This issue of *E-Discovery Connection* contains articles addressing several emerging electronic discovery issues. Several of the authors cover e-discovery considerations implicated by the use of social networking platforms. Michael Goodfried and Martha Dawson discuss the discoverability of social networking content, Eric Probst discusses the expectation of privacy, and John Mallery discusses the collection of social networking and mobile phone data.

Additionally, the two articles cover preservation issues. G. Franklin McKnight IV, Kymberly Kochis, and John F. Mullen Sr. discuss the complex preservation obligations corporations and counsel face and Angela Scafuri provides an overview of the recent *Victor Stanley II* opinion.

Furthermore, Joe Valentine provides a practice piece addressing the form and organization of production under Rule 34 and Thomas D. Esordi discusses the challenges governmental entities and health care providers face with the HITECH Act.

Please continue to submit topics for future editions of this newsletter. We are always seeking contributions in the evolving area of e-discovery.

**From the Editor in Chief**

by John D. Martin

**John Martin** is a partner at Nelson Mullins Riley & Scarborough LLP where he practices products liability, business, pharmaceutical, and medical device litigation. Mr. Martin is routinely called on by his clients to consult on e-discovery preparedness and case-specific electronic discovery strategies.

**Featured Articles**

**Discovery Of Social Networking Sites**

by Michael Goodfried and Martha Dawson

Consider how you, or someone you know, uses social networking sites; and consider how valuable this could be in litigation.

• "Check out the photos from my climb of Mt. Rainier. It rocked! I guess my back injury wasn’t that bad after all."
• "I can’t believe what my boss just did."
• "My kids are driving me crazy. Anyone want to borrow them for the night?"

**Are Social Networking Sites Discoverable?**

Social networking sites are internet sites on which individuals or companies can create profiles about themselves and share information with others. Users can update their status, type blog entries, post pictures or videos, send email or instant messages, or post comments on the profiles of their contacts, among many other offerings. One of the most important aspects of social networking sites is the ability to link up with other users as “friends” or “contacts,” and decide with whom to share information. Users can control their privacy settings and choose which information to make publicly available, share with their contacts, share with their contacts’ contacts (friends of friends), or show only to certain individuals. Some of the most popular social networking sites are Facebook, MySpace, Twitter, and LinkedIn.

Federal Rule of Civil Procedure 34 (A)(1)(a) was amended in 2006 to include "electronically stored information" ("ESI") in the definition of what is subject to a request for production. That term is intended to reflect both current and future technologies, so that the rule won’t have to be amended every time a new form of communication is created. See Fed. R. Civ. P. 34 advisory committee’s note (2006). Although social networking sites were in their infancy when the 2006 rules revision process began, the language of Rule 34 is broad enough to include the content on
any type of internet site, as long as the content is stored. Messages, status updates, pictures, videos, contact information, and all other content posted on social networking sites fits the Rule 34 definition of "data compilations stored in any medium from which information can be obtained."

Federal Rule of Civil Procedure 26 was also amended in 2006 to include "electronically stored information" within the scope of discovery. Discovery is, in general, broadly permitted, and limited only to documents which are "reasonably calculated to lead to the discovery of admissible evidence." ESI contained on a party's social networking site can be subject to discovery if it relates to the issues in the litigation. In EEOC v. Simply Storage Mgmt., No. 1:09-cv-1223-WTL-DM, 2010 WL 3446105, at *3 (S.D. Ind. May 11, 2010), the court stated that discovery of social networking sites "requires the application of basic discovery principles in a novel context", and that the challenge is to "define appropriately broad limits . . . on the discoverability of social communications."

There is a duty to preserve relevant or potentially relevant information once litigation is pending or reasonably anticipated, as long as it is in your custody or control. Zubulake v. UBS Warburg LLC, 220 F.R.D. 121 (S.D.N.Y. 2003)." (Zubulake v. UBS Warburg LLC, 220 F.R.D. 121 (S.D.N.Y. 2003).) The duty to preserve ESI can extend to the content on social networking sites. Although the user does not have custody or control over the physical location of the ESI (the site's servers), the user may still have control over what material gets posted to, or removed from, their account. See Facebook's Statement of Rights and Responsibilities, available at http://www.facebook.com/terms.php. ("You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.").

**Acquiring ESI from Social Networking Sites**

In order to obtain the private content of internet sites, the requesting party must obtain permission from the site's user, not the site operator. The Stored Communications Act ("SCA") prohibits internet operators from "knowingly divul[ing] to any person or entity the contents of a communication while in electronic storage . . ." or "which is carried or maintained on that service." 18 U.S.C. § 2702(a)(1), (a)(2). The site operator must have the "lawful consent of the originator or an addressee or intended recipient" in order to divulge the information. Id. § 2702(b)(3). A third-party subpoena issued to the site operator is generally not proper, because the SCA requires the originator's consent, not the transmitter or service provider. See also O'Grady v. Superior Court, 139 Cal. App. 4th 1423 (2006) (the discovery should be directed at the owner of the data, not the party holding it). Even if the site operator does not object to the subpoena, the user will have standing to quash the subpoena, because the subpoena seeks the user's personal and private information. Crispin v. Audigier, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

You can attempt to obtain relevant ESI by issuing requests for production to the user which seek specific documents, or which seek the content of the user's entire profile. You can also serve interrogatories requesting the user's logon names and passwords for their social networking sites. If the user refuses to provide this information, you can request the court issue an order requiring the user to provide the ESI and/or logon information, or the court can order the user to deliver a consent and authorization form as required by the site operators.

To determine when an order should be granted to provide access to the private content on the social networking site, the court should consider whether the content is subject to privacy concerns, and whether those privacy concerns are outweighed by the requesting party's need to obtain the content. The privacy rights can be derived from Rule 26(c)(1), the protections of the SCA, or from state law. See Crispin, 717 F. Supp. 2d. at 970; Fed. R. Civ. P. 26(c)(1) ("the court may . . . protect a party or person from annoyance, embarrassment, oppression . . .").

Users of social networking sites can select their privacy settings to determine what content is available to other members of the social networking site. The privacy settings can be broken out into four categories, with descending levels of privacy. The first category is content made available only to targeted individuals. The second category is where access is limited to the poster's friends or contacts. The third category is content made available to second-level contacts, or friends of friends. The fourth category is content accessible to the general public. This category, like other publicly available material on the internet, can be viewed and obtained directly by anyone without the need for a discovery request. The services offered on social networking sites, such as status updates, posting of pictures or videos, emails and text messaging, will likely change over time; but the analysis to determine the discoverability of the content depends less on the form of the content and more on the user's expectation of privacy.

The first category above, which is often limited to messaging and email services, may have a high expectation of privacy. The fourth category, public postings, may have no expectation of privacy; the third category, second-level contacts, may also have no expectation of privacy since ESI is available to people the user might not even know. The second category is more of a gray area, since the user somewhat restricted access.

Courts may also examine the privacy policies of the social networking sites themselves. Many of these sites explicitly state that they do not guarantee the privacy of user content. For example, Facebook's privacy policy, as of October 5, 2010, states that "some of the content you share and the actions you take will show up on your friends’ home pages and other pages they visit" and that Facebook may "disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required
by law.” See Facebook's Privacy Policy, available at http://www.facebook.com/policy.php. In Romano v. Steelcase, 907 N.Y.S. 2d 650, 655 (2010), the court went so far as to state that the plaintiff has no reasonable expectation of privacy “notwithstanding her privacy settings” because Facebook and MySpace did not guarantee “complete privacy.”

Once the court has determined whether and to what extent the user has an expectation of privacy (if any), the court should then balance that privacy concern with the opposing party's need to obtain the ESI. Some of the factors the court may consider are: (1) is the content material and necessary to prove the issues in the case; (2) are there other means to obtain the content; and (3) will the requesting party be at a disadvantage without access to the content. See Romano, 907 N.Y.S. 2d at 655. In general, there is a strong public policy in favor of broad discovery, so courts may allow discovery, and rely on a protective order to protect the privacy concern. See Simply Storage Mgmt., 2010 WL 3446105, at *3.

The court should require the requesting party to show a likelihood that the social networking site private profile contains relevant information. In certain cases, the content available on the public profile can go a long way toward showing the private profile contains potentially relevant information. In Romano, the court permitted discovery of the plaintiff's private profiles on Facebook and MySpace because a photo on her public profile was relevant to her claims. See Romano, 907 N.Y.S. 2d at 655.

After it has been determined that the private content on the social networking site is subject to discovery, the next element is to determine which particular content can be discovered. The court will consider whether the requests have been tailored to seek only relevant information within the scope of Rule 26, or whether the party is on a fishing expedition. The court may choose to order the user to provide access to their entire profile, or it may order access to a limited portion of the content, such as wall postings available to all of the user's contacts, or messaging with particular individuals. On at least one instance, the court has offered to provide an in camera review by becoming "friends" with the user in order to review the private content for relevancy. Barnes v. CUS Nashville, No. 3:09-cv-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).

Conclusion

Social networking sites have become a popular destination for people to post information they intend to share with others. The content on these sites may be subject to discovery where relevant to the claims in the case, as “electronically stored information” within the user's custody and control. Since the intent of social networking sites is to share information with others, one may argue that there is little to no expectation of privacy, permitting discovery of the content even when on a private page.

Michael Goodfried is a staff attorney at K&L Gates in the e-Discovery Analysis and Technology (e-DAT) practice group. His work focuses on counseling clients on electronic discovery issues and managing large-scale document review projects. Michael earned a B.A. at the University of California, Berkeley and his J.D. at the Boston University School of Law.

Martha Dawson is a partner in K&L Gates, where she co-chairs the firm’s e-Discovery Analysis & Technology group. She has been a member of DRI and Lawyers for Civil Justice since 2004.

Overcoming Reasonable Expectation Of Privacy Rights To Discover Postings On Social Networking Sites

by Eric L. Probst

"New technologies create interesting challenges to long established legal concepts." Written over fourteen years ago in a court martial decision involving the electronic transmission of pornography, United States v. Maxwell, Jr., 45 M.J. 406 (C.A.A.F. 1996), this statement has never been more relevant than it is today in the social networking era of Facebook, MySpace, Twitter, LinkedIn, and other social networking sites ("SNS"). When Congress enacted the Stored Wire and Electronic Communications Privacy Act in 1986, 18 U.S.C. §§ 2701–2711 ("SCA"), to regulate how and under what circumstances electronic information providers could produce electronic information to third parties, Mark Zuckerberg, Facebook's co-founder, was only two years old. Now, there are more than 500 million active users of Facebook spending over 700 billion minutes per month on the site, posting information about their lives, displaying photographs from recent vacations and emailing friends. See Facebook, available at http://www.facebook.com/press/info.php?statistics.

