E-Discovery

The Latest Litigation Tips

LawyersUSA

Susan A. Bocamazo, Esq. – Publisher & Editor
susan.bocamazo@lawyersusaonline.com

Henriette Campagne – Vice President of Editorial
henriette.campagne@lawyersweekly.com

Reni Gertner – Managing Editor
reni.gertner@lawyersusaonline.com

Correy E. Stephenson, Esq. – Associate Editor, New York Office
correy.stephenson@lawyersusaonline.com

Kimberly Atkins, Esq. – Staff Writer, D.C. Office
kimberly.atkins@lawyersusaonline.com

Sylvia Hsieh, Esq. – Staff Writer, California Office
sylvia.hsieh@lawyersusaonline.com

Tony Ogden – Website/Editorial Assistant
anthony.ogden@lawyersusaonline.com

Patrick M. Murphy, Esq. – Legal Editor
patrick.murphy@lawyersusaonline.com

John L. Mecklenburg – Art Director
john.mecklenburg@lawyersweekly.com

JoAnn Griffin – Audience Development Manager
joann.griffin@thedolancompany.com

Charlene J. Smith – Vice President of Sales
charlene.smith@lawyerweekly.com

Thomas F. Harrison
– Vice President, New Business Development

Malee S. Nuesse
– Vice President, Circulation –

Scott Murdoch
– Circulation Manager –

You can contact **Lawyers USA** via the
Internet at: comments@lawyersusaonline.com
Or call **Lawyers USA** at 800-444-5297

The Dolan Company

James P. Dolan
– Chairman, President/CEO –

Scott J. Pollei
– Executive Vice President/CFO –

Mark W.C. Stodder
– Executive Vice President/Newspapers –

Christopher A. Eddings
– Director of Publishing Operations –

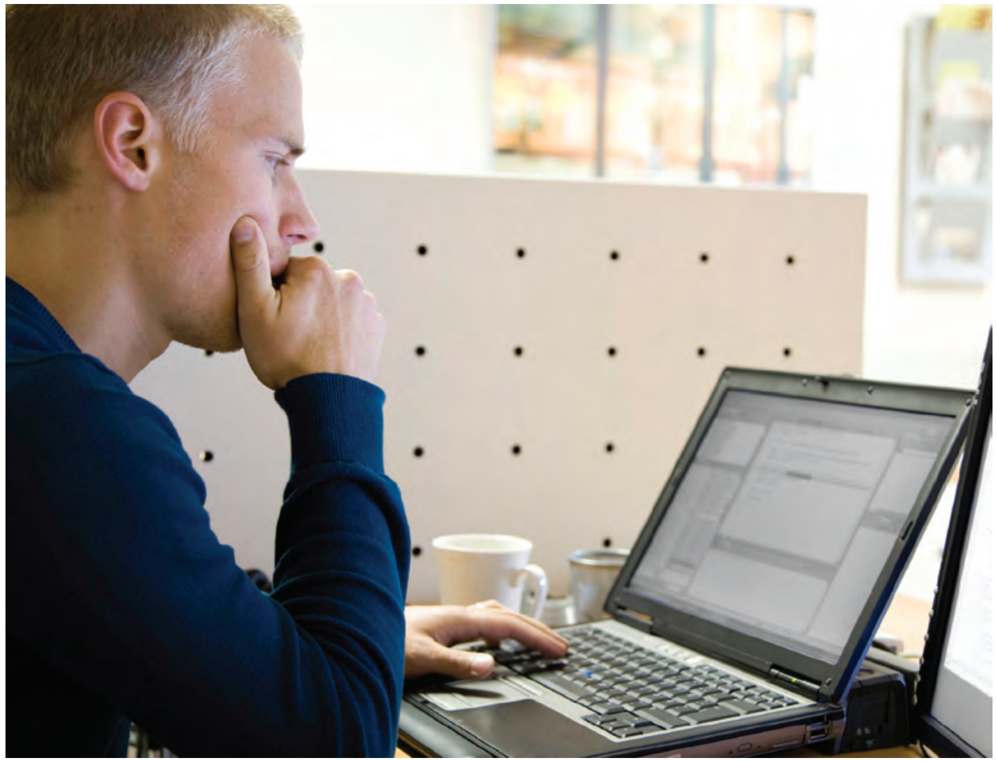
Glenda Russell
– Group Publisher –
glenda.russell@thedolancompany.com

