S. Securities and Exchange Commission ("SEC"), and U.S. Food and Drug Administration ("FDA").

explains the firms' record retention requirements when dealing with social media. Specifically, the notice provides that firms that "intend to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain the records of those communications as required by the Securities Exchange Act of 1934." FINRA rules require that a broker-dealer must retain electronic communications that relate to its business. The guidance also explains the duties of firms for supervision of associated persons using or posting to social media sites for business purposes. The entire notice is available at: http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf

- *See Investment Adviser Use of Social Media*, SEC Office of Compliance Inspections and Examinations, Vol. II, Issue 1 (January 4, 2012). On January 4, 2012, the SEC Office of Compliance Inspections and Examinations issued an alert about the use of social media by investment advisers. For our purposes, the biggest takeaway from the report was that registered investment advisers have certain record retention obligations under Rule 204-2 of the Investment Advisers Act of 1940 ("IAA"). Under this rule there is no distinction between various types of media that must be preserved. The report advises that investment advisers who use social media must retain records of those communications if the social media content/communications satisfies an investment adviser's recordkeeping obligations under the IAA. It further suggests that advisers determine if it is possible to retain all required records to be in compliance with the IAA. If so, it advises to retain such records in a manner that is easily accessible for a period of not less than five years, and ensure they are available for inspection.

- The FDA has numerous record retention policies that impact consumer products in the marketplace. As social media is used more often to promote products, etcetera, the FDA is now faced with the issue of use of social media and its regulatory requirements. In the FDA Reform Act of 2012, Congress required the FDA to issue guidance and regulations on social media, which may likely have some additional requirements. The deadline for the FDA to issue these rules is July 9, 2014.

c. Tips and Sources for Preserving Social Media. Tips for preserving social media evidence, as well as additional sources to refer to on best practices for preserving social media:

- Treat social media evidence the same as any other electronically stored information and assume that it is discoverable in litigation.

- If you are unsure about how to actually preserve the metadata and embedded materials in social media content, it is wise to consult with IT experts or employ IT personnel that are familiar with the processes for preserving electronically stored information and social media.

- Conduct staff training to educate about the need for record retention and preservation even of social media profiles and content.

- Check to see if the social media network provides for a do-it-yourself function for preserving and saving the social media content. For example, Facebook® has a feature called "Download Your Information," which it introduced in October 2010. This feature vows to allow a Facebook® user to download to the user's computer everything the user ever posted to Facebook®, including all messages, posts, pictures and status updates. However, it is not advisable for lawyers to rely exclusively on this feature as some experimenting with the program uncovered that this feature does not go back and capture things that have previously been deleted or removed.

For the best practices of preserving electronic evidence, lawyers should refer to *The Sedona Principles: Best Practices Recommendations and Principles Addressing Electronic Document Production*. In addition, for more detailed information and technological assistance on preserving social media, practitioners can refer to the September/October 2011 issue of *Information Management*, authored by Rakesh Madhava, available at: http://content.arma.org/imm/September-October2011/10thingstoknowaboutpreservingsocialmedia.aspx.

6. **Consequences of Not Preserving and/or Destroying Social Media and Other Electronic Evidence**

Please refer to **Section C.2.4** below.

7. **Preservation Cautions**

a. Use of Cleaners. What is a cleaner? A cleaner is software or services that may be used to clean up or erase a computer's Internet history, temporary Internet files, computer cache and other files on a computer that have been viewed or downloaded from the Internet. As individuals use the Internet or other online sources, the computer creates temporary files to store information such as Internet browsing history and file download history. A cleaner is often used to make a computer more efficient by eliminating the sometimes unnecessary back up of temporary files. Others may use a cleaner to erase the history or the footprint of their travels on the computer and Internet so others do not see what websites they have visited, what files have been downloaded, or what other types of files they viewed on the computer, etcetera.

(1) Software: There is software that performs such cleaning. One of the most popular cleaners is "CCleaner" (http://www.piriform.com/ccleaner), but there are others available, such as Evidence Eliminator. Such software may be used by many companies' IT departments to maintain the security of computer networks, as well as clean up unnecessary files. However, there may be

documents or files in the temporary files that could be responsive to discovery requests or show evidence of Internet history that may be relevant in litigation that could be purged or deleted through the use of these cleaners.

(2) Services that assist people to "clean" inappropriate content on different social media platforms:

- SocioClean. A free service that allows users to purge any bad or inappropriate material from different social media sites to allow them to keep their social reputation clean. SocioClean works by scanning the user's social media profiles, including pictures, postings, messages and other items on public display. After the scanning process, SocioClean analyzes the public content and grades the content for potential inappropriate material. SocioClean then provides the analysis to the user, who then has the discretion to go back and delete the negative information from their profiles. *See* www.socioclean.com.

- Reppler. A social media monitoring service that includes identification of potential issues and risks about content on social media profiles, which could result in users identifying the negative information and deleting it from the profile. *See* www.reppler.com.

- Others. There are also a number of websites that provide services for businesses and individuals to clean up their online reputation, not by necessarily removing their online history, but by tactics to boost the positive results and bury the negative results when someone searches them on the Internet, such as Google™, Firefox®, Safari, etcetera. For an example of this type of service, refer to www.reputation.com.

These are just a few examples of the types of cleaners available to the average person, as well as companies, to purge computer temporary files, online histories and/or to help hide negative information available on the Internet.

b. Sanctions for Cleaners.

Please refer to **Section C.2.5** below.

c. Practical Tips for Using Cleaners.

- Companies should update their record retention policies and procedures to address cleaners, how often they are used to delete data and the protocols for potentially suspending the use of cleaners once litigation is anticipated.

- Companies should regularly update their employee handbooks or electronic communications policies to advise employees that they are prohibited from downloading or using cleaners for business computers, devices and/or servers

and put in place security protocols that prevent employees from downloading such programs to the company servers or individual work stations.

- From the beginning of representation, when discussing an individual's duty to preserve evidence, lawyers should ask clients about the client's use of cleaners, whether there are any installed or currently used by the client. If the client uses cleaners, immediately instruct the individual to stop using the cleaners and document this in writing.

- In addition, if the individual uses a cleaner on their personal computers, find out their frequency of using the cleaners, and what types of files the individual uses the cleaner to delete. If you can show that the individual has a routine habit of performing "cleaning" on their computer, it may be easier to fight a potential spoliation of evidence claim later.

- Lawyers should frequently train and instruct staff on social media and the practices that are and are not allowable under the rules to ensure that non-lawyers under the supervision of the lawyer do not engage in conduct that puts the lawyer at risk for sanctions and ethics violations.

C. SPOLIATION FOR FAILURE TO PRESERVE EVIDENCE

1. Florida State Law on Spoliation

a. First-party Spoliation. First-party spoliation is not an independent cause of action under Florida state law. The appropriate remedies for first-party spoliation are discovery sanctions or a rebuttable presumption.

- *Martino v. Wal-Mart Stores, Inc.*, 908 So. 2d 342 (Fla. 2005).

b. Definition and Purpose.

(1) Spoliation is defined as the "destruction, mutilation, alteration, or concealment of evidence."

- *Golden Yachts, Inc. v. Hall*, 920 So. 2d 777, 780 (Fla. 4th DCA 2006) (*quoting Black's Law Dictionary 1437* (8th ed. 2004)).

(2) Spoliation sanctions are imposed in Florida "to assure that the non-spoliator does not bear an unfair burden."