In 2010, there is more potentially "relevant" information about a case available on SNS than in any other source. The flexibility of the Federal Rules of Civil Procedure and their state analogs often support the discovery of the electronically stored information contained on these sites.

However, as the Maxwell court forecast, the presumed availability of SNS postings challenges the SNS user's expected right to privacy in the communications. Though few reported decisions exist, the courts that have considered the issue have required the production of SNS posts after examining the nature and scope of the SNS discovery requests, the sites, the type of messages posted on the sites, third party access to the postings, and the legal claims at issue. Stated differently, the courts have applied “long established legal concepts”—traditional discovery principles—to determine whether a party has to produce SNS postings.
Discovering Social Networking Postings – Public v. Private Postings

No party can dispute that SNS may contain relevant information to a claim or defense. The challenge for defendants is to discover this information over plaintiffs' right to privacy objections, the threshold issue courts address when determining whether defendants are entitled to SNS postings. EEOC v. Simply Storage Mgmt., No. 1:09-cv-1223, 2010 U.S. Dist. LEXIS 52766, at *8-9 (S.D. Ind. May 11, 2010) (holding that the privacy issue is "threshold point" for court's analysis). The privacy interest discovery dispute closely resembles traditional discovery arguments. The dispute is fact-sensitive, and defendants should recognize that narrowly tailored SNS discovery requests are judicially favored. While federal and state discovery standards are liberal, they are not without limit. Fed. R. Civ. P. 26(b)(2)(C) (stating that a court can limit discovery if the requests offend, harass or are "unnecessarily cumulative or duplicative."). In certain cases, most notably when a plaintiff's mental health is at issue, courts have recognized the need to impose limits on SNS discovery. See Simply Storage Mgmt., 2010 U.S. Dist. LEXIS 52766, at *8-9. Defendants must understand when drafting discovery requests, especially in personal-injury cases, that though "anything that a person says or does might in some theoretical sense be reflective of her emotional state[,] . . . that is hardly justification for requiring the production of every thought she may have reduced to writing or, indeed, the deposition of everyone she may have talked to." Rozell v. Ross-Holst, No. 05 Civ. 2936, 2006 U.S. Dist. LEXIS 2277, at *11 (S.D.N.Y. Jan. 20, 2006). Thus, just because a plaintiff has posted information on Facebook or MySpace does not mean that it is discoverable.

From this jumping off point, the courts examine the communication in light of the sliding scale of a person's privacy interests in electronic communications. Courts have recognized that "[e]xpectations of privacy in e-mail transmissions depend, in large part, on the type of e-mail involved and the intended recipient." Maxwell, 45 M.J. at 419. Chat room communications and e-mails forwarded to several recipients "lose any semblance of privacy." Id. Therefore, defendants first need to determine which types of SNS plaintiffs use, where on those sites messages have been posted and the nature of the communication at issue. The location of the SNS postings influences considerably the right to privacy argument.

Publicly posted SNS messages relevant or potentially relevant to the issue in dispute can be discoverable. McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *4 (Pa. Ct. Common Pleas Sept. 9, 2010) (it would be unrealistic for Facebook user to expect that his disclosures on site would be considered confidential); Dexter v. Dexter, No. 2006-P-0051, 2007 Ohio App. LEXIS 2398, at *19 n.4 (Ohio Ct. App., May 25, 2007) (holding that custody-seeking parent could "harshly claim an expectation of privacy" in publicly accessible writings on MySpace detailing her intent to commence using drugs after completion of custody proceedings). Posters should expect a wide audience to view SNS postings, all but eliminating their right to privacy in the posting. See Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1130 (Cal. Ct. App. 2009) (holding plaintiffs' "affirmative act" of posting note on "hugely popular Internet site MySpace.com" exposed note to a vast audience). However, defendants will have little, if any, success subpoenaing Facebook and MySpace for the production of posted information without the consent of the plaintiff. The SCA prohibits electronic communication providers from disclosing their subscribers' communications absent subscriber consent or a federal criminal warrant. See Crispin v. Christian Audigier, Inc., No. 1:10-cv-2891, 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010); see also Burke, Social Networking Discovery: Get Used To It, DRI, Strictly Speaking, Vol. 7 Issue 3, Sept. 14, 2010. However, the Crispin court remanded the case to the magistrate to determine whether the public had access to plaintiff's postings or plaintiff had restricted access to them, potentially allowing defendants to subpoena a plaintiff's public Facebook or MySpace postings.

A unique feature of SNS is that they allow their subscribers to restrict access to their posts to designated "friends." However, a plaintiff cannot prevent discovery of potentially relevant information by unilaterally limiting access to SNS posts. See Simply Storage Mgmt., 2010 U.S. Dist. LEXIS 52766, at *9 ("merely locking a profile from public access does not prevent discovery"); see also Romano v. Steelcase, Inc., No. 2006-2233, 2010 N.Y. Misc. LEXIS 4538 (S.Ct. N.Y. Sept. 21, 2010). In Romano, the first reported decision of its kind in New York State Court, the New York Supreme Court, Suffolk County, recently ordered the production of a personal-injury plaintiff's Facebook and MySpace historical and current postings over her right to privacy arguments. Id. at *2. In Romano, plaintiff about her Facebook and MySpace public postings that revealed she traveled to Florida and Pennsylvania and had an active lifestyle despite her claims of permanent bodily injury and loss of enjoyment of life. When plaintiff refused to answer the questions, or provide defendant written authorization to subpoena the postings from Facebook and MySpace, defendant filed an Order to Show Cause to compel production of her current and deleted Facebook and MySpace postings. The court first focused on New York State's liberal discovery rules and the relevance and materiality of the public postings to defendant's defense. Next, it found that there was a reasonable likelihood that plaintiff's private postings contained relevant information, increasing the defendant's need for the information. Importantly, the trial judge found that plaintiff's "self-regulated privacy settings" should not prevent defendant from obtaining information that could be used to dispute her personal injury claims. Id. at *12.

The court also recognized that the SNS’ "privacy policies’ undermined plaintiffs’ privacy arguments. Facebook advises its users that they post information at their own risk and that personal information may become publicly available. Id. at *15-17 ("Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listing or other items, this information may become publicly available."). MySpace has a similar policy. Id. ("Although we allow you to set privacy options that
The court concluded that despite her privacy settings plaintiff consented to the public dissemination of her personal information and all but waived any claim to privacy in the posts. *Id.* at **16. Further, the Court of Common Pleas in Pennsylvania recently held that Facebook's access to a subscriber's posts negates a claim that private posts are confidential:

> Facebook users are thus put on notice that regardless of their subjective intentions when sharing information, their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook at its discretion. Implicit in those disclaimers, moreover, is that whomever else a user may or may not share certain information with, Facebook's operators have access to every post.


The *Romano* decision is sound and consistent with United States Supreme Court precedent that has "consistently held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland,* 442 U.S. 735, 743–44 (1979); *see McMillen,* 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *9-10 (["I]t is clear that no person choosing MySpace or Facebook as a communications forum could reasonably expect that his communications would remain confidential, as both sites clearly express the possibility of disclosure."). In fact, several circuits have held that a person lacks a legitimate expectation of privacy when information is posted or transmitted on-line because the person cannot prevent the recipient of the communication from forwarding the message to third parties. See *Guest v. Leis,* 255 F.3d 322, 333 (6th Cir. 2001), Some of these cases include: *Romano,* 130 S. Ct. 2619 (2010); *Quon,* 130 S. Ct. 2619 (2010); *McMillen,* 2011 F.3d at 843-844.

**Going Forward**

Several guiding principles emerge from the few reported decisions on the discoverability of SNS postings. Defendants do not have unfettered access to a plaintiff's private SNS postings. *Mackelpfang v. Fidelity Nat'l Title Agency of Nevada, Inc.,* No. 2:06-cv-00788, 2007 U.S. Dist. LEXIS 2379, at *21 (D. Nev. Jan. 9, 2007) (holding that defendant's request for plaintiff's private email messages on MySpace.com "cast too wide a net for any information that might be relevant and discoverable"). Courts have cautioned that such access would allow defendants to discover potentially embarrassing information communicated to third parties that is not relevant, discoverable or admissible. *See id.* However, the *Romano* and other decisions are encouraging despite the absence of a broad-based appellate pronouncement about the extent of a person's reasonable expectation of privacy in private SNS posts. They recognize, especially when plaintiffs raise pain and suffering and emotional distress/mental anguish claims, that the basis for plaintiffs' claims "will manifest itself in some SNS content, and an examination of that content might reveal" when the claim arose and the extent of the plaintiffs' injuries. *Simply Storage Mgmt.,* 2010 U.S. Dist. LEXIS 52766, at *13. At the same time, the decisions advise that narrowly tailored written discovery requests, focused deposition questioning and stipulated protective orders, rather than *in camera* reviews of SNS posts, are the preferred methods for counsel to secure information and resolve disagreements over the discoverability and relevancy of private SNS postings. Indeed, a more recent New York State Appellate Division decision denied a defendant's motion to compel plaintiff's Facebook posts because defendant was engaging in a fishing expedition, having not established the relevance of the alleged SNS posts to the case's disputed facts. *McCann v. Harleyville Ins. Co.,* No. 1179 CA 10-00612, 2010 N.Y. App. Div. LEXIS 8396 (N.Y. Nov. 12, 2010) (the court denied motion without prejudice to allow defendant to seek disclosure of posts in the future). Finally, when faced with a privacy challenge, defendants should not lose sight that the essence of SNS is to exchange thoughts, ideas and messages with the "public," no matter how "public" may be defined, regardless of the ability of a user to restrict access to the information, and that no privacy argument should be able to withstand the public nature of the sites. With Facebook's recent announcement that it will offer subscribers an e-mail address to expand their communication capabilities, the potential sources of discoverable information on SNS will only increase, thereby simultaneously raising the need for defendants to challenge a plaintiff's right to privacy arguments.