LAWYERS USA (ISSN-1931-9584.) is published monthly by Lawyers Weekly Inc., 10 Milk St., 10th Floor, Boston, MA 02108. Price is $26 per copy plus shipping and handling, $249 per year, $144 for 6 months. POSTMASTER: Send address changes to LAWYERS USA, 10 Milk St., 10th Floor, BOSTON, MA 02108. Periodicals postage paid at Boston, MA and additional mailing offices.

tableofcontents

LawyersUSA

Sanctions for e-discovery violations at 'historic' high



©iStockphoto.com

By Christina Pazzanese
Contributing writer

Sanction motions and awards for e-discovery violations across the country have climbed dramatically in recent years and have now hit "historic highs," according to a study published in the Duke Law Journal.

The study identified 401 cases filed in federal court before Jan. 1, 2010, with written opinions involving sanction motions or sanction awards. It found that not only have e-discovery sanction cases climbed annually since 1981, the increase in both sanction motions and awards since 2004 has been "significant."

In 2009, there were more sanction cases (97) and more sanction awards (46) than in any previous year.

Lawyers say the study, the most comprehensive effort they have seen attempt to quantify trends in what is a rapidly expanding and increasingly complicated area of litigation, confirms much of what they have witnessed in their own practices.

"E-discovery is a big issue, it's an enormous undertaking and it's incredibly expensive," said John A. Tarantino of Adler, Pollock & Sheehan in Providence, R.I. "Even if you proceed in good faith, you still can have problems."

Violations prompting the most sanctions were a failure to preserve evidence, which was cited in 131 of the 230 cases in which sanctions were handed out, followed by a failure to produce evidence, cited in 73 cases

Sanctions included dismissal and default, as well as adverse jury instructions and monetary awards that ranged from $250 to $8.8 million.

Sanctions against counsel, however, remain rare, the study found.

Timothy J. Dacey III, a veteran business litigator at Goulston & Storrs in Boston, said e-discovery violations and sanctions have become an especially hot topic in the federal courts, where high-stakes disputes involving parties that generate and retain more discoverable information – who also have the resources to pursue them from others – tend to play out.

The federal courts have also generated more "trailblazing" cases, such as 2003's *Zubulake v. UBS Warburg*, that have raised awareness among lawyers of the scope of their e-discovery obligations, as well as the pitfalls and potential for abuse, Dacey said.

Judgment calls

Lawyers say a critical factor driving e-discovery disputes is the difficulty practitioners face with issuing appropriate litigation holds to clients because there is little guidance and essentially no appellate caselaw to follow.

Clients often balk at the high cost of an overly broad hold since it may encompass a vast amount of digital evidence stored in far-flung locations, while lawyers try not to exclude something in an overly narrow hold for fear of triggering a potential violation down the road.

Striking the appropriate balance of what should be retained and for how long is easier said than done, attorneys say.

"It's one of the harder judgment calls that lawyers and clients need to make early on," said Boston Jonathan Sablone, who practices at Nixon Peabody.

"The problem is it's an unsupervised process," he said. "There's no judge telling you what you should be doing. Instead, you're trying to make a good-faith judgment at the time of what you need, and if you're wrong, you could be sanctioned."

Lawyers agree one key challenge is that the various federal and local rules governing such violations use a reasonableness standard rather than a bright line.

Rule 37(e) of the Federal Rules of Civil Procedure – which provides "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system" – was the most commonly cited rule in the cases studied.

Counsel sanctions rare

Despite the overall uptick in sanctions, those specifically against counsel are still rare and prompted by repeated misconduct, according to the study.

Of the 401 cases studied, only 30 counsel sanctions were handed out and only 25 of those were issued specific awards; the other five were deferred. Sanctions against counsel were considered in seven additional cases, but were ultimately not handed out.

