"THE RISE OF THE MACHINES" DISCOVERY AND SPOLIATION IN THE AGE OF TECHNOLOGY

by

Cynthia N. Sass, Esquire

The Florida Bar
Labor and Employment Law Section
Advance Labor Topics
June 2011

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

"THE RISE OF THE MACHINES": DISCOVERY AND SPOLIATION ISSUES IN THE AGE OF TECHNOLOGY[1]

I. TYPES OF E-DISCOVERY

A. Sources

1. Social Media. Definition of Social Media: Social media are primarily internet and mobile-based tools for sharing and discussing information. Social Media create a forum for the interactive exchange or information commonly referred to as "Web 2.0." Social media include Facebook, Wikipedia, MySpace, blogs, Twitter, LinkedIn, Media Temple, etc.

2. Instant Messages. Instant messages may be sent via the cloud, such as on Facebook or AOL Instant Messenger, or may be sent inter-office through employer-owned software programs.

3. Smart Phones. Information can be electronically stored on smart phones such as Droids, BlackBerries, and iPhones. These types of phones may keep electronic information on their own internal hard drives or may store the information on remote servers.

4. GPS

   a. Global Positioning Systems ("GPS") inside certain electronic devices provide date, time, and location information which may be useful in proving or defending a claim.

   b. *Frew v. Tolt Tech. Serv.*, 2010 WL 557940 (M.D. Fla. Feb. 11, 2010). Fact that employer regularly checked GPS records of employee's vehicle, as well as employee's employer-issued cell phone records, created a genuine issue of material fact as to whether the employer had notice the employee was performing uncompensated overtime work.

   c. *Lochin v. Verizon Florida LLC*, 2010 WL 4056034 (M.D. Fla. Oct. 15, 2010). Employer used GPS reports from employee's vehicle to determine that employee was spending approximately 20 hours a week at his residence.

5. Text Messages

---

[1] The materials included in this paper are distributed by the Law Offices of Cynthia N. Sass, P.A., as a service to clients and other interested individuals. The outline contained herein is provided for informal use only. This material should not be considered legal advice and should not be used as such. Thank you to Joshua R. Kersey, Esquire, of the Law Offices of Cynthia N. Sass, P.A. for his assistance in preparing these materials.

a. As with other electronically stored information on mobile phones, text messages may be stored on the phone's internal memory, on a remote server, or both.

b. See *Flagg v. City of Detroit*, 252 F.R.D. 346, 355 (E.D. Mich. 2008) and *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008). Prominent cases involving the production of text messages.

6. E-mail. One of the most common and voluminous forms of e-discovery, e-mail can be stored both on an employee's computer, as well as on a remote server.

7. Cloud Data. Essentially, cloud data is data which is not stored on a computer's hard drive. The "cloud" is the internet, a series of servers around the world. For example, if you send an e-mail from your Google "gmail" account, that e-mail is in the cloud, so while it may be saved on your computer, it is also saved on Google's servers located somewhere. Another example would be posting a picture to your Facebook profile. That picture, while saved on your computer, has also been put in the "cloud" and it now exists on Facebook's servers. You can delete the picture from your own computer, but it will still exist in the cloud. DropBox, Inc. runs a cloud e-mail service by which users can share e-mails and other files on an off-site server.

B. Format

1. Tagged Image File Format[2] (.tiff or .tif) is an electronic "picture" of a document that is usually created via conversion software or by printing documents and then scanning them as .tiff files.

2. Portable Document Format (.pdf) was designed by Adobe as a more functional form of .tiff files.

3. Native Format simply refers to the format in which the file is normally kept. For example, a Microsoft Word document may be kept in a .doc format, a photograph in a .gif, .bmp, or .jpg format, excel spreadsheets in a .xls format, Outlook e-mails in .pst format, etc.

4. Forensic Imaging

   a. Definition of Forensic Imaging: creating "a 'mirror image' or a 'forensic duplicate,' which replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive." *Communications Center, Inc. v. Hewitt*, 2005 WL 3277983 (E.D. Cal. 2005)

   b. Courts may enter discovery orders requiring "the mirror image" of hard drives of any computers that contain documents responsive to an opposing party's request

[2] *e-Discovery Documents Production Formats: Native, TIFF and PDF*, http://www.lexbe.com/hp/e-Discovery-production-formats-native-PDF-TIFF.aspx (last visited Apr. 26, 2011)

for production of documents. *Theilen v. Buongiorno USA, Inc.*, 2007 U.S. Dist Lexis 8998 (W.D. Mich. 2007)

C. **Metadata** is commonly described as data about data and has been defined as "information about a particular data set which describes how, when, and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location storage requirements and medial information)." See *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information in the Electronic Age,* Appendix F (Sept. 2005).