- *Reed v. Alpha Prof'l Tools*, 975 So. 2d 1202, 1204 (Fla. 4th DCA 2008).

(3) Another reason for spoliation sanctions is their "deterrent effect on miscreant defendants."

- *Perez v. La Dove, Inc.*, 964 So. 2d 777, 780 (Fla. 3d DCA 2007).

(4) Under Florida law, spoliation is established when the party seeking sanctions proves that: (i) the evidence existed at one time, (ii) the alleged spoliator had a duty to preserve the evidence, and (iii) the evidence was crucial to the movant's prima facie case or defense.

- *Golden Yachts, Inc. v. Hall*, 920 So. 2d 777, 781 (Fla. 4th DCA 2006).

(5) However, some Florida courts may be willing to impose penalties for spoliation of evidence even where no duty existed:

- *Osmulski v. Oldsmar Fine Wine, Inc.*, 93 So. 3d 389 (Fla. 2d DCA 2012) (finding that where no statutory duty to preserve, if an injured party made a written request to preserve evidence or the injured party's claims were reasonably foreseeable, then an adverse inference instruction may be appropriate).

- *Golden Yachts, Inc. v. Hall*, 920 So. 2d 777 (Fla. 4th DCA 2006) (unlike the presumption of negligence which may arise under *Public Health Trust v. Valcin*, 507 So. 2d 596 (Fla. 1987), the adverse inference concept is not based on a strict legal "duty" to preserve evidence. Rather, an adverse inference may arise in any situation where potentially self-damaging evidence is in the possession of a party and that party either loses or destroys the evidence).

- *Martino v. Wal-Mart Stores, Inc.*, 835 So. 2d 1251, 1257 (Fla. 4th DCA 2003) (fact that plaintiff showed Wal-Mart the defective cart prior to lawsuit and asked Wal-Mart to keep it safe is not sufficient to create a duty to preserve, but is sufficient for the jury to make an adverse inference based upon the cart's loss).

c. Intent. Florida state courts are inconsistent as to whether the intent of the spoliator is relevant to the imposition of sanctions.

- *Sponco Mfg., Inc. v. Alcover*, 656 So. 2d 629, 630 (Fla. 3d DCA 1995) ("what sanctions are appropriate when a party fails to preserve evidence in its custody depends on the willfulness or bad faith, if any, of the party responsible for the loss of the evidence, the extent of prejudice suffered by the other party or parties, and what is required to cure the prejudice") (citations omitted).

- *Sponco Mfg., Inc. v. Alcover*, 656 So. 2d at 631 (Fla. 3d DCA 1995) (however, "[a] determination of willful destruction [is] not imperative" where plaintiff can convince the trial court that, in the absence of the crucial evidence, the plaintiff is no longer able to proceed with the cause of action).

- *But see, Fleury v. Biomet, Inc.*, 865 So. 2d 537 (Fla. 2d DCA 2003) (court held that although the destruction of an artificial knee deprived plaintiff of his ability to prove the causation element of his cause of action, because there was no willful, bad-faith destruction on the part of the defendant, spoliation sanctions were not appropriate).

- *Wilson v. Wal-Mart Stores, Inc.*, 2008 WL 4642596, at *2 (M.D. Fla. Oct. 17, 2008) ("a party is not guilty of spoliation when it destroys documents as part of its regular business practices and is unaware of their potential relevance to litigation").

d. Third-party Spoliation. There is however an independent cause of action for spoliation by a third party under Florida law.

- *Builder's Square, Inc. v. Shaw*, 755 So. 2d 721 (Fla. 4th DCA 1999).

e. Florida Standard Jury Instructions. On October 15, 2012, the Florida Supreme Court published a notice seeking comments on a new jury instruction regarding spoliation. The deadline for public comments regarding the new instruction was November 15, 2012.

- *Proposed Jury Instruction 301.11* – Failure to Maintain Evidence or Keep Record.

- *See* Appendix A for *Proposed Jury Instruction 301.11*.

2. **Federal Law on Spoliation**

a. Florida Rules. Florida federal courts have tended to follow state courts:

- *Swofford v. Eslinger*, 2009 U.S. Dist. Lexis 111064 (M.D. Fla. 2009) ("Federal law governs the imposition of spoliation sanctions, but the Court's opinion may be 'informed' by state law, as long as it is consistent with federal law").

b. Definition. Florida federal courts define spoliation just as Florida state courts:

- *Optowave Co. v. Nikitin*, No. 6:05-cv-1083-Orl-22DAB, 2006 WL 3231422 at *7 (M.D. Fla. Nov. 7, 2008) (*quoting Black's Law Dictionary 1437* (8th ed. 2004)) ("spoliation" is the "intentional destruction, mutilation, alteration, or concealment of evidence").

c. Spoliation Established.

- *Flury v. Daimler Chrysler Corp.*, 427 F.3d 939, 944 (11th Cir. 2005) (in addition to the factors applied by Florida courts, the Eleventh Circuit has indicated that sanctions for spoliation are appropriate only where there is evidence of bad faith).

- *Swofford v. Eslinger*, 671 F. Supp. 2d 1274 (M.D. Fla. 2009) (bad faith spoliation was found where sheriff's deputies turned in their laptops pursuant to the department's computer recycling policy knowing that the information would be deleted; adverse inference, rebuttable presumption and attorneys' fees and costs awarded as a result of the spoliation).

d. Sanctions for Spoliation of Social Media. Courts have imposed significant sanctions against attorneys and their clients for spoliation of evidence.

- *See Gatto v. United Airlines, Inc.*, 2013 U.S. Dist. LEXIS 41909 (D. N.J. Mar. 25, 2013) (allowing adverse inference instruction to jury where party deleted Facebook® page in personal injury action).

- *Lester v. Allied Concrete Co., supra*, pg. 15 (awarding significant sanctions for lawyer misconduct and spoliation of Facebook® evidence).

- *Calvert v. Red Robin Intern., Inc.*, No. C 11-03026 WHA, U.S. Dist. LEXIS 66476 (N.D. Cal. May 11, 2012) (imposing sanctions of over $15,000 on plaintiff for the plaintiff's willful failure to produce certain Facebook® records).

- *Patel v. Havana Bar, Rest. and Catering*, U.S. Dist. LEXIS 139180 (E.D. Pa. Dec. 5, 2011) (acknowledging that the plaintiff had an affirmative duty to preserve Facebook® witness statements and sanctioning the plaintiff by giving an adverse inference instruction, allowing re-deposition of witnesses at the plaintiff's expense and reasonable attorneys' fees and costs).

- *Torres v. Lexington Ins. Co.*, 237 F.R.D. 533 (D.P.R. 2006) (sanctioning the plaintiff for spoliation of evidence after the plaintiff intentionally deleted webpages that proved contrary to her claims for emotional damages).

e. Sanctions for Use of Cleaners. Courts have also awarded varying sanctions for a party's use of cleaners which spoliated evidence.

- *See Multifeeder Tech. Inc. v. British Confectionary Co.*, 2012 U.S. Dist. LEXIS 132619 (D. Mn. Sept. 18, 2012) (sanctioning party $600,000 based in part on a party's intentional use of CCleaner to clean and wipe computer files).

- *Taylor v. Mitre Corp.*, 2012 U.S. Dist. LEXIS 163854 (E.D. Va. Sept. 10, 2012), upheld by 2012 U.S. Dist. LEXIS 161318 (E.D. Va. Nov. 8, 2012) (finding that a plaintiff's use of Evidence Eliminator and CCleaner while in litigation constituted willful spoliation and sanctioned the plaintiff by dismissing the case, awarding fees and costs to the defendant as a result of the spoliation).