"I think sanctioning lawyers is often only the last resort of a court," said Stephen D. Riden of Beck, Reed, Riden in Boston. "Courts will typically give lawyers the benefit of the doubt, especially with a large volume of data that's hard to wrap your arms around."

Unless the conduct is egregious and opposing counsel offers a "slam-dunk argument," judges will look for other ways to punish violations, he said.

Questions or comments can be directed to the managing editor at: reni.gertner@lawyersusaonline.com

E-discovery meets Facebook: Social networking sites complicate litigation

By Correy E. Stephenson
Staff writer

As more and more individuals and businesses take part in social media like Facebook, MySpace and Twitter, these social networking sites are inevitably becoming a factor in e-discovery.

In a recent U.S. District Court decision from California, *Crispin v. Audigier*, Judge Margaret M. Morrow concluded that private messages sent on Facebook and MySpace were analogous to e-mail under the Stored Communications Act, and quashed a subpoena seeking to have the messages produced.

However, the judge remanded the case to further develop the evidentiary record on whether Facebook wall posts and MySpace comments should also be protected from disclosure.

Practitioners expect more decisions to follow.

"This is just the first step," said Regina Jytyla, managing staff attorney at Kroll OnTrack, an Eden Prairie, Minn. computer forensics company that specializes in electronic evidence.

The decision "will help practitioners get a sense of the real complexity of e-discovery in the context of social media, like the accessibility of content contained on a social media site as well as the technical side: best practices for identifying, preserving, and collecting data, an area that is still developing," she added. "This decision is the tip of the iceberg."

Breach of contract

In *Crispin*, an artist filed a breach of contract suit against a clothing manufacturer and retailer, claiming that he had granted the defendant a limited oral license to use his works in connection with certain garments, but the defendant had failed to include his logo and violated his rights by sublicensing his artwork without consent.

The defendant then served subpoenas on Facebook, MySpace and an ISP, seeking communications between the plaintiff and others relevant to the contract dispute.

The court first decided that the plaintiff had third-party standing under the 1986 Stored Communications Act to contest the subpoenas.

It further decided that that the messaging and e-mail services provided by the social networking sites constituted "electronic communication services" under the Act.

Accordingly, the court concluded that the Act required that the subpoenas be quashed with respect to the webmail and private messaging sought by the defendants.

"[T]he court is satisfied that those forms of communications media are inherently private such that stored messages are not readily accessible to the general public," the court said.

According to Kenneth J. Withers, the lesson practitioners should take away from the case is that "social media like Facebook and MySpace are within the scope of discovery, but the use of a third-party civil subpoena under [FRCP] 45 is not the way to obtain it."

Instead, said Withers, director of Judicial Education and Content at The Sedona Conference, a non-profit organization in Phoenix that works to advance law and policy in areas like electronic discovery, such information is properly requested as part of a routine discovery request under FRCP 34.

However, he noted that there may be difficulties associated with including information from sites like Facebook in a discovery request, such as issues of format and accessibility. For example, even though the producing party is a subscriber to the services of the social networking site, it might be necessary to request electronically stored information from the site in order to access messages and wall posts, giving parties an argument that the ESI isn't readily accessible, Withers said.

And production in native format might also be difficult.

"I doubt if many individuals have the technological capacity to do more than provide a paper printout from the site," he said.

Wall posts and other issues

The decision leaves unanswered questions about the discoverability of wall posts – comments made on a user's page that are visible to all friends on the site.

Judge Morrow remanded the case to develop the factual record and instructed the magistrate to analyze Crispin's privacy settings on the site.

Specifically, the court will analyze the user's settings to see what he allowed others access to, explained Michael Hindelang, a partner at Honigman Miller in Detroit, Mich. and chair of firm's e-discovery practice group.

"Did the user make everything available to the general public, or were things limited to a small group of people, or somewhere in between?"

A user's expectation of privacy for wall posts or MySpace comments will vary depending on the amount of access he or she allows to other users, Jytyla said. And while Judge Morrow said the specific number of Facebook friends isn't determinative of privacy intentions, it might be hard to argue that comments 900 people could see are something a user considered private.