**Eric L. Probst** is counsel at Porzio, Bromberg & Newman, P.C. in Morristown, New Jersey and a member of the firm's Commercial Litigation Department. Mr. Probst represents clients in complex commercial, construction, products liability, and consumer fraud cases. He is a member of DRI and DRI's Electronic Discovery Practice Group. Mr. Probst has published and presented on the use of e-discovery requests against plaintiffs in pharmaceutical personal-injury matters.

More Places to Look: Social Networking and Cell Phone Evidence

*by John R. Mallory*

The changes to the Federal Rules of Civil Procedure in 2006 forced lawyers to start addressing electronically stored information ("ESI") as part of the discovery process.
This meant that those in the legal industry had to understand not only legal concepts but technical aspects of their client's computer networks and systems so that potentially relevant and responsive materials would not be overlooked. Decisions were rendered that put the onus on lawyers to ensure that their clients implemented and maintained a litigation hold during the entire legal process. After nearly four years, some lawyers have started to become comfortable with eDiscovery and the new concepts and terminology associated with the process. But technology is constantly changing and evolving. New forms of communication are created and new, smaller and faster computers and devices hit the market. Many devices now have embedded systems that capture data that can be recovered, reviewed, and produced during discovery. The “black boxes” inside cranes can record the status of the crane when it collapses. The signals at train crossings capture information relating to when the lights go on, when the arms go down and for how long they are active. The computers that control surgical robots store video files of surgeries that can be produced during malpractice lawsuits. A person’s shopping habits are stored electronically by the use of a frequent shopper card. While used primarily for marketing purposes, the information could potentially be recovered and used in a product liability matter. The list of devices that can store data will continue to grow. It is important to keep track of new sources of evidence so that nothing is overlooked that could be helpful to your clients.

One of the newest technologies to be embraced are social networking sites. These sites provide the ability to reconnect with old friends, classmates, and family members. Pictures can be shared, feelings expressed, travel plans divulged, and opinions can be disseminated. On the surface, social networking looks like a useful and fun creation. But as with any technology, lurking under the surface is the potential for abuse, and therefore the potential for problems.

Social networking is no longer relegated to teenagers and college students but to every age and walk of life. To understand how prevalent social networking has become, one only has to look at the statistics surrounding Facebook, the largest and most popular social networking site, available at http://www.facebook.com/press/info.php?statistics.

- More than 500 million active users
- 50% of our active users log on to Facebook in any given day
- Average user has 130 friends
- People spend over 700 billion minutes per month on Facebook
- About 70% of Facebook users are outside the United States
- There are more than 200 million users currently accessing Facebook through their mobile devices

For many, posting status updates to Facebook is much easier and more efficient than sending out an e-mail message. A status update will be received by all of your friends at the same time. Status updates occur in real-time. Status updates can be sent from a mobile device and with the recently added “Places” feature it is possible to tell everyone exactly where you are just by clicking a pushpin icon on your phone.

By looking at some of the statistics listed above it is easy to see that one of the issues surrounding social networking is productivity. While some organizations have filters in place to prevent their employees from accessing these sites, others do not. It is much more fun posting status updates and viewing your friends’ posts than it is to generate a revenue report for the last quarter.

One of the most publicized issues surrounding social networking is “cyberbullying.” There is nothing to stop someone from posting hateful, derogatory or insulting posts to a social networking page. These types of posts combined with the traditional “in person” comments and actions can be too much for some people. The news is filled with stories relating the tragic suicides of people that simply couldn’t take it anymore.

Something else a person needs to consider when posting on a social networking site is what impact will the post (or photo) have on their image. Pictures and posts that describe or display inappropriate behavior could have a deleterious impact on a person’s image. Schoolteachers, members of the clergy, aspiring politicians, and business professionals have to be very careful what they post. Knowing what witnesses or testifying experts are posting on their social networking pages might prove interesting.

Another threat posed by social networking sites is that there is nothing to stop employees from posting confidential or proprietary information on their social networking pages. Comments like, “I just learned today that our CEO is leaving. What a drag, he really turned this company around.” or “We just came out with a brand new product today. Don’t buy it, it’s really a piece of junk.” could have significant consequences to shareholders and the bottom line. Even if an organization has a policy prohibiting posting to social networking sites, how can it be enforced?

An often overlooked risk with using social networking sites is that frequently posting one’s activities and locations can have unforeseen consequences. A man who posts that he is about to take his family on a much anticipated two week vacation is announcing that his home will be empty for the next two weeks. This is an invitation to people to “rob me blind.”

Many people think that because they have configured their privacy settings that the above mentioned items are not an issue. Even if posts are set to “friends only,” there is nothing to stop a “friend” from passing on any information they wish. Those that feel that their posts are private
should look at several recent decisions such as Romano v. Steelcase, Inc.http://www.facebook.com/policy.php—last visited 11/15/10. " In McMillen v. Hummingbird Speedway, Inc., the court stated, "Facebook users are thus put on notice that regardless of their subjective intentions when sharing information, their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook at its discretion. Implicit in those disclaimers, moreover, is that whomever else a user may or may not share certain information with Facebook's operators have access to every post." (Supreme Court, Suffolk Co. NY 2010) WL 3703242 and McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD (C.P. Jefferson, Sept. 9, 2010) where courts have required access to the private portions of social networking pages. In Romano v. Steelcase, Inc., the court stated, "The information sought by Defendant regarding Plaintiff's Facebook and MySpace accounts is both material and necessary to the defense of this action and/or could lead to admissible evidence. In this regard, it appears that Plaintiff's public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed. In light of the fact that the public portions of Plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action." And a person expects that their posts will never be seen by anyone else has not read Facebook's Privacy Policy, "We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law".

While attempting to gain access to a party's social networking posts, keep in mind that there may be other methods that can be employed that may not require filing a motion with the court.

If you are attempting to determine with whom a person may be sharing their information there are a series of products offered by Lococitato that can visually map a person's social network. See http://www.lococitato.com. These products include YouTube Visualizer and MySpace Visualizer. They also have a product called Facebook Visualizer, but currently this product is only available to law enforcement. The products are inexpensive, around $35, actual cost depends on the exchange rate as Lococitato is located in the UK.

In addition to being unaware of a social networking site's privacy policy, people don't understand that many of their posts and activities are captured on their local hard drive, even if they are using a web based provider. This is great from an investigative perspective as people can use social networking sites and associated tools to communicate "out of band" because they think their posts and discussions are not recoverable.

As an example, a person's Facebook activity is captured in a person's internet history. This includes pages visited as well as status updates. The following table shows information about the author's Facebook activity. The item in bold is a Facebook status update:

<table>
<thead>
<tr>
<th>Date Last Visited</th>
<th>Hits</th>
<th>Page Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/1/2010 12:00:57 PM Thu</td>
<td>19</td>
<td>Login</td>
</tr>
<tr>
<td>4/1/2010 12:00:53 PM Thu</td>
<td>2</td>
<td>Facebook</td>
</tr>
<tr>
<td>4/1/2010 12:00:07 PM Thu</td>
<td>2</td>
<td>Facebook</td>
</tr>
<tr>
<td>4/1/2010 11:59:54 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>4/1/2010 11:59:08 AM Thu</td>
<td>1</td>
<td>Springfield Metropolitan Bar Association: SMBA events in November</td>
</tr>
<tr>
<td>4/1/2010 11:58:55 AM Thu</td>
<td>1</td>
<td>SMBA</td>
</tr>
<tr>
<td>3/25/2010 10:58:01 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>3/25/2010 10:57:46 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>3/25/2010 10:57:33 AM Thu</td>
<td>53</td>
<td>Facebook (3)</td>
</tr>
<tr>
<td>3/25/2010 10:14:17 AM Thu</td>
<td>53</td>
<td>Facebook (3)</td>
</tr>
<tr>
<td>3/25/2010 10:10:44 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>3/25/2010 10:09:55 AM Thu</td>
<td>19</td>
<td>Login</td>
</tr>
<tr>
<td>3/25/2010 10:09:55 AM Thu</td>
<td>5</td>
<td>Facebook</td>
</tr>
</tbody>
</table>

What can be gathered from this information is the number of visits to a particular page, status updates and the date and time the page was visited or the time the update was posted. While collecting the internet history from a computer and searching for relevant materials sounds complex, the process is fairly automated and requires very little "hands on" time.

Many social networking sites also provide "chat" capabilities. Once again, most people don't know that it is possible to recover deleted chat communications. Chat sessions from Facebook, Google Talk, MySpace, Bebo, and Skype, among others can be recovered. The following table shows Facebook chat sessions recovered in a recent case. The names have been changed and the Facebook id's have been obfuscated:

<table>
<thead>
<tr>
<th>Date Last Visited</th>
<th>Hits</th>
<th>Page Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/1/2010 12:00:57 PM Thu</td>
<td>19</td>
<td>Login</td>
</tr>
<tr>
<td>4/1/2010 12:00:53 PM Thu</td>
<td>2</td>
<td>Facebook</td>
</tr>
<tr>
<td>4/1/2010 12:00:07 PM Thu</td>
<td>2</td>
<td>Facebook</td>
</tr>
<tr>
<td>4/1/2010 11:59:54 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>4/1/2010 11:59:08 AM Thu</td>
<td>1</td>
<td>Springfield Metropolitan Bar Association: SMBA events in November</td>
</tr>
<tr>
<td>4/1/2010 11:58:55 AM Thu</td>
<td>1</td>
<td>SMBA</td>
</tr>
<tr>
<td>3/25/2010 10:58:01 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>3/25/2010 10:57:46 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>3/25/2010 10:57:33 AM Thu</td>
<td>53</td>
<td>Facebook (3)</td>
</tr>
<tr>
<td>3/25/2010 10:14:17 AM Thu</td>
<td>53</td>
<td>Facebook (3)</td>
</tr>
<tr>
<td>3/25/2010 10:10:44 AM Thu</td>
<td>1</td>
<td>Facebook</td>
</tr>
<tr>
<td>3/25/2010 10:09:55 AM Thu</td>
<td>19</td>
<td>Login</td>
</tr>
<tr>
<td>3/25/2010 10:09:55 AM Thu</td>
<td>5</td>
<td>Facebook</td>
</tr>
</tbody>
</table>
This type of information shows chat contents, date of communication, party names (although these could be fictitious) and Facebook id. The Facebook id can be used to visit that person's Facebook page. Simply craft a url like this, http://www.facebook.com/profile.php?id=XXXXXXXXX, where the actual id is used in place of the X's. If a page is private, this activity many not get you much information, but it could get friends' names, a profile picture, and perhaps location. You must have a valid Facebook account in order to accomplish this.