II. LAWS REGULATING ELECTRONICALLY STORED INFORMATION

A. Below are the most common laws encountered when dealing with e-discovery in the labor and employment arena; be conscious of these laws when performing e-discovery.

1. The Computer Fraud and Abuse Act ("CFAA") – 18 U.S.C. § 1030

a. The CFAA creates criminal penalties for, among other things, the unauthorized access of a protected computer. This often applies where a departing employee attempts to gain an advantage by stealing information from the employer prior to departure.

b. The CFAA focuses on whether the employee's access was authorized, but there is disagreement among the circuits as to when an employee acts without the requisite authorization:

(1) *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Authorization exceeded when employee acts "contrary to the employer's interest."

(2) *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). Employee is authorized until authorization is rescinded.

(3) *Sloan Financial Group, LLC v. Coe*, 2010 WL 4668341 (D.S.C., Nov. 18, 2010). Authorization based on access to computer, not on what plaintiff actually does with information obtained.

(4) *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010). Authorization based on intended use of information.

(5) *U.S. v. Salum*, 257 Fed.App'x 225 (11th Cir. 2007). Authorization based on intended use of information.

c. Employers should specify very clearly the purposes for which employees may access company computers. Circulated policy paperwork and employment contracts outlining when an employee has exceeded their authorization to use company computers to access or obtain certain information are a good method for protecting employers from computer-related employee fraud and abuse.

2. The Electronic Communications Privacy Act ("ECPA") – 18 U.S.C. § 2510 *et seq.*

   a. 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, and it most often arises in the labor context where employers monitor and intercept communications between employees.

   b. *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). Szymuszkiewicz's license had been suspended for driving while intoxicated. He was worried this would lead to his termination because his job required him to drive to people's homes. The jury found that Szymuszkiewicz had gone on his supervisor's computer while she was away and activated a "rule" on her e-mail account so that any e-mail sent to Szymuszkiewicz's supervisor was also forwarded to him. Szymuszkiewicz was convicted of intentionally intercepting an electronic communication in violation of the ECPA. The case illustrates the fact that the law is as applicable to employees as it is to employers.

   c. See also Florida Statutes § 934.03 – Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. *O'Brien v. O'Brien*, 899 So.2d 1133 (Fla. 5th DCA 2005). Court found wife violated Florida Statute § 934.03 when she installed software on husband's computer which intercepted e-mails, chat conversations and instant messages.

3. The Stored Communications Act – 18 U.S.C. § 2701 *et seq.*

   a. Title II of the ECPA is called the Stored Communications Act ("SCA"). The SCA pervades many areas of electronic discovery and prohibits a provider of communication services from divulging the contents of private communications to certain outside parties. First, the SCA limits the right of outside parties to compel providers of communication services to disclose private information in their possession about subscribers, and second, it limits the ability of those same providers to voluntarily provide that information.

   b. The SCA distinguishes between an electronic communication service provider ("ECS") and a remote computing service provider ("RCS"). The main characteristics in determining categorization are the primary use of the service and the length of time the information is stored. The SCA does NOT include an exception for civil subpoenas. Several courts have concluded this means that electronic-communications holders may not produce "content" records in response to a civil subpoena and cannot be compelled by court order to do so. *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423 (2006); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp.2d 606, 609-610 (E.D. Va. 2008);

Federal Trade Commission v. Netscape Communication Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000). This disallowance of subpoenas makes the distinction between an RCS and an ECS an important one in determining what information the communication provider is allowed to provide under the SCA, and when they are allowed to provide it. *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008); *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008); *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (C.D. Cal. 2010). Because the SCA contains a general rule against disclosure, distinguishing between "ECS" and "RCS" becomes important in deciding when information can be disclosed under the SCA. Essentially, "[t]he provider of an RCS may divulge the contents of a communication with the 'lawful consent' of the subscriber to the service, while the provider of an ECS may divulge such a communication only with the 'lawful consent of the originator or an addressee or intended recipient of such communication.'" *Flagg*, 252 F.R.D. at 350.

c. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002). Where employer's vice president gained unauthorized access under false pretenses to a site where airline pilot posted bulletins critical of his employer, court found employer violated the SCA.