Because there are so many different variations on privacy settings – which are also subject to change – this issue will continue to come up in cases, Hindelang said.

"As more and more users get involved in these social networking sites, more and more people are trying to figure out how they can use it in litigation," he noted.

There are also other e-discovery issues associated with social media.

For example, said Hindelang, companies that have a social networking presence may need to consider preservation issues when a lawsuit arises.

"Every case needs to be evaluated for social media issues," he said.

Jytyla agreed.

"This case illustrates the fact that there is no one-size-fits-all solution to the preservation, collection and review of social media content," she said.

While practitioners should expect many more opinions on the topic, Hindelang noted that the technology will continue to change.

"Who knows what things are going to look like five years from now?" he said, noting that five years ago social networking sites weren't nearly as common as they are today.

Withers sees this court's discussion of privacy issues as a preview of a broader discussion of the application of the Fourth Amendment in the electronic age.

"More and more of our communications are computer-based and computer-mediated, but does that mean we have voluntarily waived our Fourth Amendment privacy expectations?" he asked.

Questions or comments can be directed to the writer at:
correy.stephenson@lawyersusaonline.com

Preserving social media for electronic discovery

By Correy E. Stephenson
Staff writer

The amount of litigation-related information on sites like Facebook and Twitter is rising.

For lawyers, these sites can be an electronic discovery gold mine – or they can be the downfall of a case.

How can lawyers ensure that social media communications are preserved for trial? Conversely, how can they stop their clients from putting themselves at risk of sanctions for deleting information?

Social media is implicated "in every kind of case, from corporate espionage all the way down to a fender-bender," said Stephen D. Riden, a commercial litigator and partner at Beck Reed Riden in Boston.

Josh Gilliland, an e-discovery practitioner in San Jose, Calif. and author of the Bow Tie Law blog on e-discovery, noted a recent trademark infringement case between two restaurants where the plaintiff sought sanctions against the defendant after the latter changed an allegedly infringing Facebook profile photo. (*Katiroll Co. v. Kati Roll & Platters, Inc.*, No. 85212 (D.N.J. 2011).)

The court concluded that changing a Facebook profile picture could result in the loss of discoverable evidence, but declined to impose sanctions on the defendant, recognizing that changing such a photo is a "common occurrence" and that it was not surprising the defendant didn't realize its actions would impact evidence in the litigation.

Because the court found that the spoliation was unintentional, it ordered the defendant to change its profile picture back to the allegedly infringing photo so that the plaintiff could print the information it believed supported its case.

"This … opinion … recognized how fast [social media] can change," Gilliland said.

Preserving client information

Because sites like Twitter and Facebook change every minute, parties involved in litigation must be prepared to deal with the preservation of such mediums, Gilliland said. Education may be the first step, Riden said.

"Parties are typically unwilling to cough up [social media] communications," he said. "When I inform clients of their obligation to preserve information or explain that it is discoverable, they are surprised – and resistant."

While clients may understand that things like work e-mails are discoverable, they feel that Facebook "is a personal mode of communication," Riden said.

Businesses aren't well-prepared either, noted Karen Hourigan, a partner at Redgrave LLP in San Francisco who focuses her practice on records litigation preparedness and electronic discovery. "Companies feel obligated to have a social media presence but they don't realize what they are putting out there."

To get the importance of preservation across, "I read my clients a variation of the riot act," Riden said. "I let them know the penalty for deleting things like a Tweet or an IM over Facebook is high and could affect the outcome of the case."

Riden instructs clients not to delete or change anything on their social media platforms. In one case, he even had a client share his Dropbox password so he could ensure that all the information was being properly preserved.

"I tell my clients that to the extent any communication over any websites pertains to this action, don't delete anything and keep it as is," Riden said. "Further, don't have any future communications about this case, including on these websites."

Riden suggested that lawyers conduct such a discussion face-to-face and even in front the client's computer, to walk through all the different ways they interact with others online.

"I try to do that in every case, and I've found that it is really the only way to be comprehensive in gathering information," he said.