Another source of "out of band" communications can be cell phones. It is important to recognize that the phones we use today are essentially computers. The iPhone runs a scaled down version of the same operating system used on a MacBook Pro. Because of the power of our handheld devices, one must keep in mind that they can store, create and transmit, Word, Excel, PowerPoint, and PDF files. They can take pictures, send, and receive e-mail and text messages, etc. In fact there are some people (this author included) that have e-mail accounts they only check with their cell phones. If you want to capture a person's entire universe of e-mail communication and you don't request or examine his cell phone, you may miss some relevant information.

Unfortunately, the ability to analyze cell phones is still in its infancy. Despite what vendors might say, what can be recovered from cell phones often depends on make, model and carrier. And the model listed on the front of the device may not actually match what is inside the case. What can often be the most problematic part of examining a cell phone is getting a hold of the proper cable with which to conduct the analysis. Since there is currently no standardization in the U.S., many phones require proprietary cables.

While the process of examining a phone can be cumbersome, there is some hope if you are interested in recovering cell phone data. If it is not possible to get a hold of the relevant phones for the parties in a case, it might be possible to recover the relevant data from a phone backup. Users may backup their phones to their computer for disaster recovery purposes, but some phones, the iPhone in particular, automatically backs up its data whenever it is synced. During a recent investigation, the author was provided with an iPhone and the user's laptop computer. The lawyer was really hoping to recover text messages from the phone. Unfortunately there were no text messages on the phone as the user had deleted them prior to returning the phone to her employer. However, a backup existed on her computer that contained over 3,000 text messages.

In addition to text messages, the iPhone backup files contain an incredible amount of information (unfortunately not e-mail). Intact, playable voice mail messages can be recovered. Call history and contacts are recoverable. Google Maps searches are available. Bookmarks and Internet history are also available for review.

One of the more interesting items that can be retrieved from an iPhone backup involves photographs taken with the phone. Many people don't realize that when they take a picture with their iPhone, the longitude and latitude of where that picture was taken is added to the picture. This information can be used to refute someone's claim that they had never been in a particular location. What is even more interesting is that when these photos get posted to some social networking sites, this location information remains intact (Facebook apparently strips this information).
The items listed here are just a sample of what can be recovered from cell phones and social network activity. Wikipedia lists approximately 175 social networking sites—many of them are culture and age specific. Do not overlook the fact that a party to litigation may be using one of these to express their innermost thoughts and activities.

The eDiscovery landscape will continue to change. Digital data will continue to be a multi-tentacled beast that constantly changes and evolves. Staying up to date on these changes can help you identify data storage locations that could contain relevant materials.

John R. Mallery is a member of BKD, LLP's Forensics & Valuation Services group and specializes in the practical applications of computer forensics and network security. He works as a consulting expert in a wide range of litigation matters, providing assistance with electronic discovery requests, deposition questions and clarification of technology issues.

Recognizing the Complexities of E-Discovery Preservation
by G. Franklin McKnight IV, Kymberly Kochis and John F. Mullen Sr.

For litigants and their counsel, e-discovery preservation can be a complex and difficult area of litigation to navigate. Although judicial decisions on the subject of preservation are becoming commonplace, publicized orders and opinions do not generally compliment clients and their counsel. In fact, most decisions cause attorneys to reflect on whether their clients could be at risk of creating similar unfavorable decisions, and what preemptive steps must be taken and costs incurred to eliminate such risks. As companies, counsel and the judiciary are confronted with the intricacies of e-discovery preservation, the potential for missteps becomes evident. When allegations of such missteps occur, a party's ability to develop a succinct and understandable defense in this tech-driven area, while challenging, is key to helping the Court with the difficult task of weighing the reasonableness of a party's e-discovery efforts.

A Litigant's Preservation Responsibilities

As parties and counsel are required to navigate the complex preservation landscape, they must be cognizant of their responsibilities and vigilant that those responsibilities are fulfilled. Because the scope of e-discovery is subject to divergent opinions, and the existence and location of relevant information within a complex computing architecture may be difficult to reasonably identify without well thought-out investigatory efforts, parties and counsel must understand the steps necessary to fulfill their preservation obligations as well as when those efforts fall short. This is not easy. According to Kroll Ontrack's "Fourth Annual ESI Trends Report," the preservation and the collection of data were survey respondents' biggest discovery concerns, followed by changing technology platforms, compliance with discovery obligations and unforeseen costs. See Kroll Ontrack, Fourth Annual ESI Trends Report (2010) at 10. While Southern District of New York Judge Shira Scheindlin, in the Zubulake and Pension Committee decisions, elaborated extensively on litigants' preservation obligations, both decisions left many readers with the conclusion that the steps to comply with preservation obligations are not easily accomplished, and that noncompliance can be costly. See Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004); Pension Comm. of the Univ. of Montreal Pension Plan v. Bank of Am. Sec., LLC, 685 F. Supp. 2d 456 (S.D.N.Y. 2010).

The Pension Committee decision provides an excellent example of the in-depth look Courts may take when analyzing whether a party's preservation and collection obligations have been met and demonstrates several potential pitfalls parties can encounter. While Judge Scheindlin prefaced the opinion with the statement that "Courts cannot and do not expect that any party can meet a standard of perfection," the framework set forth in that opinion, when applied to today's technology standards, in no way suggests easy application absent the costly decision to preserve very broadly and collect thoroughly. At the outset, the Court admits that the continuum of conduct from what's acceptable through what's unacceptable cannot be measured with exactitude. The Court stresses that the imposition of sanctions is a judgment-call and a "guilt reaction" based on experience as to whether a party complied with ESI discovery obligations and—perhaps more interestingly—how far it worked to comply. See Pension Comm., 685 F. Supp. 2d at 471. As a baseline, Pension Committee held that the failure to meet contemporary discovery standards, such as issuing a litigation hold, identifying key players, and ensuring that their records are preserved and ceasing the deletion of email, should be considered gross, rather than ordinary negligence. In contrast, the Court found that the failure to collect records from other employees constituted ordinary negligence. Bearing this in mind, the Pension Committee decision turns on measuring to what extent certain parties' conduct was unreasonable and the extent to which the innocent parties were harmed. This subjective determination guides the Court's assessment on the type and degree of sanctions warranted under the circumstances.

Once the obligation to preserve exists and relevant evidence is alleged to have been destroyed, lost or simply not produced, the Pension Committee analysis is consulted in weighing the spoiling party's culpability as well as the prejudice imposed upon the innocent party. Because negligence results even from a "pure heart and empty head," and managing technology is a
complex and constant process, the line between reasonably prudent and negligent can be vague. See id. at 464. By the time hindsight sheds light on potential gaps in preservation, it may be too late. This uncertainty makes meeting the required standard of care dependent on skilled employees, knowledgeable in their defined preservation duties that have the foresight to understand the scope of information to be preserved and where such information is located.

The facts in Pension Committee gave the Court plenty of reason to engage in an in-depth discussion of the parties’ preservation efforts. In that case, it was defendants who sought sanctions against multiple plaintiffs for discovery violations. With multiple plaintiffs and co-defendants involved in the action, defendants’ cross-referenced the other parties’ productions and found evidence that certain documents should have been produced by particular plaintiffs, but were not. This discovery failure provided sufficient support for defendants to investigate whether plaintiffs had met their preservation obligations as of the day when they reasonably anticipated litigation and the duty to preserve arose. Despite attempts by plaintiffs to justify the preservation steps they undertook, the Court found that they failed to fulfill their responsibilities.

Addressing counsel's initial notification to plaintiffs explaining plaintiffs' preservation obligations, the Court found that it failed the standard for a proper litigation hold—it was deficient in directing employees to preserve relevant records—and, perhaps more noteworthy, also failed to provide a mechanism for the collection of the preserved records, suggesting an immediacy to both obligations. The Court likewise found that the directive's reliance on employees to identify relevant documents, without supervision from counsel, was deficient. The eventual institution of a written litigation hold four years later was similarly unacceptable and did nothing to cure the earlier deficiency. Other discovery violations by specific plaintiffs were noted, including use of deficient searches, delegating search efforts to inexperienced personnel and destroying backup data potentially containing responsive information not otherwise available. See id. at 479.

After learning of the discovery violations, the Court ordered plaintiffs to provide declarations discussing their efforts to preserve and produce documents. Plaintiff's candor towards the Court in this regard fared no better than its deficient litigation hold efforts, with the eventual revelation that almost all of the declarations were false and misleading and/or executed by a declarant without personal knowledge. Considering these findings, the Court accepted defendants' argument that the lack of records discussing substantive matters that certainly would have been documented by plaintiffs lead inexorably to the conclusion that relevant records were lost or destroyed, although no direct proof of such records existed.

Regarding culpability, the Court found that plaintiffs' pre-2005 conduct ranged from negligent to grossly negligent. With respect to plaintiffs who were grossly negligent, the Court found that prejudice existed such that an adverse inference jury instruction was warranted. The jury was permitted to presume the relevance of the missing documents and the resulting prejudice to defendants, subject to plaintiffs’ ability to rebut the presumption. The Court also awarded monetary sanctions. For plaintiffs that were guilty of ordinary negligence, the Court found that monetary sanctions alone were appropriate. Interestingly, the Court opined that had defendants demonstrated that plaintiffs destroyed documents after 2005—when the matter was transferred to this Court—such conduct would have justified more severe sanctions.

The Pension Committee decision provides a number of practice pointers to litigants. As the decision demonstrates, contemporary discovery standards represent the minimum requirements litigants must achieve to avoid allegations of discovery misconduct. While the decision provides examples of such standards, litigators are well-advised to stay abreast of new developments affecting those standards to update once-acceptable procedures that may now fall short. It also shows that resolving motions relating to the spoliation of evidence can be time-consuming, distracting, and expensive to the parties and the Court. Finally, with respect to substantive matters, the decision shows that a spoliation finding can jeopardize a party's prosecution or defense of its case. Considering the complex technical foundation on which e-discovery rests, parties are well-advised to formally develop and re-evaluate procedures to fulfill their litigation responsibilities and—importantly—be open and candid with the Court and opposing counsel if relevant information is lost or destroyed.