III. DISCOVERY OUTSIDE THE RULES

A. E-mails on Company Computers

1. <u>Cases Where Employer Could Retrieve Attorney-Client E-mails</u>

a. *Kaufman v. SunGard Inv. System*, 2006 WL 1307882 (D. N.J. 2006). The court held that employee waived attorney-client privilege by sending e-mails to her attorney on company e-mail system where company policy clearly notified all e-mails on company system were subject to monitoring, searching, or interception at any time.

b. *Alamar Ranch, LLC. v. County of Boise*, 2009 WL 3669741 (D. Idaho 2009). *Citing Stengart v. Loving Care Agency Inc.*, 973 A.2d 390 (N.J. App. Ct. 2009), the court found employee waived attorney-client privilege regarding e-mails sent to attorney because unlike employee in *Stengart*, employee simply used her employer-provided work e-mail instead of web-based password-protected e-mail account.

c. *Holmes v. Petrovich Dev. Co., LLC*, 119 Cal.Rptr.3d 878 (Cal. Ct. App. 2011). The court found that plaintiff had waived her attorney-client privilege with respect to e-mails she sent to her attorney through her company computer and company e-mail address where there was a clear company policy in place prohibiting personal use of the computer and where the policy warned that e-mails were subject to review.

2. Cases Where Employer Could Not Retrieve Attorney-Client E-mails

    a. *Stengart v. Loving Care Agency Inc.*, 973 A.2d 390 (N.J. App. Ct. 2009). The court held that (1) e-mails exchanged between an employee and her attorney on employer's company-issued laptop computer through the former employee's personal, web-based e-mail account were protected by the attorney-client privilege, (2) employee's breach of company's policy regarding use of its computer did not justify company's claim of ownership of employee's e-mail communications to her attorney.

    b. *U.S. v. Hatfield*, 2009 WL 3806300 (E.D.N.Y. 2009). The court upheld an employee's attorney-client privilege with respect to attorney-created documents stored on his company-issued computer hard drive by using the following five-factor test: (1) did the employer maintain a computer policy banning personal or other objectionable use, (2) did the employer monitor the use of the employee's computer or e-mail, (3) did the employer or third parties have a right to access the employee's computer or e-mails, (4) did the employer notify the employee or was the employee aware of the employer's policies regarding computer use and monitoring, and (5) how did the employer interpret its computer usage policy.

    c. *Curto v. Medical World*, 2006 WL 1318387 (E.D.N.Y. 2006). The court found that employer with e-mail monitoring policy went too far when it accessed e-mails an employee had sent to her attorney while working at home via her company-issued laptop computer.

    d. *Convertino v. U.S. Dept. of Justice*, 2009 WL 4716034 (D. D.C. 2009). The court upheld attorney-client privilege for e-mails employee sent to his attorney from work computer at the Department of Justice which the Department of Justice later obtained from its e-mail server where the Department of Justice (1) did not have a policy banning personal use of company e-mail, (2) never notified employee it would regularly access and retain e-mails from his account, and (3) employee had attempted to keep e-mails private by deleting them, unaware they still existed on e-mail servers.

3. Self-Help by Plaintiff/Defendant

    a. *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). The court found the defendant in violation of Wiretap Act and Stored Communications Act for creating a "rule" on his supervisor's e-mail which forwarded all of her incoming e-mails to his computer.

IV. MANAGEMENT OF E-DISCOVERY

A. Obligation to Preserve Electronic Evidence

1. Federal Law - When does the duty to preserve arise

a. Duty to Preserve. 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).

(1) *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.

(2) *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F. Supp. 2d 1317, 1327 (S.D. Fla. 2010). The court found that upon defendant's letter to plaintiff stating defendant's position with respect to plaintiff's violation of an exclusivity position 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.

(3) *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.

(4) *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."

(5) *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."

2. 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.*

(1) *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.")

(2) *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.")

B. Litigation Holds

1. A "litigation hold" is a notice issued in anticipation of a lawsuit or investigation, ordering employees to preserve documents and other materials relevant to that lawsuit or investigation. Black's Law Dictionary (9th ed.)(2009)

2. Issuing a litigation hold

a. "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)

C. Handling Production of Voluminous E-Discovery

1. Determining whether a disclosure was inadvertent

a. There is no exhaustive list of factors, but courts have looked at (1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of document production; (2) the number of inadvertent disclosures; (3) the extent of disclosure; (4) any delay and measures taken to rectify the disclosures; and (5) whether the overriding interests of justice would be served by relieving a party of its error." *Lightbourne v. McCollum*, 969 So.2d 326, 334 n.6 (Fla. 2007).