- *Ameriwood Indus. Inc. v. Liberman*, 2007 U.S. Dist. LEXIS 74886 (E.D. Mo. July 3, 2007) (awarding default judgment to plaintiff and fees and costs because of defendant's intentional use of "Window Washer" scrubbing software to scrub and/or delete files from computer).

- *Arista Records, LLC v. Tschirhart*, 241 F.R.D. 462, 466 (W.D. Tex. 2006) (granted default judgment and awarded fees and costs incurred related to sanctions motion against defendant who willfully destroyed evidence by installing data-wiping software).

- *Communication Center, Inc. v. Hewitt*, 2005 U.S. Dist. LEXIS 10891 (E.D. Cal. April 5, 2005) (recommending default against defendant for use of Evidence Eliminator software and awarding attorneys' fees and costs in the amount of $145,811.75).

- *Kucala Enters. v. Auto Wax Co.*, 2003 U.S. Dist. LEXIS 8833 (N.D. Ill. May 27, 2003) (dismissing plaintiff's lawsuit and awarding defendant attorneys' fees and costs from the date the plaintiff's first use of Evidence Eliminator).

- *But see Coburn v. PN II*, 2010 U.S. Dist. LEXIS 110613 (D. Nev. Sept. 30, 2010) (finding that use of CCleaner alone without other evidence is insufficient to conclude a destruction of evidence occurred).

3. **Range of Penalties for Spoliation**

a. Courts have used a wide variety of sanctions in response to e-discovery violations: evidence preclusion, witness preclusion, disallowance of certain defenses, reduced burden of proof, removal of jury challenges, limiting closing statements, supplemental discovery, additional access to computer systems, payments to bar associations to fund educational programs, participation in court-created ethics programs, referrals to the state bar, payments to the clerk of court, and barring the sanctioned party from taking additional depositions.[3]

b. Additional sanctions include:

(1) Monetary Sanctions.

- *See Simon Prop. Group, Inc. v. Lauria*, 2012 U.S. Dist. LEXIS 184638 (S.D. Fla. Dec. 13, 2012) (allowing an award of attorneys' fees and costs as sanction for party's spoliation of electronically-stored information on a laptop).

- *Lester v. Allied Concrete Co.*, 83 Va. Cir. 308, 2011 Va. Cir. LEXIS 245 (Sept. 2011); 83 Va. Cir. 308, 2011 Va. Cir. LEXIS 132 (Oct. 2011).

[3] Dan H. Willoughby, Jr., Rose Hunter Jones, and Gregory R. Antine, *Sanctions for E-discovery Violations: By the Numbers*, Duke Law Journal, 60 Duke L.J. 789 (December 2010)

(Sanctioning attorney and attorney's client in the amount of $720,000 for lawyer's instruction to clean up Facebook® page and client's subsequent spoliation of Facebook® photos).

- *Kipperman v. Onex Corp.*, 260 F.R.D. 682, 700 (N.D. Ga. 2009) (defendant's failure to comply with court's order regarding production of e-mails on backup tapes (as well as issues with defendant's responses to interrogatories) resulted in monetary sanctions in the amount of $1,022,700).

(2) Exclusion of Expert Testimony.

- *See Vanliner Ins. Co. v. ABF Freight Systems*, 2012 U.S. Dist. LEXIS 30676 (M.D. Fla. Mar. 8, 2012) (stating that in the Eleventh Circuit, appropriate sanctions for spoliation of evidence includes exclusion of expert witness testimony) (*citing Flury v. Daimler Chrysler Corp.*, 427 F.3d 939, 944 (11th Cir. 2005).

- *Unigard Sec. Ins. Co. v. Lakewood Engineering & Mfg. Corp.*, 982 F.2d 363, 369 (9th Cir. 1992) (where space heater that caused yacht fire was destroyed by insurance company, the court excluded the testimony of plaintiff's expert regarding the heater as a sanction for spoliation).

(3) Adverse Inference Jury Instruction

- *Southeastern Mechanical Services, Inc. v. Brody*, 657 F. Supp. 2d 1293 (M.D. Fla. 2009) (where testimony of computer experts suggested that defendants had deleted the contents of their Blackberries and laptops after being given notice to preserve the information, the court found an adverse inference jury instruction was appropriate).

- *Optowave Co., Ltd., v. Nikitin*, 2006 U.S. Dist. LEXIS 81345 (M.D. Fla. Nov. 7, 2006) (imposing sanction of adverse inference for spoliation of important e-mails as well as attorneys' fees and costs).

- *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, Case No. 502003CA005045XXO-CAI (Fl. Cir. Ct. 2005) (showing an adverse inference can be a devastating sanction, Judge Elizabeth T. Maass granted plaintiff's motion for an adverse inference instruction due to Morgan Stanley's destructions of e-mails and Morgan Stanley's noncompliance with the court's order to search backup tapes for 36 Morgan Stanley employees involved in relevant transactions and review a serious of e-mails containing 29 specified search terms, as well as produce all non-privileged e-mails responsive to plaintiff's document requests. The jury in that case then awarded plaintiff $1.45 billion).

(4) Dismissal of Offending Party's Claim.

- *United States ex rel. King v. Dse, Inc.*, 2013 U.S. Dist. LEXIS 22245 (M.D. Fla. Jan. 17, 2013) (granting dismissal of claim with prejudice as against relator for loss of video diaries and failing to back up evidence).

- *Kvitka v. Puffin Co., LLC*, 2009 WL 385582 (M.D. Pa. 2009) (where plaintiff destroyed her laptop after being instructed by defendant to preserve e-mail files on it, court affirmed spoliation sanction of dismissal of plaintiff's claim).

(5) Default Judgment Against Offending Party.

- *See Simon Prop. Group, Inc. v. Lauria*, 2012 U.S. Dist. LEXIS 184638 (S.D. Fla. Dec. 13, 2012) (entering a "default" as opposed to a "default judgment" against the spoliating party).

- *Keene v. Brigham and Women's Hospital, Inc.*, 786 N.E.2d 824 (Mass. 2007) (court entered default judgment in favor of plaintiff where hospital failed to produce records relating to newborn infant's care over a 20-hour period and hospital could not show that losing the records was through no fault of its own).

(6) Imprisonment.

- *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 2010 WL 3530097 (D. Md. Sept. 9, 2010) (chief magistrate recommended to the judge a default judgment against defendant and ordered up to two years of imprisonment for its president as sanctions for their electronic discovery misconduct).

D. ETHICAL DO'S AND DON'TS OF USING SOCIAL MEDIA

1. By Attorneys Surveilling Clients, Witnesses and Opposing Parties: Friending Concerns

a. Communication with Persons Represented by Counsel – **Fla. Bar R. Prof. Conduct Rule 4-4.2**:

> In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer. Notwithstanding the foregoing, an attorney may, without such prior consent, communicate with another's client in order to meet the requirements of any court rule, statute or contract requiring notice or service of process directly on an adverse party, in which event the communication shall be strictly restricted to that required by the court rule, statute or contract, and a copy shall be provided to the adverse party's attorney.