Cooperating to Meet Preservation Obligations

While decisions like Pension Committee help guide litigators along the path of proper preservation, cooperation can be an important tool in meeting preservation responsibilities. Because Courts encourage parties to reach agreement on solutions to e-discovery issues, having the scope of e-discovery defined early in the litigation can help identify the expectations each party has with respect to the scope of e-discovery. Conversely, a failure to cooperate can provoke a Court's ire. For instance, in Home Design Services, Inc. v. Trumble, the Court admonished plaintiff for its dilatory discovery and pointed out that a litigator has an equally important role as a case manager. No. 09-cv-00964, 2010 WL 1435382 (D. Colo. Apr. 9 2010) at *5. The Court noted that counsel's case management responsibilities should not be seen as antithetical to the role of advocate, because a well-managed case progresses through discovery more efficiently and cost-effectively. See id. Citing to "The Sedona Conference Cooperation Proclamation," the Court reminded counsel that while they are "retained to be zealous advocates for their clients, they bear a professional obligation to conduct discovery in a diligent and candid
Parties that demonstrate considerable recalcitrance in cooperating may be ordered to do so by a disgruntled judge, as Courts have a responsibility towards case management. See id. at 5. In Burt Hill, Inc. v. Hassan, the Court found that defense counsel unethically retained a document provided by an anonymous source that, on its face, was privileged. No. Civ. A. 09-1285, 2010 WL 419433 (W.D. Pa. Jan. 29, 2010). Besides requiring that defendants return the documents (along with the imposition of other measures to protect plaintiffs), the Court required that the parties promptly meet and confer to determine whether the scope of one of defendants' Requests for Production could be narrowed, and whether agreement could be reached on the use of search terms. See id. at 10. A similar result occurred in Ross v. Abercrombie & Fitch Co., where, after granting plaintiffs' Motion to Compel, the Court ordered that the parties meet-and-confer on ways in which the information plaintiff was seeking could be obtained, and how much in terms of time and money any electronic search might cost. No. 2:05-cv-0819, 2010 WL 1957802 (S.D. Ohio May 14, 2010) at 4. Finally, in Multiven, Inc. v. Cisco Systems, Inc., the Court found that the dilatory review process the parties put in place was far too slow and a new method for review and production was needed. In that regard, the Court ordered the parties to retain a third party vendor to assist with "the further collection, search, review and production of documents" and that the parties split the costs. No. 5:08-cv-05391, 2010 WL 2813618 (N.D. Cal. Jul. 9, 2010) at 3. The Court also ordered that the Special Master's duties be expanded to include "full authority to choose a third party vendor, craft a search protocol, establish deadlines and otherwise resolve any future discovery disputes or objections." Id.

Cooperation can be an important consideration in obtaining greater certainty that a party's preservation obligations have been met and establishing before the Court that e-discovery responsibilities have been addressed. By working with the opposing party to define the scope of the information sought, a party can better define its preservation obligations in line with key individuals and information systems. Also, by establishing adequate boundaries for e-discovery, the parties can address any issues that arise within a pre-determined framework, mitigating against unfair accusations of spoliation.

Clarifying Preservation Responsibilities under the Federal Rules

Recognizing the breadth of e-discovery in litigation, companies have expressed their reservations about their ability to consistently comply with their preservation obligations. The difficulties inherent in meeting such obligations have not gone unnoticed by the bench and bar. According to Fulbright's "7th Annual Litigation Trends Survey," 68% of respondents indicated that the duty to preserve is not sufficiently clear. See Fulbright & Jaworski L.L.P., Fulbright's 7th Annual Litigation Trends Survey Report (2010) at 54. In an Executive Summary by the E-Discovery Panel at the Duke Conference on Civil Litigation (comprised of Judges Scheindlin and Facciola, and Messrs. Allman, Barkett, Garrison, Joseph and Willoughby), the panel urged the Federal Rules Advisory Committee to consider a rule addressing preservation and spoliation. See Memo from Gregory P. Joseph to Hon. Richard G. Koelll Re: Executive Summary: E-Discovery Panel, Duke Conference on Civil Litigation, May 11, 2010. The purpose of such a rule would be to better define the principles governing when the preservation duty attaches (when a party reasonably anticipates litigation) and the scope of that duty (relevant evidence within a party's control). See Fujitsu Ltd. v. Federal Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) and Treppel v. Biovail, 249 F.R.D. 111, 118 (S.D.N.Y. 2008).

The E-Discovery Panel's Executive Summary provides an outline of potential provisions to be included in a preservation rule. All panel members agreed that such a rule should treat large cases with enormous discovery differently. Provisions suggested, but not necessarily agreed to by all panel members, include specific triggers defining when the preservation obligation attaches and specific parameters defining the scope of a party's preservation obligations with respect to timeframe, subject matter, data types and data sources. The panel suggested considering whether presumptive limits should be applied to the key custodians and the types of data or sources that must be searched, as well as whether duties should differ for parties and non-parties. The proposal offered that dissemination of a litigation hold notice should be evidence of due care on the part of the party issuing it, and that consideration should be given as to whether actions taken in furtherance of the preservation duty are privileged. Finally, the proposal suggested that the consequences for non-compliance and the procedures to be taken by parties involved in a discovery dispute be specifically set forth.

Considering the general standards offered to litigants on when the duty to preserve arises and its scope as compared to the complex considerations often necessary to meet those standards, the development of a Federal Rule on the duty to preserve would be a welcome step. However, without doubt, the provisions of such a rule will be hotly debated. Specifics regarding what must be preserved, what sanctions are acceptable for different degrees of non-compliance and when a party must disclose that it has reason to believe that relevant information might have been lost may be difficult to define. Efforts to balance the concept of reasonable preservation and collection costs against the inherent power of the Courts to preserve the integrity of a judicial process, working to uncover the truth and Rule 26’s standard for relevant evidence, may be a narrow tightrope to walk. See Pension Comm., 685 F. Supp. 2d at 466.
Conclusion

Meeting preservation obligations remains a difficult road for parties. Although Court rules and decisions provide a framework for such compliance, effectively fulfilling the obligations set forth inevitably falls to the litigant who must effectively apply its duties to the practices of the organization. The information technology platforms utilized by companies can be varied and complex. Determining whether e-discovery obligations are being satisfied requires a thorough understanding of the litigant's organization, including what information they store, the destruction policies applicable to them, and their capability to preserve and export relevant information in a reasonably-useable form. Because each case may raise its own specific preservation and collection issues, and the parties may have different ideas of what constitutes relevant information, meeting and conferring on preservation is an important step in clarifying expectations. Finally, litigants should recognize the sometimes painful necessity of bringing preservation disagreements to the Court before spoliation issues arise.

G. Franklin McKnight IV, an associate at Nelson Levine de Luca & Horst, represents insurance company clients in institutional matters and applies his understanding of technology and knowledge management to develop strategic solutions to legal concerns. Mr. McKnight can be reached at 215-358-5197 or at fmcknight@nldhlaw.com.

John F. Mullen, Sr. heads the Complex Litigation Practice Group at Nelson Levine de Luca & Horst where he focuses his practice on a combination of mass tort, construction and data privacy litigation. Mr. Mullen can be reached at 215-358-5154 or at jmullen@nldhlaw.com.

Kymberly Kochis is a partner at Nelson Levine de Luca & Horst where she represents clients in insurance and reinsurance litigation and regulatory matters as well as corporate governance. Ms. Kochis can be reached at 212-233-2906 or kkochis@nldhlaw.com.

Proportionality, Reasonability, and Sanctions: Victor Stanley II

by Angela Scafuri

One of the most interesting and thought provoking decisions to come out of the courts this year is the decision in Victor Stanley v. Creative Pipe, Inc. et al., No. MJG-06-2662, 2010 U.S. Dist. LEXIS 93644 (Sept. 9, 2010) (“Victor Stanley II”). While much of the focus this year has centered on the Pension Committee opinion, the Victor Stanley opinion takes a closer look at the concept of proportionality and reasonableness, using a case of wholly egregious preservation failures as a spring board for a thought provoking discussion regarding preservation of ESI. See, e.g., Pension Comm. of the Univ. of Montreal Pension Plan v. Bank of Am. Sec., LLC., 685 F. Supp. 2d 456 (S.D.N.Y. 2010). Emphasizing proportionality and reasonableness in preservation efforts, Victor Stanley II provides an excellent roadmap for all attorneys and corporate clients struggling with compliance issues surrounding e-discovery obligations. Of equal significance, not only does Victor Stanley II provide a working roadmap, but it also demonstrates that courts will not flinch at imposing severe sanctions, including jail time, for egregious non-compliance with e-discovery obligations. Thus, the Victor Stanley II opinion should be given considerable weight for both its attempt to provide a much needed voice for the well-reasoned premise of proportionality and reasonability in all things, including e-discovery, as well as an advancement of the law of sanctions for ESI preservation failures.

In Victor Stanley II, the Court was faced with what to do with a corporate litigant (and its president) that freely chose to ignore litigation holds and court orders. Defendants, Creative Pipe, Inc. ("CPI") and its president, Mike Pappas ("Pappas") essentially "thumbed their nose" at the Court. Indeed, the Court itself stated that Defendants abuses in this matter account for " . . . the single most egregious example of spoliation that I have encountered in any case that I have handled or in any case described in the legion of spoliation cases I have read in nearly fourteen years on the bench." Victor Stanley II, 2010 U.S. Dist. LEXIS 93644, at *60.

The e-discovery spoliation included both attempted and successful permanent deletions of ESI, as well as what the Court determined to be eight specific, discrete preservation failures:

(1) Pappas's failure to implement a litigation hold; (2) Pappas's deletions of ESI soon after VSI [Victor Stanley, Inc.] filed suit; (3) Pappas's failure to preserve his external hard drive after Plaintiff demanded preservation of ESI; (4) Pappas's failure to preserve files and emails after Plaintiff demanded their preservation; (5) Pappas's deletion of ESI after the Court issued its first preservation order; (6) Pappas's continued deletion of ESI and use of programs to permanently remove files after the Court admonished the parties of their duty to preserve evidence and issued its second preservation order; (7) Pappas's failure to preserve ESI when he replaced the CPI server; and (8) Pappas's further use of programs to permanently delete ESI after the Court issued numerous protection orders.