For businesses, Hourigan advises her clients with a presence on social media to draft a policy that describes their online purpose as well as guidance about preservation, so that such procedures are already in place if and when litigation occurs.

Preservation by the other side

In requesting social media communications from the other side, Riden said he is careful to be very specific.

"I ask for all communications in electronic form and I specify that I mean e-mail and social media sites, naming specific sites," he said, including Facebook, Twitter, MySpace and even certain mobile apps like salesforce.com.

In some cases – such as suits for defamation or libel – attorneys may want to make attempts to preserve an opponent's communications prior to sending a cease and desist letter or complaint, Hourigan said.

"In some instances, it makes sense to take our own steps to preserve what is already out there," using screen shots, for example, she said.

However, it's important to resist the temptation to friend an opposing party or witness. Ethics boards in California, New York and Pennsylvania have found that such requests are deceptive and improper ex parte communications.

Riden suggested that attorneys can contact social media companies directly to preserve an opposing party's information.

Facebook will allow litigants to request preservation of an account through its security department, Riden said, although to have the company actually produce the content lawyers will need to provide a subpoena or court order as well as pay a fee.

"Different sites have different requirements about downloading and copying," Hourigan noted, so a case that involves multiple social media sites could get complicated. For example, Twitter considers itself the owner of all Tweets, but Facebook has an option that allows a user to download his or her own profile and information, she said.

Another cheap method of preservation: hit "print."

In smaller suits involving individual plaintiffs or small companies, courts may be forgiving and recognize that the parties are less tech-saavy, Gilliland said. That means a screen shot or a printed screen, as long as it is authenticated, could possibly be introduced as evidence.

In those cases, "the screen shot should include the full URL and a header at the top or bottom giving the date," and metadata that shows when the screen shot was taken to meet authentication standards, he said.

In bigger cases, or where concerns about authentication exist, Gilliland suggested hiring a private investigator to take screen shots or using software to capture website architecture.

"That way, you have an outside, third party who can do the authentication, as opposed to your own client taking the screen shot," he said.

For cases involving big companies, there is software that lets you follow the company's activity on social media and take screen captures of those actions, Gilliland said.

Questions or comments can be directed to the writer at:
correy.stephenson@lawyersusaonline.com

Misspellings can create issues for the e-discovery process

By Correy E. Stephenson
Staff writer

You might have thought that electronic discovery always requires accuracy. But the latest advice from e-discovery experts is that misspelled words and names are just as essential to the process as accurate ones.

That's because misspellings and abbreviations are common in both texts and e-mails, where people tend to be more casual with their language and keep their messages short.

"This is a huge issue," said Michael R. Arkfeld, an attorney at Arkfeld & Associates in Phoenix and the author of the treatise, "Electronic Discovery and Evidence." "E-mail accounts for almost 60 percent of all [electronically stored information], with text messaging as another huge source."

In a recent order, U.S. District Court Judge Blanche M. Manning of the Northern District of Illinois ordered the defendant in *Northington v. H&M International, Inc.* to "include misspellings of [the] plaintiff's first name as well as other key search terms reasonably related to each of the topics set forth" in the production request.

Josh Gilliland, an e-discovery practitioner in San Jose, Calif. and author of the Bow Tie Law blog on e-discovery, said it was the first time he had seen a court order parties to include misspellings.

"The order reminds us that there is no easy way to go through the thousands or sometimes millions of documents to cull through and find what is truly responsive to a search in a particular case," said Andrew Cosgrove, a partner at Redgrave LLP in Minneapolis.

Cosgrove, whose information law practice focuses on e-discovery, information management, privacy and data protection, said the order also shows "the danger of using too strict a keyword search approach, where one missing or transposed letter in a word in a key e-mail may [mean it is] excluded from a search."

Due to these problems, some practitioners are now turning to alternative ESI search methodologies, such conceptual searching, he said, where the search is less tied to specific words.

How many ways to spell a name?

While the plaintiff in the *Northington* case – a Title VII sex and race discrimination suit – has an unusual first name (Ehnae), lawyers should include alternate spellings even for common names.