- *See infra, The Philadelphia Bar Ass'n Prof'l Guidance Comm., Op. 2009-02* (March 2009); *SDCBA Legal Ethics Opinion 2011-2*. A lawyer or its legal staff friending an opposing party on Facebook® that the lawyer knows to be represented by counsel could violate Rule 4.2.

b. Responsibility Regarding Non-Lawyer Assistance – **Fla. Bar R. Prof. Conduct Rule 4-5.3**:

(b)With respect to a nonlawyer employed or retained by or associated with a lawyer or an authorized business entity as defined elsewhere in these Rules Regulating The Florida Bar:
(1) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
(2) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
(3) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
(A) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
(B) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.
(c) Ultimate Responsibility of Lawyer**.** Although paralegals or legal assistants may perform the duties delegated to them by the lawyer without the presence or active involvement of the lawyer, the lawyer shall review and be responsible for the work product of the paralegals or legal assistants.

c. Misconduct – **Fla. Bar R. Prof. Conduct Rule 4-8.4**:

A lawyer shall not: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;…(c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation, except that it shall not be professional misconduct for a lawyer for a criminal law enforcement agency or regulatory agency to advise others about or to supervise another in an undercover investigation, unless prohibited by law or rule, and it shall not be professional misconduct for a lawyer employed in a capacity other than as a lawyer by a criminal law enforcement agency or regulatory agency to participate in an undercover investigation, unless prohibited by law or rule;

- *The Philadelphia Bar Ass'n Prof'l Guidance Comm., Op. 2009-02* (March 2009). In 2009, the Philadelphia Bar Association's Professional Guidance Committee (the "PBAPG Committee") issued an opinion regarding an attorney's proposed method of gaining access to a witness's Facebook® and MySpace™ accounts. The attorney deposed the witness and found out the witness maintained Facebook® and MySpace™ accounts. Believing that the witness might be posting useful information relevant to her deposition on these websites, the attorney visited her Facebook® and MySpace™ accounts and attempted to gain access. However, the attorney discovered that to access the accounts, he would have to "friend" the witness who could then decide whether to grant him access or not. The attorney believed that if he identified himself and asked the witness to "friend" him, she would deny his request. Therefore, the attorney sought the PBAPG Committee's opinion as to whether the following proposed course of action would violate any ethical rules. The attorney proposed that he would ask a third person, a person whose name the witness would not recognize, to go to her Facebook® and MySpace™ pages and ask her to "friend" him. The person would state only truthful information to the witness, i.e., his real name, but would not reveal that he is affiliated with the attorney. If the witness "friended" the third person, the third person would provide the attorney with the information the witness was posting on her Facebook® and MySpace™ pages. The PBAPG Committee found that the attorney's proposed course of action could violate various state ethics rules. For example, the PBAPG Committee found that that proposal could violate:

  - Rule 8.4 (Misconduct) because it is inherently deceptive as the plan purposely omits the key fact to the witness that the third party is only seeking to "friend" her so that he can obtain information for the attorney.
  - Rule 4.2 (Communication with Person Represented by Counsel).
  - Rule 4.3 (Dealing with Unrepresented Person)
  - Rule 4.1 (Truthfulness in Statements to Others); and
  - Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants).

- *The Ass'n of the Bar of the City of New York Comm. on Prof. Ethics, Formal Op. 2010-2* (September 2010). In 2010, in a similar opinion of its own, the New York City Bar Association Committee on Professional Ethics ("NYCBA Committee") echoed the PBAPG Committee's opinion, stating that neither attorneys nor their agents were permitted to "friend" potential witnesses under false pretenses. The NYCBA Committee did state, however, that lawyers and their agents were permitted to "friend request" potential witnesses so long as they used only truthful information to obtain the access. The opinion stated, "[a]n attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website[.]" A key distinction between the PBAPG Committee's and NYCBA Committee's opinions is that the NYCBA Committee opinion states that the lawyer or her agent has no duty to disclose to the party the reasons for making the request. While New York Professional Conduct Rules 4.1 and 8.4(c) are nearly identical to those of

Pennsylvania, the NYCBA Committee finds that the fact that the attorney or his agent seeks information to be used in the course of litigation is not a necessary ethical disclosure.

- *The New York State Bar Ass'n Comm. on Prof. Ethics, Opin. #843* (September 10, 2010). Also, in September 2010, the New York State Bar Association ("NYSBA") issued a second opinion on the issue of whether an attorney can ethically access public social network pages of an opposing party for the purpose of obtaining possible impeachment evidence for use in litigation. In that opinion, the NYCBA concluded that there was no ethical issue for an attorney who accesses public social network information that is available to the public domain for viewing. However, the opinion notes that "as long as the lawyer does not 'friend' the other party or direct a third party to do so" there would be no violations of the ethics rules. This analysis is directly in line with its *Formal Opinion 2010-2* cited above.

- *SDCBA Legal Ethics Opinion 2011-2.* In May 2011, the San Diego County Bar Legal Ethics Committee ("SDCBA Committee") issued an opinion as to whether an attorney violated the ethical rules when he "friended" two high-ranking employees of the adverse party whom his client believed would have negative information about the employer on their social media profiles. The lawyer knew the high-ranking employees were represented by corporate counsel. The opinion found that the lawyer's conduct violated the rules. The opinion went on to note that the rule (Rule 4.2) prohibits the attorney from making an *ex parte* "friend request" of a represented party. The SDCBA Committee further found "friending" an unrepresented third party without disclosing the purpose of the friend request would violate the lawyer's duty not to deceive (Rule 8.4).

- *Oregon State Legal Ethics Comm., Formal Ops. 2005-164* (August 2005) and *2005-173* (August 2005). However, the Oregon State Bar ("OSB") seemingly takes a different view on the permissibility of "misrepresentation and subterfuge" by attorneys. In an August 2005 opinion addressing ethically permissible conduct by an attorney with respect to an adversary's website, the OSB states that information on publicly available websites, or even websites for which a membership or subscription is required, is fair game because it is no different than "reading a magazine article or purchasing a book written by the adversary." The opinion warns, however, that a lawyer may not communicate through the Internet with a represented adversary, as doing so would violate the lawyer's ethical duty.

    - Significantly, in footnote 1 of the opinion, the OSB writes, "[w]e express no opinion concerning access to Web sites involving or obtained through the use of deception. *Cf*. OSB Formal Ethics Op No 2005-173."

    - A review of the opinion referenced in footnote 1 shows that the OSB rules, like the Model Rules, prohibit an attorney from engaging in "conduct involving dishonesty, fraud, deceit or misrepresentation that reflects adversely

on the lawyer's fitness to practice law[.]" However, unlike the Model Rules, the OSB rules further state:

> [Notwithstanding certain provisions of the Oregon Code] it shall not be professional misconduct for a lawyer to advise clients or others about or to supervise lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights, provided the lawyer's conduct is otherwise in compliance with these Rules of Professional Conduct. **"Covert activity," as used in this rule, means an effort to obtain information on unlawful activity through the use of misrepresentations or other subterfuge. "Covert activity" may be commenced by a lawyer or involve a lawyer as an advisor or supervisor only when the lawyer in good faith believes there is a reasonable possibility that unlawful activity has taken place, is taking place or will take place in the foreseeable future.**

- The OSB interprets this to mean that the lawyer must have some rational basis for his belief that an "unlawful activity" has, is or will take place. An "unlawful activity" is defined as "violations of civil law, criminal law, or constitutional rights." Further, it states that civil law "clearly encompasses both statutory and common-law duties, including duties imposed by tort or contract law. 'Civil law' duties regulate both intentional violations and reckless or negligent breaches of civil standards. It is not, however, reasonable to conclude that a 'violation' of 'civil law' refers to a situation in which no breach of any recognized duty is evident or alleged."