Id. at *11-12.

Creating the above list of e-discovery abuses was an arduous task in and of itself, based on the prolific and vagrant discovery abuses which Defendants engaged in over the course of several
years as well as countless motions, hearings, and even a succession of defense counsel. While no means an exhaustive list, the following vignettes highlight Defendants' transgressions:

- Large deletions of ESI occurred on the "eve of scheduled discovery regarding the contents of [Defendant] Pappas's work computer. First, the Court scheduled a discovery hearing for February 1, 2007 and the afternoon before, Pappas deleted 9,234 files from his work computer, a password-protected laptop. Second, an imaging of [Defendant] Pappas's work computer was scheduled for the week of February 21, 2007. Pappas deleted almost 4,000 files on February 16 and 17, 2007 and someone ran Microsoft Windows's Disk Defragmenter program immediately afterward, rendering the files unrecoverable." *Id.* at *21-22.

- Defendants did not present any evidence to show that Defendants "considered, let alone implemented, a litigation hold after Plaintiff filed suit or after the Court issued preservation orders." *Id.* at *24.

- [Defendant] CPI named one of its product lines the 'Fuvista' line. [Defendant] Pappas admitted during discovery that 'Fuvista' stood for . . . you Victor Stanley." . . . demonstrating that Pappas's wit transcended sophomoric pranks . . . and extended to inventing insulting acronyms to name his competing products. When disclosed, the meaning of this acronym removes any doubt about his motive and intent. No doubt Pappas regarded this as hilarious at the time. It is less likely that he still does." *Id.* at 35-36, h. 19.

- After an Order on December 22, 2006 cautioned the parties of "their substantive duty to preserve evidence, including electronic evidence. . . . Subsequent forensic examination of Defendants' computers showed that the CPI System Registry reflected 9,282 user-pasted deletions of file between [the] December 22, 2006 order and the February 1, 2007 discovery hearing . . . Given the file names, it is evident that the files were relevant and would have supported Plaintiff's case . . . " *Id.* at *40, *41, *44-45.

- "[F]ollowing a series of ESI preservation and production orders by the Court, Defendants allowed their computer consultant to run programs that eliminated temporary internet files. It cannot be ignored that this occurred in a case the essence of which involves surreptitious entry to Plaintiff's website for the purposes of downloading design drawings that Defendants then pirated and misrepresented to be their own in order to compete with Plaintiff. It is no coincidence that the deleted files included those showing the internet site that Defendants had accessed. I am persuaded that these files were relevant, and that their loss caused prejudice to Plaintiff." *Id.* at *58.

As demonstrated from the above, limited, examples, the Defendants in *Victor Stanley II* surpass mere negligence, and dive straight into bad faith spoliation of ESI. As the Court noted: "Plaintiff has proved grave misconduct that was undertaken for the purpose of thwarting Plaintiff's ability to prove its case and for the express purpose of hamstringing this Court's ability to effect a just, speedy, and inexpensive resolution of a serious commercial tort." *Id.* at *61

Before addressing the appropriate punishment for such flagrant e-discovery abuses, the Court takes the time to discuss that it is not demanding "perfection" in preservation and collection efforts, but emphasizes the growing need for *proportionality and reasonableness* when undertaking e-discovery obligations. It is clear from the opinion that the Court is very sensitive to the concerns of the legal community regarding burgeoning costs associated with e-discovery as well as the, at times, unrealistic burdens placed on both litigants and counsel with respect to preservation and collection efforts. *See id.* at *67-68. The Court specifically emphasizes in its Opinion that nothing in the text of the opinion should add to the "collective anxiety," because, in the *Victor Stanley II* matter, Defendants actually admitted the egregious conduct:

> Defendants do not dispute that spoliation took place, relevant evidence was lost, and Plaintiff was prejudiced accordingly; that Defendants’ misconduct was sufficiently egregious to warrant sanctions; and that the sanctions warranted are serious. Nor is this a case where Defendants have claimed or demonstrated that what they did was reasonable and involved effort and expense that were proportional to what is at stake in the litigation.

*Id.* at *68.

While the Defendants in *Victor Stanley II* engaged in egregious acts of spoliation of ESI warranting sanctions, the Court provides guidance to counsel to focus on proportionality and reasonableness in preservation requests and efforts. "Whether preservation or discovery conduct is acceptable in a case depends on what is reasonable, and that in turn depends on whether what was done—or not done—was proportional to that case and consistent with clearly established applicable standards." *See id.* at *89 (citing Rinkus Consulting Group, Inc., v. Cammarata, 868 F. Supp. 2d 598, 613 (S.D. Tex. 2010)) (emphasis in original). In other words, the scope of the preservation request should be proportional to the amount in controversy and the costs and burdens of the preservation effort. The *Victor Stanley II* Court takes the call for proportionality and reasonableness a step further by pointing out all of the jurisdictions that have, perhaps, "overlooked" this critical need for balance and citing the Federal Rules for support of the proposition:
Although, with few exceptions, such as the recent and highly instructive Rinkus decision, courts have tended to overlook the importance of proportionality in determining whether a party has complied with its duty to preserve evidence in a particular case, this should not be the case because Fed. R. Civ. P. 26(b)(2)(C) cautions that all permissible discovery must be measured against the yardstick of proportionality. Moreover, the permissible scope of discovery as set forth in Rule 26(b) includes a proportionality concept of sorts with respect to discovery of ESI, because Rule 26(b)(2)(B) permits a party to refuse to produce ESI if it is not reasonably accessible without undue burden and expense. Similarly, Rule 26(g)(1)(B)(iii) requires all parties seeking discovery to certify that the request is “neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, the amount in controversy, and the importance of the issues at stake in the action.” Thus, assessment of reasonableness and proportionality should be at the forefront of all inquiries into whether a party has fulfilled its duty to preserve relevant evidence.

Id. at *89-91 (internal citations omitted).

Based on Defendants bad faith e-discovery abuses, the Court was taxed with the task of fashioning an appropriate sanction. The Court did not rely on its inherent powers to impose sanctions, but, instead, relied upon Federal Rule of Civil Procedure 37 for the imposition of sanctions as multiple discovery orders were disobeyed or otherwise ignored. See id. at *76. Defendants objected to the imposition of sanctions under Rule 37 under a very specious argument—that the discovery orders required preservation of evidence, not production of documents. The Court properly rejected the argument, finding:

On its face, Rule 37(b)(2) permits sanctions for disobedience of “an order to provide or permit discovery...[t]he rule does not define what is meant by “provide or permit” discovery, but the advisory committee’s notes to Rule 37 reflect that subsection (b) was amended in 1970 to broaden its ability of a court to sanction for a violation of discovery...[[t]t cannot seriously be questioned that a court order to preserve information, including ESI, has as its core purpose the objective of ensuring that the ESI can be “preserved” during discovery, and is intended to “permit” that discovery. It would clearly violate the purpose of Rule 37(b) if a court were unable to sanction a party for violating the court’s order to preserve ESI simply because that order did not also order the production of the evidence. ...[T]he duty to preserve relevant evidence is a common law duty, not a rule-based duty. It therefore is no surprise that Rule 37(b)(2) does not specifically refer to court orders to “preserve” evidence. The reference to Rule 26(f), however, which does specifically refer to preservation obligations, makes it clear that court orders issued to enforce discovery plans agreed to by the parties, which include preservation obligations, would be enforceable by Rule 37(b)(2) sanctions. If so, then it is equally compelling that a preservation order issued by the court sua sponte, and designed to govern the discovery process by ensuring that evidence be preserved, if within the scope of discoverable information, may be provided in response to an appropriate discovery request, also is an order to “permit discovery.” To reach a contrary conclusion would be to exalt form over substance.

Id. at *76-78.

In addressing the appropriate sanctions, the Court determined that proportionality and reasonableness “are not at issue because Defendants have never alleged that it would have been an undue burden for them to preserve the ESI they destroyed.” Id. at *111. The Court also examined the “culpability of the state of mind” of the spoliator, Pappas, determining that “[[n]sum, Defendants took repeated, deliberate measures to prevent the discovery of relevant ESI, clearly acting in bad faith, and in affidavits, depositions, and in open court, Pappas nonchalantly lied about what he had done.” Id. at *122-123.

Ultimately finding that Defendant Pappas acted in bad faith, the Court next goes on to consider the relevance of the lost evidence and the resulting prejudice. The Court found that, not only were relevance and prejudice established, but were even admitted by Defendants—”[W]e’ve given up on prejudice . . . which I think was the appropriate thing to do. We gave up on the issue of relevance.” Id. at . *128.

Accordingly, it was incumbent upon the Court to determine the severity of the sanctions. Along with the extent of the prejudice and the degree of culpability, the Court also discussed the following factors to consider in making such a determination:

Thus, the range of available sanctions serve both normative – designed to punish culpable conduct and deter it in others – and compensatory – designed to put the party adversely affected by the spoliation in a position that is as close to what it would have been in
had the spoliation not occurred—functions. Because, as noted above, the duty to preserve relevant evidence is owed to the court, it is also appropriate for a court to consider whether the sanctions it imposes will "prevent abuses of the judicial system" and "promote the efficient administration of justice." The court must "impose the least harsh sanction that can provide an adequate remedy."

Id. at *131-32 (internal citations omitted).

Plaintiff was granted most, but not all, of its request for sanctions. First, Plaintiffs received an entry of default judgment as to liability on one count of their claim. See id. at *148. Most notably, however, the Court awarded Plaintiffs attorney fees and costs and found Pappas to be in civil contempt of court for violating various court orders. The Court explained:

For such clearly contemptuous behavior, a very serious sanction is required. Accordingly, I order that Pappas's acts of spoliation be treated a contempt of this court, and that as a sanction, he be imprisoned for a period not to exceed two years, unless and until he pays to Plaintiff the attorney's fees and costs that will be awarded after Plaintiff has submitted an itemized accounting of the attorney's fees and costs associated not only with filing this motion, but also with respect to all efforts expended throughout this case to demonstrate the nature and effect of Pappas's spoliation. These costs and fees likely will amount to a significant figure, and that will properly vindicate this Court's ability to enforce its discovery orders. The commencement of Pappas's confinement will be determined at the conclusion of the proceedings to quantify the amount of attorney's fees and costs.