b. *Preferred Care Partners Holding Corp. v. Humana, Inc.*, 258 F.R.D. 684 (S.D. Fla. 2009). Humana produced over 10,000 pages of documents in response to a discovery request. Among those documents were five documents, including e-mails which Humana stated were attorney-client privileged and were inadvertently disclosed. For three of the five documents, the court found (1) the production was clearly inadvertent; (2) Humana realized it quickly, requesting plaintiff return the document within a short period of time; (3) Humana took reasonable steps to prevent the disclosure as they spent hours, even days, reviewing the production for privileged material prior to producing it and released only five privileged documents out of roughly 10,000. The court ultimately decided that privilege was not waived with regard to three of the five documents.

2. Cost-Shifting

   a. When e-discovery becomes voluminous, equity may require a sharing of the costs of production. The *Zubulake* case has become widely known in e-discovery circles as the basis for the Advisory Committee Notes to Fed. R. Civ. P. 26(b)(2)(B). Essentially:

      (1) Usual rules of discovery apply to data kept in an accessible format, and the responding party should pay for the costs of producing this responsive data.

      (2) If responsive data is relatively inaccessible (i.e. exists only on backup tapes), it is reasonable to consider cost-shifting analysis. It may also be reasonable to ask the responding party to produce a small sample of responsive information from the archiving medium to show that the sought-after information actually exists.

      (3) The Advisory Committee Notes suggest seven-factors very similar to *Zubulake*: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of further information; (6) the importance of the issues at stake in litigation; and (7) the parties' resources.

   b. *Semsroth v. City of Wichita*, 239 F.R.D. 630 (D. Kan. 2006). Despite fact that e-mails were on inaccessible backup tapes, *Zubulake* factors did not warrant shifting any part of restoration cost to plaintiffs, as it was only $4,000.

   c. *Major Tours, Inc. v. Colorel*, 2009 WL 3446761 (D. N.J. 2009). Because information on backup tapes was largely duplicative and cost to retrieve would likely exceed $100,000, plaintiffs would be liable for cost of duplicative information and would split the retrieval costs of non-duplicative content.

d. *Takeda Pharmaceutical Co. Ltd. V. Teva Pharmaceuticals USA, Inc.*, 2010 WL 2640492 (D. Del. June 21, 2010). Court found good cause shown for the production of ESI for a period of 18 years in patent case and ordered parties to share in the costs of production.

V. HOW TO OBTAIN E-DISCOVERY

A. Federal Rules

1. Rule 16

   a. In a scheduling order issued under Rule 16, a judge may provide for the disclosure of ESI.

   b. The judge may also take whatever action may be appropriate to "facilitat[e] in other ways the just, speedy, and inexpensive disposition of the action," which could easily encompass orders regarding the production of electronic discovery. Fed. R. Civ. P. 16(c)(2)(P)

2. Rule 26(a)(1)(ii)

   a. A party must provide to other parties, "a copy — or a description by category and location — of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment;"

   b. Determining whether a party has "control" under the Rule

      (1) *Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1984). Court found that documents or other items do not need to be in a party's possession in order to be discoverable; they need only be in that party's custody or control. A party has "control" if it "has the legal right to obtain the documents on demand;" *MCC Management of Naples, Inc. v. Arnold & Porter LLP*, 2010 WL 2889350 (M.D. Fla. July 20, 2010) (Same)

      (2) *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474, 477 (D.Colo. 2007). The court found that El Paso Corporation had "control" within the meaning of Rule 34(a)(1), of electronic records maintained by a third party on the company's behalf.

   c. If a party "controls" the content, the court may compel the party's consent. *Flagg v. City of Detroit*, 252 F.R.D. 346, 355 (E.D. Mich. 2008). Court first determined that the party controlled the content stating "[i]f the city can block the disclosure of [text] messages by withholding its consent, it surely follows that it can permit the disclosure of these communications by granting its consent." Court then ordered the City to consent to the release of the contents of the text messages.

3. Rule 26(b)(2)(B). "A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery." Fed. R. Civ. P. 26(b)(2)(B).

    a. *Calixto v. Watson Bowman Acme Corp.*, 2009 WL 3823390 (S.D. Fla. 2009):

        (1) Provides an analysis of Rule 26(b)(2)(B).

        (2) Court first put burden on defendant to demonstrate that the information plaintiff sought was not reasonably accessible because of undue burden or cost. Defendant successfully showed that the information was on backup tapes, which would have to be reformatted at an approximate cost of $40,000. The documents would then have to be reviewed for privilege, creating even greater costs.