- The opinion suggests that, so long as the attorney has a rational basis to believe the investigation relates to unlawful conduct and so long as they do not otherwise violate the Rules of Professional Conduct (for example, by friending a represented party and thereby "communicating" with them in violation of the rules), he or she may use "misrepresentations and subterfuge" to try to obtain informal discovery.

- In August 2012, two New Jersey defense attorneys were charged by the New Jersey Office of Attorney Ethics for violating numerous ethics rules (Rules 4.2, 5.3, 8.4) when their paralegal friended, using her real name, the opposing party who was represented. As of April 12, 2013, we could not locate any decision as to potential discipline for these attorneys based on the ethics charges.

2. **By Attorneys Researching or Monitoring Jurors**

a. Competence and Diligence. Does a lawyer have an ethical obligation to research and learn about jurors on social networking sites who could be on their jury panel?
(1) Competence – **Fla. Bar R. Prof. Conduct Rule 4-1.1 (2013)**:

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

(2) Diligence – **Fla. Bar R. Prof. Conduct Rule 4-1.3 (2013)**:

A lawyer shall act with reasonable diligence and promptness in representing a client.

- The comments suggest that "a lawyer should pursue a matter on behalf of a client despite opposition, obstruction, or personal inconvenience to the lawyer and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor. A lawyer must also act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf."

- *See also The New York State Bar Ass'n Formal Opinion 2012-2* (stating that "standards of competence and diligence may require doing everything reasonably possible to learn about the jurors who will sit in judgment on a case").

- *Johnson v. McCullough*, 306 S.W.3d 551, 558-59 (Mo. 2010) (a Missouri Supreme Court opinion raises the issue of an attorney's duty, in the course of zealous representation of a client, to research potential jurors online. In *McCullough*, the court admonished an attorney for failing to perform an Internet search on a juror. The juror had stated that they had never been a party to a non-family law litigation when, in fact, the juror had been party to several debt collection suits as well as a personal injury suit).

- *Carino v. Muenzen*, 2010 N.J. Super. Unpub. LEXIS 2154, at *27 (N.J. Sup. Ct. App. Div. Aug. 30, 2010) (the trial court prohibited the plaintiff's attorney from using a computer during jury selection to perform research on prospective jurors based on defendant's objection. The Supreme Court of New Jersey held that the trial judge "acted unreasonably" in prohibiting the attorney from researching the potential jurors on the Internet).

- *But see De La Rosa v. Zequeira*, 659 So. 2d 239, 242 (Fla. 1995) (*citing De La Rosa v. Zequeira*, 627 So. 2d 531, 534 (Fla. Cir. Ct. 1993) (Baskin, J., dissenting)) (holding that an attorney may rely on the potential juror's duty of honesty, and refusing to impose a duty on attorneys to conduct independent fact-confirming research).

- *But see also Roberts v. Tejada*, 814 So. 2d 334, 344-345 (Fla. 2002) (due diligence does not require lawyer to perform a lawsuit index search on jurors prior to the conclusion of jury selection).

- *See also In Re: State of New Jersey Through the ESSEX COUNTY PROSECUTOR'S OFFICE, Compelling the Jury Manager to Provide Information on Prospective Jurors* (February 27, 2012) (rejecting a prosecutor's request for birth dates of potential jurors to perform background checks).

3. **By Attorneys Communicating with Jurors**. The Florida Bar Rules allow lawyers to contact jurors after trial with certain restrictions. However, researching jurors prior to or currently empanelled is a bigger problem and can trigger the professional rules of conduct. Essentially, lawyers should have no contact with jurors. This includes no friending jurors or prospective jurors or otherwise inviting to share information through social media.

   a. **Fla. Bar R. Prof. Conduct Rule 4-3.5(d)**:

   A lawyer shall not:
   (1) before the trial of a case with which the lawyer is connected, communicate or cause another to communicate with anyone the lawyer knows to be a member of the venire from which the jury will be selected;
   (2) during the trial of a case with which the lawyer is connected, communicate or cause another to communicate with any member of the jury;
   (3) during the trial of a case with which the lawyer is not connected, communicate or cause another to communicate with a juror concerning the case;
   (4) after dismissal of the jury in a case with which the lawyer is connected, initiate communication with or cause another to initiate communication with any juror regarding the trial except to determine whether the verdict may be subject to legal challenge; provided, a lawyer may not interview jurors for this purpose unless the lawyer has reason to believe that grounds for such challenge may exist; and provided further, before conducting any such interview the lawyer must file in the cause a notice of intention to interview setting forth the name of the juror or jurors to be interviewed. A copy of the notice must be delivered to the trial judge and opposing counsel a reasonable time before such interview. The provisions of this rule do not prohibit a lawyer from communicating with members of the venire or jurors in the course of official proceedings or as authorized by court rule or written order of the court.

   - *See New York City Bar Ass'n Committee on Professional Ethics Formal Opinion 2012-2* (June 4, 2012). In 2012, the NYCBA issued a Formal Opinion regarding jury research and social media. The opinion concluded that it is ethically permissible for an attorney to use social media to research jurors so long as no communication is made with the juror under its Rule 3.5. While the NYCBA looked at one other opinion on the matter, the NYCBA noted that the main issue is what constitutes a communication. The NYCBA stated that whether research conducted constitutes a communication would depend on, "in part on, among other things, the technology, privacy settings and mechanics of each service." The

NYCBA decided that the following would constitute inappropriate communications with jurors even if inadvertent: 1) friending the juror or inviting the juror to share information on a social network; or 2) a juror learning that an attorney viewed or attempted to view the juror's social media. (For example, LinkedIn® allows its users to see who has viewed their profiles.) Significantly, the NYCBA did not take a position as to whether an inadvertent communication would in fact be a violation. The NYCBA advised that lawyers should "understand the functionality of any social media service" used for juror research.

- *See New York City Lawyers Ass'n Committee on Professional Ethics Formal Opinion 743* (May 18, 2011). In 2011, the New York City Lawyers Association Committee on Professional Ethics ("NYCLA Committee") issued a Formal Opinion on juror research and similarly found that lawyers are permitted to research jurors at the pretrial stage as well as during the trial to monitor for misconduct. The NYCLA Committee cautioned that while lawyers can review social media sites on jurors, the lawyers should not communicate with jurors through friending, subscribing to their Twitter accounts, sending Tweets or otherwise. The NYCLA Committee similarly found that such research may implicate its counterpart equivalent to the Fla. Bar R. Prof. Conduct 4-3.5(d). The NYCLA Committee found the following examples to be communication in violation of Rule 3.5: "sending a 'friend request'; attempting to connect on LinkedIn®; signing up for an RSS feed for a juror's blog or 'following' a juror's Twitter account."

b. **Fla. Bar R. Prof. Conduct Rule 4-8.4:**

A lawyer shall not: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;…(c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation, except that it shall not be professional misconduct for a lawyer for a criminal law enforcement agency or regulatory agency to advise others about or to supervise another in an undercover investigation, unless prohibited by law or rule, and it shall not be professional misconduct for a lawyer employed in a capacity other than as a lawyer by a criminal law enforcement agency or regulatory agency to participate in an undercover investigation, unless prohibited by law or rule;

- *New York City Bar Ass'n Committee on Professional Ethics Formal Opinion 2012-2* (June 4, 2012). In its Formal Opinion 2012-2, the NYCBA also stated that an attorney cannot use deceptive practices when researching jurors. Similar to the decisions on friending Facebook® users under false pretenses, etcetera, a lawyer cannot use such practices to obtain access to juror social media information. This is true even for third parties. The lawyer cannot direct a non-lawyer or third party to do what the lawyer cannot do. *See Fla. Bar R. Prof. Conduct 4-5.3*; *ABA Model R. Prof. Conduct 5.3*.

c. The no-contact rule does not prevent lawyers from ethically performing passive monitoring of empanelled jurors to verify the absence of misconduct. Monitoring jurors during trial has become an important issue as many cases have had fatal results due to juror misconduct and/or jurors improperly researching and/or discussing cases.