Id. at *158. (emphasis added).

The Court further emphasized that jail time was critical in order to properly punish Defendant Pappas and provided something more than an empty paper judgment to Plaintiffs.

In sum, Victor Stanley II is a must read for every attorney facing e-discovery challenges. The opinion provides a well-reasoned argument for proportionality and reasonableness where parties must preserve and collection efforts. Parties should be careful not to misuse e-discovery, however, as a sword instead of the shield it is intended to be to preserve critical ESI in warranted cases. All aspects of e-discovery should be analyzed and understood in the context of proportionality. Further, reasonableness must be judged on a case by case basis, taking into consideration the risks, benefits and value of the case. But make no mistake: engaging in this balancing act does not give corporate litigants a free pass to engage in e-discovery abuses. No party burdened with a preservation order or a litigation hold letter should simply engage in a half hearted effort or otherwise ignore its obligations and claim they believe thought they did the requisite amount of preservation and/or collection necessary in proportion to the amount at issue. Indeed, the Victor Stanley II Court demonstrates the court's power to punish those that believe e-discovery is a nuisance or a joke.

Ultimately, the Victor Stanley II opinion provides a cohesive roadmap for all attorneys and corporate litigants to follow in their quests for compliance with e-discovery obligations. While not meant to be the "be all and end all" of e-discovery guidance, this detailed and insightful opinion regarding the resolution of preservation and spoliation issues will likely provide a great deal of comfort to future litigants in their efforts to avoid disproportionate e-discovery costs or not unpredictable outcomes of spoliation motions.

Angela Scafuri is a member of Bressler, Amery & Ross, PC's Commercial Litigation Department where she focuses her practice on the defense of insurance companies in complex premium, coverage and insurance bad faith actions. Ms. Scafuri also represents policyholders with respect to coverage, claims handling and bad faith issues. She has appeared in and argued cases at both the trial and appellate levels, and has successfully defended clients in federal courts throughout the country.

Production of ESI in "Reasonably Usable Form" Under Rule 34(b)(2)(E)(ii) Means that ESI Does Not Have to Be Labeled to Correspond to Individual Requests

by Joseph Valentine

A party producing electronically stored information ("ESI") in a reasonably usable form or forms is not bound by the requirement that the party either "produce documents as they are kept in the usual course of business or . . . organize and label them to correspond to the categories in the request. Fed. R. Civ. P. 34(b)(2)(E)(i). Instead, a production of ESI in "a reasonably usable form or forms" satisfies the alternative and independent requirements of Fed. R. Civ. P. 34(b)(2)(E)(ii).

The following hypothetical will assist in assessing the validity of this conclusion.

THE HYPOTHETICAL

(1) A requesting party served a 50-item document demand, asking for all documents in
multiple broad categories.

(2) The responding party produced 40,401 electronic files, with TIFF images, full searchable text, and a "load file" for use in readily available litigation-support applications.

(3) The "load file" contained data columns identifying

(a) for all files, the file source (i.e., the "custodian" or employee in whose files the document was located), file name, Bates range, attachment Bates range (if applicable), and document type;

(b) for e-mail files, date sent, author, addressee, persons copied and blind-copied, and subject; and

(c) for non-e-mail files, author and date created.

THE CONFLICT

The document request demanded ESI in its "native file format" and also included a requirement that the responding party "produce documents as they are kept in the usual course of business or . . . organize and label them to correspond to the categories in the request," Fed. R. Civ. P. 34(b)(2)(E)(i). In a written response, the responding party objected to those requirements and stated that it would proceed with the method of production described above, i.e., production in a "reasonably usable form." After the production, the requesting party did not complain about the lack of a native-file-format production but claimed that the method of production did not satisfy the "usual course of business" requirement under subsection (E)(i) and that, therefore, the 40,401 documents must be labeled to correspond to each of the 50 requests to which the documents were responsive.

DISCUSSION

As a preface, it is vital to recognize that the method of organizing the hypothetical electronic production described above currently represents a type of "gold standard" in producing ESI. There is no space available here to discuss either the evolving standards for an ESI production in "reasonably usable form" or the negative consequences of cutting corners in the production of electronic data—for example, by failing to produce fully searchable text or by omitting production of "load files" containing data like those described in the hypothetical. The few cases found that even touch on the issue of the interpretation of subsections (E)(i) and (E)(ii) of Rule 34(b)(2) dealt with demonstrable or apparent substandard electronic productions. As a result, these cases (some of which appear to accept without analysis that subsection (E)(i) applies to electronic productions) do not provide guidance or reasonable precedent in resolving the issues discussed here. E.g., Estate of Eva Boles v. Nat’l Heritage Realty, Inc., 2010 U.S. Dist. LEXIS 79770 (N.D. Miss. Aug. 6, 2010); In re Bisphenol a Polycarbonate Plastic Prods. Liab. Litig., 2010 U.S. Dist. LEXIS 52444 (W.D. Mo. May 26, 2010); Valeo Elec. Sys. v. Cleveland Die, 2009 US Dist. Lexis 51421 (June 17, 2009); Suarez Corp. Indus. v. Earthwise Technologies, 2008 WL 2811162 (W.D.Wash.).

Amended Rule 34(b)(2) distinguishes the method of production for documents, on the one hand, and for ESI, on the other hand:

(E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

(i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;

(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

Subsection (b)(2)(E) thus identifies separate procedures for "producing documents or electronically stored information." The procedure for documents is set out in subsection (E)(i), and the procedure for electronically stored information is set out in subsection (E)(ii). The requirement to label documents to correspond to the categories in the request therefore applies only to documents, as distinct from electronically stored information.

The amended rules incorporate the recognition that "it has become increasingly difficult to say that all forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a 'document' . . . . Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents." Fed. R. Civ. P. 34(a), advisory committee’s note. This distinction pervades all of the amended discovery rules. For example, Rule 26(a)(1) requires initial disclosure of three categories of materials, namely, "documents, electronically stored information, and tangible things." As another example, Rule 26(b)(2)(B) explicitly identifies limits on discovery of electronically stored information, as distinguished from documents. Likewise, Rule 26(f)(3)(C) requires discussion of issues unique to electronically stored information. The judicial recommendations leading up to adoption of the amendments repeatedly highlighted the distinction between traditional documents and electronically stored information. E.g., Report of the Judicial Conference, Committee on Rules of Practice and Procedure (Sept. 2005) at 4 (Jud. Conf. Rep.), available at http://www.uscourts.gov/
Specifically with respect to Rule 34, the ESI “alternatives” (in (E)(ii)) were intended to provide functional analogues to the existing rule language that provides choices for producing hard-copy documents: the form in which they are kept in the usual course of business or organized and labeled to correspond to the categories in the request. Advisory Comm. Rep. at 56. This recommendation was confirmed by the Judicial Conference:

The [amended] rule provides an electronic discovery analogue to the existing language that prevents massive “dumps” of disorganized documents by requiring production of documents as they are ordinarily maintained or labeled to correspond with the categories in the request. Under the proposed amended rule, absent a court order, party agreement, or a request for a specific form for production, a party may produce responsive electronically stored information in the form in which the party ordinarily maintains it or in a reasonably usable form.

Judicial Conf. Rep., supra, at 9. Finally, the official Committee Note to Rule 34(b) states that the separate forms of production specified for ESI (“as ordinarily maintained” or “in a reasonably usable form”) represent “comparable requirements” to the forms traditionally specified for documents, so as to “protect against deliberate or inadvertent production in ways that raise unnecessary obstacles for the requesting party. Rule 34(b) is amended to ensure similar protection for electronically stored information.” Accord, Advisory Comm. Rep., supra, at 57 (just as the traditional requirements for production of paper documents had the purpose of preventing abusive “document dumps,” so too the ESI requirements in (E)(ii) have the objective “to provide the same kind of protection against discovery abuse that is provided for paper discovery”).

In addition to the literal language of the amended rules and the associated commentary, there are fundamental policy reasons for the conclusion discussed here. Because of space limitations, it is possible now only to give the barest outline of such policy reasons. The Advisory Committee Report makes clear that production of ESI in a reasonably usable form protects against discovery abuse precisely when the method of ESI production is by essentially the same technological capabilities available to the producing party. Advisory Comm. Rep., supra, at 67. Key among those capabilities is the ability to search the text of the produced ESI. Id. Among other things, this means that both the producing and receiving parties have essentially the same ability to examine and categorize the produced ESI. Furthermore, commentators and courts increasingly are recognizing the importance of applying principles of proportionality to the discovery process. E.g., Sedona Conference Commentary on Proportionality in Electronic Discovery (2010) (Principle 6: Technologies to reduce cost and burden should be considered in the proportionality analysis). Specifically in the context of the amended rules on ESI discovery, those rules represent more than a half decade of detailed analysis and discussion, and—equally importantly—a more than three-decade trend, to adopt rules that “provide more effective means for controlling overuse and occasional misuse of the discovery devices.” Judicial Conf. Rep., supra, at 5. Applying subsection (E)(ii) to all ESI productions both obliges a producing party to provide discoverable materials that the receiving party can use in a reasonably efficient and cost-effective manner and minimizes in reasonable ways the burden and expense on the producing party of organizing and categorizing the produced electronic files.

The hypothetical facts outlined above were selected purposely to highlight a potential ambiguity or lacuna in subsection (E)(ii) caused by the conditional phrase, “If a request does not specify a form for producing electronically stored information.” Under the facts hypothesized here, the requesting party demanded a native format production. The question thus arises, is subsection (E)(ii) inapplicable here? Stated in another way, can a requesting party cancel the applicability of subsection (E)(ii) by the apparently simple expedient of specifying an electronic format in which ESI must be produced?