        (3) After finding the information was "not reasonably accessible" the court turned to whether plaintiffs had nonetheless demonstrated good cause for the court to require defendants to produce the ESI. The court found that plaintiffs had failed to establish that the production would yield any new, relevant information that the other forms of discovery had not. Therefore the court refused to compel the disclosure of the ESI.

4. FRCP 26(b)(5)(B) and FRE 502 – Inadvertent Disclosures

    a. Due to the large number of documents produced in voluminous e-discovery, the danger of divulging potentially privileged or confidential information increases substantially. To help compensate for this increased danger, Federal Rule of Evidence 502 and Federal Rule of Civil Procedure 26(b)(5)(B) were enacted to provide a mechanism for a "claw-back" procedure to, in certain instances, retrieve privileged discovery inadvertently produced to the opposing side without waiving the privilege.

    b. The rules provide that there is no waiver of privilege when: (1) the disclosure was inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B). (Federal Rule of Evidence 502 (West 2011)).

See Section IV(c) herein.

5. Rule 26(f) Discovery Conference

   a. "[T]he parties must confer as soon as practicable … [and] discuss any issues about preserving discoverable information; and develop a proposed discovery plan." Fed. R. Civ. P. 26(f)

   b. Discuss any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced, costs, setting up a teleconference between each of their IT personnel, and beginning to try to develop a list of search terms that will be used to cull out the most relevant ESI.

   c. Further, counsel should be sure that the parties unequivocally agree on the format in which the ESI will be produced. If the parties cannot agree, they should go to the court before the commencement of any e-discovery and get an order from the judge directing the format in which the ESI will be produced.

      (1) *Seven Seas Cruises S. De R.L. v. V. Ships Leisure Sam, et al.*, 2011 WL 181439 (S.D. Fla. 2011) Where plaintiffs argued that defendants did not produce the ESI in .tiff format as "agreed" upon but rather in .pdf format, the court found that there was no clear agreement and therefore denied the plaintiff's motion to have the ESI converted.

6. Rule 34 Requests for Production

   a. Rule 34(a)(1)(A): "A party may serve on any other party a request within the scope of Rule 26(b) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control: any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."

   b. Drafting Requests for Production

      (1) Remember that Rule 34(b)(1)(C) states that a request for production "may specify the form or forms in which electronically stored information is to be produced." Therefore counsel should take time to consider the advantages and disadvantages of each format of production and specify which format they prefer.

         (a) *In re Netbank, Inc. Securities Litigation*, 259 F.R.D. 656, 681 (N.D. Ga.

2009). Where defendants argued that they were not required to produce ESI in native format and instead produced the information in .tiff format, the court ruled that Rule 34(b)(1)(C) allowed the requesting party to determine the format of production and so long as defendant's were not able to provide the court a "good reason" that it should not produce the ESI in native format, the files must be produced as requested.

(b) *Williams v. Sprint/United Management Company*, 230 F.R.D. 640, 652 (D. Kan. 2005). Where documents were requested in their "native format," such format included metadata.

(2) Metadata. A party who seeks metadata in an electronic discovery request should be sure to <u>specifically request that all metadata be included</u>. This is because there is a lack of agreement among the courts as to whether metadata is automatically included in ESI production.

(a) *Autotech Technologies Ltd. Partnership v. Automationdirect.com, Inc.*, 248 F.R.D. 556, 559-60 (N.D. Ill. 2008). The court stated, "[o]rdinarily courts will not compel the production of metadata when a party did not make that a part of its request."

(b) *D'Onofrio v. SFX Sports Group, Inc.*, 247 F.R.D. 43, 48 (D.C. 2008) The court refused to compel the production of metadata where the requesting party did not specify any particular form in which the ESI was to be produced.

(c) *But see, National Day Laborer Organizing Network, et al. v. U.S. Immigration and Customs Enforcement Agency, et al.*, 10 Civ. 3488 (SAS), (S.D.N.Y. February 7, 2011) The court held that a response to a Freedom of Information Act request must include metadata.