- Both the U.S. District Federal Courts and Florida Supreme Court on Standard Jury Instructions Committee have proposed updated jury instructions to emphasize a juror's obligation not to discuss or engage in research of the case in the hopes to avoid the improper juror conduct in a technology-driven era.

- In August 2012, the Judicial Conference Committee on Court Administration provided an updated proposed Model Jury Instruction entitled *The Use of Electronic Technology to Conduct Research on or Communicate about a Case* that specifically focused on jurors' use of social media networks. The instruction identified numerous social media networks and advised the jurors about the implications of using these technological outlets to engage in improper research or communications about the cases to which they are empanelled. See **Appendix B** with the proposed jury instruction.

- On October 21, 2010, the Florida Supreme Court adopted new and amended standard jury instructions for both criminal and civil cases on juror use of electronic devices. The instructions advise jurors not to discuss the case through electronic communications, such as blogs, tweeting, e-mail or text messages, etcetera. *See SC10-51 – In Re: Standard Jury Instruction in Criminal Cases-Report No. 2010-01 and Standard Jury Instructions in Civil Cases-Report No. 2010-01* available at:
  http://www.floridasupremecourt.org/decisions/2010/sc10-51.pdf.

d. Juror misconduct and improperly researching or posting about cases has resulted in significant consequences for cases. For example, in the last few years, juror use of social media has resulted in verdicts being overturned and mistrials.

- In January 2013, Middle District of Florida Judge James Moody ordered seizure of a jury forewoman's computer to determine whether there was any juror misconduct and/or research of the case during the trial. The Defendant is seeking a new trial based on alleged juror misconduct. The court is still conducting evidentiary hearings to determine juror misconduct was present. *See U.S. v. Myrie*, Case No. 8:09-cr-572-T30TGW (M.D. Fla. January 8, 2013).

- In late 2012, the Suffolk (Massachusetts) Superior Court dismissed a juror who researched "ballistics" during murder trial, requiring the jury deliberations to start anew.

- *Sluss v. Commonwealth*, 381 S.W.3d 215 (Ky. Sept. 20, 2012) (Supreme Court of Kentucky granted a defendant post-trial hearings following his convictions to inquire further if two jurors failed to disclose they were friends on Facebook®).

- *State v. Abdi*, 2012 VT 4, 2012 Vt. LEXIS 5 (Vt. Jan. 26, 2012) (Vermont Supreme Court overturned a child sexual abuse conviction because a juror had conducted cultural research of the alleged crime in the defendant's culture).

- *See Dimas-Martinez v. State*, 2011 Ark. 515 (Ark. 2011) (similarly, the Arkansas Supreme Court overturned a murder conviction because a juror tweeted during the trial even after receiving prior reprimands by the court not to do so).

4. **For Judges Using Social Media**

   a. ***Fla. Supreme Court Judicial Ethics Advisory Committee Opinion No. 2009-20* (November 17, 2009).** In this opinion, the JEA Committee addressed four questions regarding a judge's use of social media; however, the most important question being "whether a judge may add lawyers who appear before the judge as 'friends' on a social networking site, and permit such lawyers to add the judge as their "friend." The JEA Committee concluded that it is a violation of Canon 2B for a judge to "friend" attorneys who may appear before them or allow attorneys who may appear before them to "friend" the judge. Canon 2B provides, "a judge shall not lend the prestige of judicial office to advance the private interests of the judges or others; nor shall a judge convey or permit others to convey the impression that they are in a special position to influence the judge." Further, the JEA Committee notes that a judge's use of social media must conform to the requirements of Canon 5A on extrajudicial activities. From the JEA Committee's perspective, a judge having lawyers who may appear before him or her conveys to others that the lawyer may have a special influence on the judge.

   b. ***Fla. Supreme Court Judicial Ethics Advisory Committee Opinion No. 2010-04* (March 19, 2010).** Following the JEA Committee's decision in 2009 prohibiting judges from friending lawyers on social media networks, an inquiry was posed whether a judge's judicial assistant is prohibited from adding lawyers who may appear before a judge as "friends" on social networking sites. The JEA Committee answered this question in the negative. The JEA Committee held that a judicial assistant may friend lawyers that may appear before the judge as long as it is done independently of the judge, and the judge or judge's office is not referenced. In other words, the JEA Committee concluded that Jane Smith, Judge XYZ's assistant, is not precluded from adding lawyers who may appear before Judge XYZ to her own individual social networking site. The JEA Committee's decision is based on the longstanding precedent that judicial assistants are not bound by the Code of Judicial Conduct. However, the opinion does caution judges that while judicial assistant's may have their own personal social media sites, the judge may have a responsibility under Canon 3C(2) to "require staff, court officials and others subject to the judge's direction and control to observe the standards of fidelity and diligence that apply to the judge…." Thus, for example, if a lawyer attempts to make an *ex parte* communication through the social networking site, the judicial assistant must report it

and the judge should instruct the assistant to immediately disassociate or de-friend the lawyer.

c. ***Fla. Supreme Court Judicial Ethics Advisory Committee Opinion No. 2010-06*** **(March 26, 2010).** In this opinion, the JEA Committee addressed whether a judge who is a member of a voluntary bar association must de-friend lawyers who are also members of the organization's Facebook® page or use Facebook® to communicate about the organization. The JEA Committee concluded that a judge did not have to de-friend members of the voluntary bar association and noted that it is the organization that controls the Facebook® page and the acceptance and rejection of friend posts, not a judge.

- In addition, the JEA Committee was again posed with circumstances surrounding judges friending lawyers or accepting friend requests from lawyers that practice before them. One inquiry was whether a disclaimer that the term "friend" did not mean a close personal friend in a traditional sense. The JEA Committee affirmatively held that a disclaimer would be ineffective to prevent the impression of an improper influence. Thus, judges are not permitted to use disclaimers as a way to avoid violating Canon 2B.

- The JEA Committee also re-affirmed its decision in Opinion No. 2009-20 that judges are prohibited from friending attorneys or accepting friend requests from attorneys that practice before them. After much debate by the minority opinion, the majority opinion held that it correctly decided that "judges cannot accept requests from lawyers who appear before them" as friends or recognized contacts on social media sites.

d. ***American Bar Association Formal Opinion 462*** **(Feb. 21, 2013).** At issue in this opinion was whether a judge may participate in social networking. The ABA concluded that a judge can use social networking so long as the judge ensures compliance with the Model Code of Judicial Conduct. The ABA pointed out specific rules that may be triggered by a judge's use of social media. For example, the ABA noted that use of social media should not form relationships with persons or organizations that may influence the rule, as governed by MRJC 2.4(C). Also, judges should use caution that comments or posts are not interpreted as *ex parte* communications in violation of MRJC 2.9(A). Further, the ABA cautioned that a judge's use of social media should refrain from commenting on pending matters pursuant to MRJC 2.10 and should not give legal advice (MRJC 3.10).