For example, with a party named William, the lawyers should include alternatives like Bill, Billy, Will and Willy, Gilliland said, adding that he knows a family friend who spells Bill with one "l." And in some cases, people go by a completely different name, a middle name or a nickname.

In addition to individual names, names of corporations or products, or in a pharmaceutical case the name of a drug, might also be terms for which to consider misspellings.

Social networking sites, including Twitter accounts, will also be a source of abbreviations and misspellings, Gilliland noted.

"Anything where people are typing on a smartphone in a moving vehicle increases the chance of error," he said.

Documents that involve more formal work will typically have correct spelling and many programs – like Microsoft Word, for example – have validation protocols that will highlight words spelled incorrectly or unusual spellings, Arkfeld noted.

Lawyers should address the issue early in the e-discovery process and discuss it with opposing counsel at the Rule 26(f) meet and confer, Gilliland suggested.

Arkfeld said a lawyer's approach may depend upon whether he or she is the requesting or producing party.

"A requesting party wants the other side to search for any kind of iteration of words and put in any and all spellings," he said. "For a producing party, it's a double-edged sword."

While a longer list of search terms will increase the defense's obligation to preserve all relevant ESI, not including misspellings could skew the search results, Arkfeld said.

"The best thing [the defense] can do is sit down and agree with the other side on what search terms to use," he explained.

That way, if the agreed-upon search terms are used and don't result in a smoking gun e-mail or document, the defense can point to the parties' agreement and avoid sanctions or a second collection.

"Especially if you are the producing party, get a search protocol in place to protect you," Arkfeld said.

A new type of searching

The misspellings issue aside, Arkfeld noted that many federal court judges are unhappy with keyword searching itself for failing to bring back all the data expected in a search.

In fact, U.S. Magistrate Judge John M. Facciola in the District of Columbia, a well-respected jurist in the world of e-discovery, has said that in some cases, the use of as certain search methodology requires an expert opinion.

In a 2008 case, he wrote that "[w]hether search terms will yield the information sought is a complicated question involving the sciences of computer technology, statistics and linguistics. … For lawyers and judges to dare opine that a certain search term would be more likely to produce information is truly to go where angels fear to tread. This topic is clearly beyond the ken of a layman," he wrote. (*U.S. v. O'Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008).)

Continued on page 11

Avoiding the pitfalls of 'frictionless' social media

By Correy E. Stephenson
Staff writer

Technological advances continue to make life easier and yet more complicated at the same time.

Take "frictionless" social media – full integration between sites like Facebook and various third party applications and websites so that friends and family know where you are and what you are doing at all times, without a user having to make any status updates.

More and more sites and apps automatically share user information without any action taken on the part of the user, hence the lack of friction.

"The idea is that people who are connected to Facebook are connected to everything else on the Internet," said Stephen D. Riden, a commercial litigator at Beck Reed Riden in Boston. "But it also means giving away information. I have several friends that on a daily basis, I know what articles they are reading – it's a little creepy."

For fans of social media, such ease of use is a positive development.

But for lawyers?

"This is a treasure trove of information," said Lee Rosen, who practices family law at the Rosen Law Firm in Raleigh, N.C. "No one realizes that they have authorized that sort of checking in and frictionless reporting and we suddenly know things about them they don't even realize."

As a divorce lawyer, "in the old days we had to follow an adulterous couple sneaking into a hotel room, holding hands," Rosen said. "Now [the information] is on Facebook for the world to see."

Online, worldwide

Facebook has made several recent additions to its social media platform to increase users' sharing of information with a minimum of effort. As it continues to increase its partnerships with third party sites, users who enable other sites will then have their information displayed on Facebook as a status update or on their wall, depending on the app.

Once enabled, a user's activity is continuously tracked – and shared. So the videos that are watched, the articles read, the music listened to or the purchases made may all be visible for others to see.

"What I'm really excited about as a divorce lawyer is frictionless check-ins at locations," Rosen said. While most users still have to check in manually, GPS-enabled devices will soon automatically check in at the location and share the news that a user just checked in at the Bellagio Hotel in Las Vegas, for example, to cheat on his or her spouse, he said.