7. <u>Rule 45 – Third-Party Subpoenas to Providers of Electronic Services</u>. Many forms of discoverable electronically stored information (ESI) are subject to the Stored Communications Act (SCA), which prevents certain providers of electronic communication services from releasing ESI to third parties. Because the SCA contains no exception for civil subpoenas, Rule 45 third-party subpoenas are largely an ineffective means of obtaining this content.

   a. *In re Subpoena Duces Tecum to AOL LLC*, 550 F.Supp. 2d 606 (E.D. Va. 2008). Court granted motion to quash subpoena directed to AOL, holding that the SCA prohibited AOL from divulging contents of e-mails because the act contains no exception for civil subpoenas.

   b. *Hone v. Presidente U.S.A. Inc.*, 2008 U.S. Dist. Lexis 55722 (N.D. Cal. July 21, 2008). Court found that the SCA prohibited Yahoo! from divulging the contents of Hone's e-mails at the Defendant's request.

c. *Viacom Internat'l Inc. v. YouTube, Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008). Court found that YouTube was prohibited from divulging subscribers' actual videos, but was required to divulge the number of times the videos had been viewed because the Court felt the number of views was not "content" under the SCA.

d. *J.T. Shannon Lumber Co. v. Gilco Lumber, Inc.*, 2008 WL 3833216 (N.D. Miss. Aug. 14, 2008). Court quashed subpoenas to Microsoft Corporation, Yahoo!, Inc. and Google, Inc. requesting subscriber e-mails because the SCA does not include an exception for civil subpoenas.

e. *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (C.D. Cal. 2010). Court quashed defendant's third-party subpoenas to Facebook, MySpace and Media Temple to the extent they requested content covered under the SCA.

VI. OBJECTIONS / MOTION TO COMPEL ISSUES

A. Relevance

1. *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, 2007 WL 119149 (D. Nev. 2007) (Sexual Harassment Case). The court ruled that the content of plaintiff's MySpace page regarding her emotional distress was relevant to her complaint of harassment at Fidelity and was therefore discoverable.

2. *McCann v. Harleysville Ins. Co. of New York*, 910 N.Y.S.2d 614 (N.Y. App. Div. 4th Dept. 2010) (Personal Injury Case). The court ruled that the defendant had not adequately shown the relevance of the content of the plaintiff's Facebook page in order to compel production. Notably, the court stated that it would not allow the defendant to go on a Facebook "fishing expedition."

3. *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (N.Y. Sup. Sept. 21, 2010) (Personal Injury Case). The plaintiff claimed she was injured and largely confined to her home. Defendant sought access to the plaintiff's Facebook and MySpace content (i.e. photos) that showed the plaintiff on vacation in other states, smiling happily. The court held that the defendant was entitled to discover the relevant content of the social network pages.

B. Privacy Concerns. Generally, courts will allow for the discovery of material that is <u>relevant</u> to an action, regardless of any privacy settings a party has placed on the information.

1. *Moreno v. Hartford Sentinel, Inc.*, 172 Cal.App. 4th 1125 (Cal. App. 2009). The court said that because plaintiff's MySpace page was not restricted in any way (anyone with a computer could access it), plaintiff had no reasonable expectation of privacy in the content.

2. *City of Ontario v. Quon*, 2010 WL 2400087 (U.S. 2010). The Supreme Court

recently held that a public employer may search its employee's personal text messages sent on an employer-provided texting device without violating the Fourth Amendment.

3. *Thygeson v. U.S. Bancorp.*, 2004 U.S. Dist. Lexis 18863 (D. Or. 2004). Employee has no reasonable expectation of privacy as to which internet sites he visits on his work computer.

4. *Pietrylo v. Hillstone Restaurant Group*, 2008 WL 6085437 (D.N.J. 2008). The court denied summary judgment where there was an issue as to whether an employee was coerced into providing access to electronic content on a MySpace page that was open only to those that were invited.

5. *Equal Employment Opportunity Commission v. Simply Storage Management*, Discovery Order Issued on May 11, 2010, Case No. 1:09-cv-1223-WTL-DML (S.D. Ind. 2010) The court held that privacy settings had no effect on a party's expectation of privacy. The court wrote, "[a]lthough privacy concerns may be germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for proper purpose in the litigation, a person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery."

VII. PUBLIC SECTOR ISSUES

A. 1st Amendment Issues

1. *Spanierman v. Hughes*, 576 F.Supp. 2d 292 (D. Conn. 2008). The court stated that while some speech on the plaintiff-teacher's MySpace was protected speech on a matter of public concern, the plaintiff had failed to show a causal connection between the protected speech and the adverse employment action (his termination was for other content discovered on his MySpace page, namely inappropriate communications with students).

2. *Snyder v. Millersville University*, 2008 WL 5093140 (E.D. Pa. 2008). The court stated that there is no First Amendment protection for the Plaintiff-teacher's MySpace comments on private matters not of public concern.