- For judges who do have connections with attorneys or parties on social media networks, the judges should carefully evaluate the relationship and determine whether disclosure of the relationship is necessary "prior to, or at the initial appearance of the person before the Court." However, the ABA emphasizes that this does not require a judge to search all of the judge's social media relationships where the judge is without specific knowledge of a relationship that may pose problematic or be in derogation of the judicial canons.

5. **For Mediators Who Use Social Media Sites**

    a. ***Florida Mediator Ethics Advisory Committee, Opinion MEAC 2010-001* (June 1, 2010).** The Mediator Ethics Advisory Committee addressed whether a certified mediator can designate mediation clients or attorneys as friends and allow attorneys to add the mediator as a friend. The MEAC concluded that a mediator may ethically add past mediation clients and attorneys as friends on a social networking site as well as allow attorneys to add the mediator as a friend on their social media sites. However, the MEAC cautioned mediators of their obligation to disclose potential conflicts of interests under Rules 10.340(a) & (b) of the Florida Rules for Certified and Court-Appointed Mediators. The MEAC did note that parties viewing the mediator's social networking sites or attorneys with friends of mediators on their social networking sites may view the "friendship" as a potential influence over the mediator, which could limit the clients with whom the mediator may provide services for in the future. Overall, the MEAC finds that it is ethically acceptable to allow such friendships on social networking sites, but reminds mediators of their obligations to disclose potential conflicts of interest and if all parties agree, the mediator may provide mediation services.

E. CONFIDENTIALITY AND CLOUD COMPUTING. The following are additional ethical considerations for attorneys when dealing with social media issues or other electronically stored information:

1. **Confidentiality of Information – Fla. Bar R. Prof. Conduct Rule 4-1.6 (2013):** "A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent."

    - *See In the Matter of Peshek*, No. 6201779, Comm. No. 09 CH 89 (Ill. August 25, 2009); *In re: Disciplinary Proceedings Against Kristine A. PESHEK, Attorney at Law: Office of Lawyer Regulation v. Kristine A. Peshek*, No. 2011AP909-D (Wis. June 24, 2011) (an Illinois public defender posted information about her clients on her blog. She was ultimately disbarred for 60 days for violating Rule 1.6, revealing client confidences, under Illinois Rule of Professional Conduct. Similarly, the Supreme Court of Wisconsin issued reciprocal discipline on this attorney for 60 days since she was a member of the Wisconsin bar as well).

2. **Use of Electronic Devices – *Professional Ethics of the Florida Bar, Formal Opinion 10-2 (*September 24, 2010).** This opinion addressed the ethical considerations lawyers face when they use devices, such as printers, copiers, fax machines, flash drives, etcetera, that contain internal hard drives. In the opinion, the Ethics Committee concluded that use of such devices may trigger Fla. Bar R. of Prof. Conduct 4-1.1 (Competence), 4-1.6 (Confidentiality) and 4-5.3 (Supervision of Non-Lawyer). More specifically, the opinion outlines the concerns that may arise as to the confidential information saved on devices with an internal hard drive if the lawyer later sells the equipment, returns it to a leasing company or disposes of it. From the Ethics Committee's perspective, disposal of such a

device could result in inadvertent disclosure of confidential client information in violation of Fla. Bar R. Prof. Conduct Rule 4-1.6. The opinion advises that lawyers should take all reasonable steps to protect confidentiality when using such devices. Further, a lawyer has a duty to obtain assurances that any electronic devices it wishes to dispose of are adequately stripped of any confidential client information.

3. **Wrongfully Obtained Electronic Documents – *Professional Ethics of the Florida Bar, Formal Opinion 07-1* (September 7, 2007).** The Ethics Committee addressed the issue of how to handle wrongfully obtained electronic documents. An attorney representing his client in a divorce proceeding received documents that his client had taken from her spouse's computer and office. The attorney did not review the documents and sought an opinion from the Ethics Committee as to what his obligations were to disclose or return the documents to opposing counsel. Since the disclosure was not the result of an inadvertent disclosure governed by Rule 4-4.4, the Ethics Committee concluded that it was a legal issue as to a lawyer's duty when receiving wrongfully obtained documents. However, the Ethics Committee suggested that there are still ethical obligations in such a scenario:

   a. The attorney is obligated by the duty of confidentiality under Rule 4-1.6. and cannot reveal the information relating to representation without the client's consent.

   b. The attorney cannot assist the client in conduct that is fraudulent or criminal as provided in Rule 4-1.2(d).

   c. Nor can the attorney engage in conduct that is dishonest or that will have a prejudicial impact on the administration of justice under Rules 4-8.4 (c) and (d).

   d. The lawyer cannot violate the ethics rules through the acts of another, including the client under Rule 4-8.4(a).

   e. Finally, under Rule 4-3.4(a), a lawyer may not prohibit or unlawfully obstruct another party's access to evidence or destroy or conceal evidence.

   In light of these ethical considerations, the Ethics Committee advised the attorney to take the following steps:

   - discuss the potential that the client may need criminal representation;

   - discuss with the client that the court may disqualify the attorney from representing him;

   - advise the client that the attorney may be subject to sanctions by the court, and

   - inform the client that the improperly obtained documents may not be retained, reviewed, or used without informing the opposing party that the attorney has the

documents in question and that the attorney must withdraw from representation if the client refuses to consent to such a disclosure.

4. **Metadata – *Professional Ethics of the Florida Bar, Formal Opinion 06-2* (September 15, 2006).** The opinion held that "a lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata." Rule 4-1.6 (Confidentiality). Further, a lawyer has an obligation not to view metadata it believes to have received inadvertently or knows it was not intended for the lawyer and inform the sender of its receipt of the metadata in accordance with Rule 4-4.4(b) (Inadvertent Disclosure).

   - *See also American Bar Association Formal Opinion 06-442* (August 5, 2006) on metadata.

5. **Cloud Computing Ethically Acceptable For Lawyer Practice.** Cloud computing is governed by the following Florida Bar professional rules of conduct:

   a. Rule 4-1.1 Competence;

   b. Rule 4-1.6 Confidentiality; and

   c. Rule 4-5.3 Responsibility Regarding Non-Lawyer Assistance.

   The main concern is client confidentiality and the security of confidential client information on lawyer's files maintained on the cloud.

   - *Professional Ethics of the Florida Bar Proposed Advisory Opinion 12-3* (January 25, 2013). On January 25, 2013, the Ethics Committee issued *Proposed Advisory Opinion 12-3* regarding the use of cloud computing. The Ethics Committee recognized that cloud computing is permissible; however, lawyers are cautioned to take reasonable precautions to ensure the confidentiality of client information. After reviewing other state opinions on cloud computing, the Ethics Committee agreed with the advice of the Iowa and New York state bars as to the types of precautions to take with respect to cloud computing. Those precautions are as follows:

     - Ensure that the provider will maintain confidentiality of the information and has an enforceable obligation to preserve the confidentiality of the client's information;

     - Research the service provider and consider its provider agreement, such as a governing law provision for disputes, whether the service provider retains the information if the lawyer terminates the relationship, or whether the agreement limits the provider's liability;

- Determine whether the information is password protected or encrypted or whether the lawyer can provide additional security measures to the information;

- Ensure that the lawyer will have adequate access to the client information and that others will not have access to the data; and

- Consider backing up remote- or cloud-saved data as a precaution.

Comments to the proposed advisory opinion were accepted until March 18, 2013. In addition, those attending the Florida Bar Annual Convention on June 28, 2013 may also have an opportunity to comment on the proposed advisory opinion.