Dating services are also starting to use this frictionless reporting, Rosen added, so that the fact a person is using the site, as well as details about their activities on it, will be added to a user's status update as well.

People don't understand the technology and its implications, Rosen said.

"No one understands the privacy settings on Facebook and they forget who they are friends with and which apps collect information and disseminate it to others," he said. "No one [will] care until it is too late."

Facebook's 750 million users are also in the process of receiving a new feature known as "Timeline," which compiles all available data about a user – including information from friends and third party sources – and plots it all by date and time.

For opposing counsel, that means simply looking up relevant dates to find out what a party was doing, whether it was eating at the local McDonald's, shopping for new shoes online or reading an article about the side effects of medication.

The electronic discovery implications of such technology are boundless.

While it may be innocuous for friends to know of a recent purchase of the latest Stephen King novel, "a criminal defendant may have just purchased what turns out to be a weapon on Amazon and that purchase information is evidence of interest to a District Attorney," Riden said.

Employers could check an employee's Facebook account to learn that they spent their day surfing the web, buying holiday gifts or watching kittens do funny things on YouTube.

"So much of the discovery process is just setting up a timeline and creating a chronology of events, when certain things happened and what was said and done," Riden said. "Technology that can do that automatically and is almost failsafe makes a lawyer's job much easier."

The Timeline feature also serves as a reminder that what you do online is never forgotten and does not just disappear, Riden said. So pictures from a college fraternity party can still be found by a potential employer performing a background check years later.

Accessing a user's information is surprisingly easy, attorneys said.

Rosen said in the majority of cases he doesn't need to serve a subpoena because the opposing party has set their information to be public.

Riden agreed, noting that a subpoena can also be obtained for access.

Digital breadcrumbs

While the possibilities for opposing counsel are positive, keeping a client who is a social media fan from exposing too much presents a challenge.

"By the time most people come to see us, it's too late," Rosen said. "They have already created mounds of evidence in this way that they didn't even realize they were creating."

Defending a client with "digital breadcrumbs" – items left in their online tracks that leave a trail for opposing counsel – puts lawyers in a tougher position, Riden acknowledged, and some circumstances may require disclosure of information to the other side. In situations where potentially damaging comments have been made, "I try to get the context for what was said and the background to hopefully make the errant Tweet or comment better understood to not harm my client's case," he said.

Most importantly, do not remove information from social media or instruct a client to do so.

Recently, a state court judge in Virginia awarded defense counsel $722,000 in clawback legal fees after the plaintiff attempted to thwart access to his Facebook account where he also deleted pictures.

Judge Edward Hogshire ordered the plaintiff's attorney to pay $522,000 of the total sanction; he had previously reduced the $10 million jury award by $4.13 million after finding that both the plaintiff and his attorney had withheld and lied about evidence to the court.

Instructing clients to stay off Facebook or Twitter is impossible, Rosen said.

"Telling someone to get off of social media is like telling them to stop breathing," he said. "Our responsibility is to make them aware of what they may have done and may continue to do," by explaining the implications of social media use.

Riden said he warns clients about the ramifications of expressing their frustration with their legal situation online, and suggests that they put it all in a long e-mail, which they can send to him. "It helps them vent and is protected by the privilege."

Questions or comments can be directed to the writer at: correy.stephenson@lawyersusaonline.com

Tips for capping e-discovery costs in smaller cases

By Nora Tooher
Contributing writer

Electronic discovery shouldn't cost more than a case is worth.

Uncovering relevant electronic evidence has become critical in a wide range of civil litigation, from divorce cases to business disputes. But keeping a lid on e-discovery costs can be challenging, especially in smaller cases.

To curb e-discovery costs, Conrad Jacoby, an attorney and litigation technology consultant in the Washington, D.C. area, recommends "thinking creatively."

Target searches, split costs with the opposing side and shop for the most cost-effective document retrieval, storage and review options, he suggested.

And don't panic.