B. Social Media Kept by Public Sector. The main concerns with regard to Public Sector entities maintaining social media sites revolve around what information then becomes a public record. This issue was addressed in a question posed to the Attorney General's Office by the City of Coral Springs, Florida:

1. When public entities choose to use social media platforms such as Twitter or Facebook, the issues become more convoluted because of public records laws. In a question to then Attorney General Bill McCollum, an attorney for the City of Coral Springs, Florida asked, "[i]f the City chooses to maintain a Facebook page, would all

the contents of the City's page, including information about the city's 'friends' and their pictures, and the friends' respective Facebook pages, be subject to the Public Records Law?"

2. In response, the Attorney General advised that the City did have the authority to establish a Facebook page so long as the page was for a valid municipal purpose. Whether information on the Facebook page would constitute a public record would depend on whether the information was made or received in connection with the transaction of official business by the City. Due to the fact that the purpose of the page must be a municipal one, it follows that the placement of material on the City's page would presumably be in furtherance of such purpose and in connection with the transaction of official business. Thus, it is likely that the information on the City's Facebook page would be a public record.

3. The issue as to whether the City's "friends'" Facebook pages would be public record was not decided, but the AGO did warn that if the City should choose to create a Facebook page, it should be sure to warn all those who became its friend of the application and implications of the Public Records Law.

C. **Public Sector Requirement to Give Metadata.** While there is currently no Florida case or statute that specifically mentions metadata, several other states have held that it should be included in a public document as a public record:

1. *Irwin v. Onondaga County Resource Recovery Agency*, A.T., 895 N.Y.S.2d 262, 319 (N.Y. App. Div. 4th Dept. 2010). The court held narrowly that "system" metadata, that is, metadata that reflects automatically generated information about the creation or revision of a document, such as the document's author, or the date and time of its creation or modification, should be included in a Freedom of Information Act request. However, the court refused to extend the ruling to include substantive (data created by the software used to make the product reflecting edits or changes) or embedded (data inputted into a file by its creators or users) metadata.

2. *Lake v. City of Phoenix*, 218 P.3d 1004, 1007-08 (Ariz. 2009). "The metadata in an electronic document is part of the underlying document; it does not stand on its own. When a public officer uses a computer to make a public record, the metadata forms part of the document as much as the words on the page."

3. *O'Neill v. City of Shoreline*, 240 P.3d 1149, 1152 (Wash. 2010). "Metadata may contain information that relates to the conduct of government and is important for the public to know. It could conceivably include information about whether a document was altered, what time a document was created, or who sent a document to whom. Our broad PRA exists to ensure that the public maintains control over their government, and we will not deny our citizenry access to a whole class of possibly important government information. We agree with the Supreme Court of Arizona that an electronic version of a record, including its embedded metadata, is a public record subject to disclosure."

VIII. SPOLIATION

A. Florida State Law on Spoliation

1. Definition of Spoliation and Purpose of Sanctions

    a. 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)). Spoliation sanctions are imposed in Florida "to assure that the non-spoliator does not bear and unfair burden." *Reed v. Alpha Prof'l Tools*, 975 So.2d 1202, 1204 (Fla. 4th DCA 2008). 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)

    b. Under Florida law, spoliation is established when the party seeking sanctions proves that: (1) the evidence existed at one time, (2) the alleged spoliator had a duty to preserve the evidence, and (3) 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)

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

        (1) *Golden Yachts, Inc. v. Hall*, 920 So.2d 777 (Fla. 4th DCA 2006) (unlike the presumption of negligence which may arise under *Valcin*, 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.)

        (2) *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).

2. Florida State Courts are Inconsistent as to Whether the Intent of the Spoliator is Relevant to the Imposition of Sanctions

    a. "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 629, 630 (Fla. 3d DCA 1995).

b. 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. *Id.* at 631.

c. *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.

d. "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." *Wilson v. Wal-Mart Stores, Inc.*, 2008 WL 4642596, at *2 (M.D. Fla. Oct. 17, 2008)

3. Additionally, it is of note that 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).

4. 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).

B. Federal Law on Spoliation

1. Florida federal courts have tended to follow state courts:

   a. *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.")

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

   a. *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.")

3. Spoliation Established: 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. *Flury v. Daimler Chrysler Corp.*, 427 F.3d 939, 944 (11th Cir. 2005)

   a. *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.)