A reasonable answer to these questions is, no. The conditional phrase, “specifying a form for producing” ESI, actually refers only to alternative forms of production of ESI in either hardcopy or electronic form: “Rule 34 is also amended to provide a third way to specify the form of production, such as in paper or electronic form.” Judicial Conf. Rep., supra, at 8-9 (emphasis added). Cf. Suarez Corp., 2008 WL 2811162, at 3 (“‘The comments do not refer to the term ‘form’ as encompassing the organization of all of a party’s production. Therefore, ‘form’ does not refer to the organizational mandates of Rule 34(b)(2)(E)(i) and Suarez is without authority to mandate how Earthwise produces material under that provision’). The conditional phrase in subsection (E)(ii) thus does not apply to, and properly should not affect applicability of, the distinct methods of organizing paper documents, on the one hand, and ESI, on the other hand. Furthermore, the policy considerations identified above, both those leading to adoption of the amended rules regarding ESI and those dealing with proportionality in discovery generally, require an interpretation of this conditional phrase that would not unfairly increase the burdens and expense on the producing party when that party produces ESI in a “reasonably usable form.”

Joseph Valentine is Of Counsel with the Denver-based trial law firm of Wheeler Trigg O’Donnell LLP. In over 30 years of practice, Joe has litigated hundreds of cases involving product-liability and commercial matters in the automotive, consumer, pharmaceutical, and medical-device industries. He now concentrates his law practice on electronic discovery issues. Joe combines his experience in complex litigation document collection and organization.
and the issues pertaining to attorney-client privilege and work product immunity with in-depth working knowledge of information systems within corporations to provide concrete advice to the firm's clients regarding the discovery and protection of electronic data. Joe formerly practiced in the New York offices of Hughes Hubbard & Reed and Skadden Arps and is a graduate of Fordham University School of Law.

Preserving Long Life Electronic Information-Special Concerns for Governmental Entities and Health Care Providers

by Thomas D. Eosodi

In today's corporate world, businesses are generating enormous amounts of electronic information. Most of this information becomes obsolete before hardware and software configurations can no longer handle it. At a minimum, it becomes legacy data and remains out the litigation process. Governmental entities and health care providers face different challenges. The Health Information Technology for Economic and Clinical Health ("HITECH") Act as part of the American Recovery and Reinvestment Act of 2009 and other developing legislation is creating this new atmosphere. Governmental entities and health care providers may be required to maintain electronic information for long periods of time if not forever. For those records, a preservation plan must take into account not only hardware and software advancements, but limitations of storage media, and the information use reliability. This article will address handling those obstacles.

Developing Requirements for Health Care Providers and Governmental Entities

E-mail, as the new primary means of business communication, became the focus of decision after decision in the ever entertaining discovery dispute arena. The mere size and amount of e-mail generated coupled with its inherent preservation and production problems contributed to this attention. When Congress passed HITECH as part of the American Recovery and Reinvestment Act of 2009, health care providers were guaranteed similar retention and production issues. Earlier this year, the Centers for Medicare and Medicaid Services ("CMS") clarified qualifications for health care facilities wanting large payments in 2011 and 2012. These qualifying health care facilities are required to maintain 80% of patient records and 40% of prescription records in digital form. The very nature of this information mandates an extended life span with corresponding preservation concerns.

Government records face the same exponential growth likelihood. The Federal Records Act of 1950 (44 U.S.C. § 3101) requires agency heads to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and is designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities." As electronic information became more prevalent further legislation developed. The Paperwork Reduction Act of 1980 (44 U.S.C. § 3501) calls for the coordination of three electronic record keeping elements: the integration of automatic data processing; telecommunications; and records management policies and procedures. Further, the Office of Management and the Budget ("OMB") Circular No. A-130 specifically includes information in any form in meeting the creation, maintenance, and disposal requirements of the Federal Records Act of 1950.

Supplementary nourishment of this growth is the plethora of state laws implementing similar necessities. As an example, for purposes of effectively reducing the significant paperwork and associated costs in the daily operations of state government, Hawaii enacted Act 177, Session Laws of Hawaii, Regular Session of 2005 (HB 515), allowing state and county agencies to create and maintain their records in electronic format. This act calls for storage of government records in electronic format, as well as the conversion of existing paper and microfilm documents to electronic documents. The Illinois Local Records Act (50 ILCS 205) also allows local government agencies to reproduce existing public records in digitized electronic format. However, the Act only allows this process if electronic records are reproduced on a "durable medium that accurately and legibly reproduces the original record in all details," and "that does not permit additions, deletions, or changes to the original document images."

While business entities rapidly continue to produce records in electronic form, most if not all of this information will be subject to destruction within industry standard timelines that accommodate current technological limitations. However, as governmental entities and health care providers generate electronic information, which, by its nature is designed to have a lengthy if not infinite life span, two issues will develop: (1) Can electronic information be retained for long periods in compliance with applicable law and, (2) since this information remains available, can it be maintained in a form suitable for use in the defense of a governmental or health care client?

Software and Hardware Restraints

A fundamental issue involving preservation of electronic information with a long life span develops from the nature of the information itself. Anyone that has dealt with the most basic e-discovery issue will attest that it is inherently more fragile than traditional technologies as it is more easily subject to corruption and alteration. As time progresses, the briskly increasing number of formats and the increasing complexity of each unit of information (many times combining these various formats) exacerbates this issue and increases software dependency.
Copyright/intellectual property rights associated with much of the software in use and the absence accepted industry standards for long term access makes software dependency a negative factor.

Each type of storage media available for storage of electronic information with a long life span has its own shortcomings. The media's negative attributes are typically emphasized when considered for long term storage. Hard disk drives are routinely used in forms ranging from corporate servers to hand held devices. Information is accessed quickly, efficiently, and in its intended format. However, 10 years would be an extreme life expectancy of a hard drive. Close spacing between the heads and the disk surface make hard disk drives vulnerable to head crash damage. Physical shock, contamination, and corrosion are the typical culprits. Tape drives are the preferred archiving technology despite significantly slow accessibility rates. The two key components that make tape drives favorable for back up purposes make it the less than perfect media for long life span information. Tape is rewritable and not designed to read or write individual files. Moreover, software for tape drive use tends to be highly proprietary. Optical discs offer 100% WORM media. Unfortunately, limited rpm rates from a non-fixed drive and optical head weight produce slow data access rates.

Preservation Techniques Including Metadata Maintenance

Long life span electronic information retention plans must include an assumption that the periodic transfer of electronic information from one configuration to another, or from one technology to another is inevitable. Those of us that have read case after case where discovery sanctions are imposed based on the destruction or alteration of metadata from this type of activity cringe at the thought. Given this inevitable migration of information, a method must be selected to ensure such information is appropriately maintained to conform to applicable standards. Additionally, certain levels of metadata must be maintained to elicit any hope of using such information in support of a defense.

The "computer museum" is always presented as an alternative. Saving all hardware, software, and documentation needed to support stored electronic information however, is unrealistic. Costs associated with equipment storage will be overwhelming. Furthermore, the likelihood of hardware failure without available replacement materials is enormous. Just envision the scenario with a separate system for every 5 years of information. The next alternative is usually emulation. By creating programs and/or hardware to simulate previous versions while preserving the functionality of the information, this approach removes the need to maintain the original hardware and software. However, creation can be time-consuming and difficult to achieve. Despite the original cost of developing an emulator, arguments remain that creating an emulator may prove to be the more cost efficient solution. An additional approach of packaging the electronic information with all information on how to interpret it may also be used. This is typically referred to as Encapsulation. These packages are usually very large in size. Migration of the encapsulation packages and creation of encapsulated packages is the largest drawback. Probably the most common approach of preserving long life electronic information includes a combination of refreshing and conversion. Refreshing involves the transfer of information to a new media. The conversion process then changes the information from one format to another. Many times information can be moved out of a proprietary format. Tests to determine what information, including metadata, will be lost are an absolute necessity, sometimes proving the process to be less attractive.

Whether the intent is to present electronic information as evidence or simply have it available for public access, information, in any form, is only valuable if it can be easily used. Metadata is essential to this purpose. Metadata must contain standardized elements and fields ("structured format") as well and consistent recognizable content (e.g., "03/17/11" as the standard expression of a date) commonly referred to as controlled vocabularies. Metadata standards are typically based on The Dublin Core elements. These elements, intended for cross-domain information, provide fundamental components to describe and catalogue most information. The Dublin Core Metadata Initiative http://dublincore.org/ provides an open forum for the development of interoperable online metadata standards. Regardless of the migration process, adoption of appropriate metadata elements will increase the successful use of such information.

Addressing the Two Developing Issues

Preservation of long life span electronic information will place an ever increasing burden on multiple levels of health care providers and governmental entities. Both will need to address the assessment demand of time and money, whether it includes hired expertise, increased staffing or system hard costs. Many decisions will be made with anticipated miscalculations. The ongoing process of analyzing and implementation should be well documented.

In development of the plan to preserve electronic information with a long life span, the following topics should be considered.

- The frequency at which the information will be accessed,
- The amount of time required to maintain the information (its lifespan), and
- Potential cost savings by mass storage with anticipation of sharing within the organization.

Once these issues are addressed the plan with the following considerations can be put into place:
What media source will be selected?
What software is efficient and appropriate and will the proprietary nature impact other decisions?
What hardware is necessary to process and store the information?
What process will be used to assure that the information remains accessible and reliable, while addressing applicable security requirements?
What level of metadata will remain intact during anticipated migrations?

Consideration of these factors will help ensure that electronic information is retained for long periods in compliance with applicable law and can be maintained in a form suitable for use in the defense of a governmental or health care client.

**Thomas D. Esordi** is a Principal with Kitch Drutchas Wagner Valitutti & Sherbrook, representing businesses and governmental entities in complex and high profile litigation. Mr. Esordi regularly advises his clients on electronic information preservation and production issues.

---

**News & Announcements**

**Get Involved!**

DRI membership is the key to growing your practice. Please share the [Young Lawyer Membership Flyer](#) with your colleagues interested in getting more involved in DRI.

---

**Special Offer**

Have you visited DRI's new online portal, [DRI Today](#) yet? DRI Today is your one-stop resource to news, market updates, legal commentary and more all designed specifically with the defense attorney in mind. Browse the [DRI Blog](#) for interesting discussions or catch up on past articles from *For The Defense*. [DRI Today](#) provides a convenient resource to find information on any practice area topics with just the click of your mouse. Be sure to make [DRI Today](#) your homepage to keep up with the fast changing world of legal news. Don't forget to like [DRI on Facebook](#) and follow [DRI on Twitter](#)!