F. COMPUTER LAWS THAT IMPACT THE USE OF TECHNOLOGY BY CLIENTS AND ATTORNEYS

1. **The Stored Communications Act, 18 U.S.C. §2701, *et seq*. ("SCA").** The SCA prohibits intentionally accessing stored communications without authorization or in excess of authorization. The SCA provides for a cause of action to remedy conduct constituting a violation. Those remedies include preliminary and other equitable and declaratory relief as may be appropriate, actual damages suffered by the plaintiff, any profits made by the violator as a result of the violation, punitive damages where appropriate (for willful or intentional violations), and a reasonable attorney's fee and other litigation costs reasonably incurred. The SCA also states that in no case shall a person entitled to recovery receive less than the sum of $1,000. 18 U.S.C. §2707. In addition, there are possible criminal penalties including a fine and imprisonment for up to 10 years. 18 U.S.C. §2701(b).

   a. Definition of electronic storage. "Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and any storage of such communication by an electronic communication services for purposes of backup protection of such communication." 18 U.S.C. §2510(A-B).

      - *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010) (social networking sites such as Facebook® and MySpace™ have been held to constitute electronic communications providers subject to the SCA).

   b. Accessing Electronic Communications: Performing searches of a party's personal e-mail or social media profiles may violate federal law.

      - *Snyder v. Fantasy Interactive, Inc.*, 2012 U.S. Dist. LEXIS 23087 (S.D.N.Y. Feb. 9, 2012) (holding that plaintiff stated a claim for violation of SCA where employer accessed plaintiff's private Skype instant messages outside of the office).

      - *Maremont v. Susan Fredman Design Grp.*, 2011 U.S. Dist. LEXIS 140446 (N.D. Ill. Dec. 7, 2011) (denying summary judgment on employee's claim for violation

of SCA when employer accessed employee's Facebook® and Twitter accounts without permission).

- *Shefts v. Petrakis*, No. 10-cv-1104, 2011 U.S. Dist. LEXIS *16 (C.D. Ill. Nov. 29, 2011) (stating that a party cannot avoid SCA liability by hiring a third party to access and copy stored electronic communications even if the files are not opened or read).

- *Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011) (finding that plaintiff sufficiently pled claim under SCA where defendant allegedly used key-logger software to access plaintiff's e-mail and financial accounts).

- *Miller v. Meyers*, 766 F. Supp. 2d 919 (W.D. Ark. 2011) (finding that a husband's use of key-logger software on to access ex-wife's e-mail violated the SCA).

- *Pietrylo v. Hillstone Restaurant Group*, 2008 WL 6085437 (D.N.J. 2008) (pressuring a third party for his or her password to gain access to a party's or witness's MySpace™ page or group violates the SCA).

c. Surveillance or research of a party: When researching or surveilling parties or witnesses, any "friending" of the person under false pretenses, or using someone else's social media profile to gain access to their private information may violate the SCA.

- *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-84 (9th Cir. 2002) (gaining access to a private group bulletin board by false pretenses violates the Federal Wiretap Act, the SCA and the Railway Labor Act).

2. **The Computer Fraud and Abuse Act, 18 U.S.C. §1030 ("CFAA").**

a. The CFAA prohibits the unauthorized access of a computer (or exceeding authorized access of a computer) and obtaining information. The statute focuses on whether a party's accessing of another party's computer was without authorization or exceeded any authorization which was granted. The CFAA provides both criminal penalties, including fines and imprisonment for up to 10 years (18 U.S.C. §1030(c)), and a civil cause of action for certain violations of the CFAA where compensatory damages and other injunctive or equitable relief may be granted. 18 U.S.C. §1030(g).

b. *See S.B. 3569 112th Cong.* (2012). The Cloud Computing Act of 2012 is currently pending before the U.S. Senate and, if passed, would extend the CFAA to include unauthorized access to cloud computing.

- *Eagle v. Morgan*, 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012) (employer's access to a former employee's LinkedIn® site that was associated with the employer may have violated the CFAA, but summary judgment granted

for the defendant because the plaintiff could not prove a cognizable loss as a result of the access).

- *Contrast Lee v. PMSI, Inc.*, 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011) (dismissing party's CFAA counterclaim where former employee only accessed her personal websites, such as Facebook®, personal e-mail, and news websites from employer's computer and did not improperly access employer's information).

3. **The Electronic Communications Privacy Act, 18 U.S.C. §2510, *et seq*., a/k/a the Federal Wiretap Act ("ECPA").** Title I of the ECPA regulates the search and seizure of electronic communications while they are in transit. It provides civil and criminal penalties for the unlawful interception, disclosure or use of electronic communications. However, under the ECPA, consent to the interception by one party to the communication is a defense to a violation.

   The ECPA provides for separate causes of action, both by private individuals and by the government. In a private cause of action under the ECPA, a plaintiff may recover preliminary and other equitable or declaratory relief as may be appropriate, declaratory damages, punitive damages where appropriate, and reasonable attorney's fees and other litigation costs reasonably incurred. 18 U.S.C. §2520. Notably, the ECPA provides that the plaintiff will receive at a minimum $10,000, regardless of a showing of any actual damages. In addition, if the communication involves certain radio or private satellite video communications, the violator may be subject to suit by the federal government. 18 U.S.C. §2511(5). Finally, the ECPA provides for criminal penalties including a fine and imprisonment for up to five years. 18 U.S.C. §2511(4).

   a. No Interception. Courts will likely find that viewing Internet postings or webpages, such as Facebook® and Twitter, does not constitute an interception under the ECPA:

      - *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-84 (9th Cir. 2002) (gaining access to and viewing of group's private bulletin board was not an interception as defined by the ECPA).

      - *See also Ehling v. Monmouth-Ocean Hosp. Serv.*, 872 F. Supp. 2d 369 (D.N.J. May 30, 2012 (dismissing claim under analogous state wiretap act against an employer who accessed an employee's private Facebook® page via another employee's account because the posting accessed was in "post-transmission storage").

   b. State Protection. Another source that may provide protection of unauthorized access or interception is state law. Many states have laws similar to the ECPA that prohibit the interception and/or unauthorized access to stored communications or communications in transit.

- **Florida Wiretap Statute, Florida Statute §934.03 (2013)**. Florida law makes it a crime to intercept or record a "wire, oral or electronic communication," unless all parties to the communication consent. In addition to criminal penalties, violating the Florida Wiretap Statute can expose a party to a civil lawsuit for damages for the injured party.

4. **Potential Violation of the Fair Credit Reporting Act, 15 U.S.C. §1681, *et seq.* ("FCRA").**

   a. Notification. The FCRA requires that a party notify applicants if consumer reports will be used in an employment decision. The statute provides that in general, "a person may not procure a consumer report, or cause a consumer report to be procured, for employment purposes with respect to any consumer," unless:

      - a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes; and

      - the consumer has authorized in writing (which authorization may be made on the document referred to in clause (i)) the procurement of the report by that person.

   b. Consumer Report. A "consumer report" means "any written, oral, or other communication of **any** information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, **character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for … employment purposes.**"

   c. Purpose. "Employment purposes" means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

   d. Inapplicable. The FCRA is typically inapplicable because employers tend to do their own searches of social media sites. However, if an employer were to employ an outside firm, or "consumer reporting agency" such as Info Check USA, to research the candidate's social networking profiles, the FCRA may require that the candidate is first given notice.

   e. Penalties for Noncompliance. Noncompliance with the FCRA can result in civil penalties including a $1,000 fine, punitive damages and the award of attorney's fees and costs.