4. Employers may be responsible for spoliation by their employees:

   a. *Connor v. SunTrust Bank*, 546 F. Supp. 2d 1360, 1377 (N.D. Ga. 2008). Court found Bank could be held liable for a supervisor's destruction of an e-mail that stated the reasons for the plaintiff's termination.

   b. *Nucor Corp. v. Bell*, 251 F.R.D. 191 (D. S.C. 2008). The employer was held liable for information on company owned computers that was destroyed by its employee, Mr. Bell. Mr. Bell had also destroyed evidence in the case that was contained on his own, personal thumb drive. The court held that the employer could not be held liable for the information destroyed on Mr. Bell's personal thumb drive, but that Mr. Bell himself could be held liable for the destruction.

C. Range Of Penalties

1. 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]

2. Additional sanctions include:

   a. Monetary Sanctions. *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 back up tapes (as well as issues with defendant's responses to interrogatories) resulted in monetary sanctions in the amount of $1,022,700.

   b. Exclusion of Expert Testimony. *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.

   c. Adverse Inference Jury Instruction

      (1) *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

[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)

instruction was appropriate.

(2) An adverse inference can be a devastating sanction. In *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, Case No. 502003CA005045XXO-CAI (Fl. Cir. Ct. 2005), 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.

d. Dismissal of Offending Party's Claim. *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.

e. Default Judgment Against Offending 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 the losing of the records was through no fault of its own.

f. Imprisonment. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 2010 WL 3530097 (D. Md. Sept. 9, 2010). Chief Magistrate Judge Paul Grimm of the United States District Court for the District of Maryland recommended to the judge a default judgment against defendant Creative Pipe and ordered up to two years of imprisonment for its president Mark Pappas as sanctions for their electronic discovery misconduct.

IX. ETHICAL CONCERNS

A. Wrongfully Obtained Electronic Documents. The Florida Bar's Professional Ethics Committee addressed this issue in its Ethics Opinion 07-1. 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 Committee as to what his obligations were to disclose or return the documents to opposing counsel. The Committee advised the attorney that he should take the following steps: (i) discuss the potential that the client may need criminal representation; (ii) discuss with the client that the court may disqualify the attorney from representing him; (iii) advise the client that the attorney may be subject to sanctions by the court, and (iv) 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.

B. Metadata. The American Bar Association's ("ABA") Standing Committee on Ethics and Professional Responsibility has issued a formal opinion regarding the review and use of metadata. The ABA noted that its Model Rules of Professionalism do not contain any specific prohibition against a lawyer reviewing and using metadata embedded in electronic documents that he or she receives through legitimate means from opposing counsel. The American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 06-442 (August 5, 2006).

C. Researching Jurors

1. Ethicists advise that lawyers are encouraged to research potential jurors before trial on sites such as Twitter, Facebook, MySpace, LinkedIn and blogs. Most state ethics rules also allow lawyers to contact jurors after trial with certain restrictions. However, during trial, lawyers should have no contact with empanelled jurors.

2. The no-contact rule does not prevent lawyers from ethically performing passive monitoring of empanelled jurors to verify the absence of misconduct. If the juror publishes publicly available information on the internet on sites such as Facebook or MySpace, then monitoring those social media sites may not be inappropriate. However, sending friend requests, following the juror on Twitter, attempting to make contact on LinkedIn or similar actions would constitute impermissible juror contact.

3. Monitoring Jurors Online. A Missouri Supreme Court opinion in *Johnson v. McCullough*, 306 S.W.3d 551, 558-59 (Mo. 2010) 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.

D. Friending Jurors, Witnesses or Parties

1. In 2009, the Philadelphia Bar Association's Professional Guidance Committee (the "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 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 Committee found that the attorney's proposed course of action could violate various state ethics rules. For example, the 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. The Committee found that the proposal could also violate Rule 4.2 (Communication with Person Represented by Counsel), 4.3 (Dealing with Unrepresented Person), Rule 4.1 (Truthfulness in Statements to Others); and 5.3 (Responsibilities Regarding Nonlawyer Assistants). *The Philadelphia Bar Ass'n Prof'l Guidance Comm.*, Op. 2009-02 (March 2009).

2. In 2010, in a similar opinion of its own, the New York City Bar Association Committee on Professional Ethics echoed the Philadelphia Committee's opinion, stating that neither attorneys nor their agents were permitted to "friend" potential witnesses under false pre-tenses. The New York City 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 Philadelphia and New York City Committee opinions is that the New York City 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 New York City 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 Ass'n of the Bar of the City of New York Comm. On Prof. Ethics*, Formal Op. 2010-2 (September 2010).