"You just have to get over the fear of [electronic discovery]," Jacoby said. "You're still using your lawyer/investigator skills to figure out the relevant evidence. We just are looking in different places."

Jacoby said the most important step for controlling e-discovery costs is scheduling a "meet and confer" with the attorneys for the other side.

"The number one thing is to talk to your opposing counsel," he said.

Even where it's not required, it's a great way of limiting the scope of a legal hold, he said, by agreeing on date restrictions, for example.

Michele Lange, director of legal technologies at Kroll OnTrack, an Eden Prairie, Minn. computer forensics company, agreed.

"The federal rules of civil procedure and various states mandate that you have a meet-and-confer conference early in the discovery process and that you discuss discovery. Don't let that be a formality. Use it to your advantage," said Lange. "If you can narrow the scope – by person, by time frame – you're going to limit the cost."

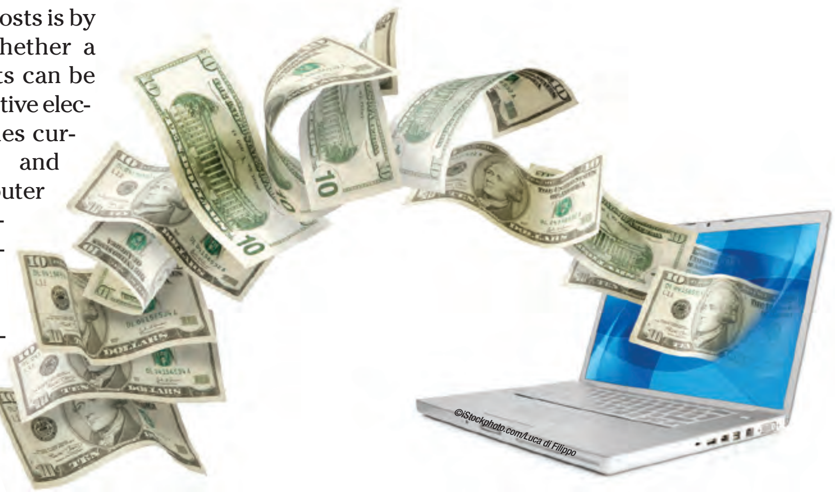
Paula Weseman Theisen, a partner and chair of the electronic litigation group at Meager & Geer in Minneapolis, encourages attorneys to conduct an e-discovery interview of their own client.

If you can determine that your client put everything that had to do with a contract dispute, for example, in one specifically identified folder, it will make collecting the data much faster and more cost-effective.

Getting the data

Another way to control discovery costs is by determining whether a party's requests can be satisfied with active electronic data – files currently stored and seen on a computer hard drive, according to Jacoby.

Sometimes, obtaining relevant data can be as simple as having the client create a Microsoft Personal Storage Table (.pst) file, which can be done by an outside vendor for $100 to $200 per computer user, or by the in-house IT person, he noted.



©iStockphoto.com

"You can collect that information without changing metadata and do it at a modest cost to a client," Jacoby commented. "For some materials, like e-mail messages, you don't have to bring in an exotic forensic specialist. You can work out a much lower-cost way of collecting [evidence]."

Or, you can hire a forensic expert just to extract key evidence, he suggested. For example, in a contract dispute with a former employee, a forensic expert could be brought in to examine the former employee's laptop, rather than every computer in the office.

Low-cost document review tools

Several experts said that there are an increasing number of tools aimed at reducing costs and speeding up the review process.

Theisen suggested keyword software review tools, such as Summation or Clearwell.

Jacoby suggested a web-hosted site, such as Catalyst CR, which allows attorneys to search documents using field, text, range, proximity and dates.

Lange recommends using early case assessment tools that for a small, upfront fee can show "who was talking to whom, what they were talking about, and through a series of charts and graphics really help you get a handle on your case."

Early case assessment tools include Ontrack's Advanceview and Equivio's Relevance, a document review product that uses "learning technology" for early case assessment and culling relevant documents.

Based on initial input from an attorney, the software assesses document relevance, which means the data set can be reduced to a much lower volume.

Share the costs

It's always a good idea to try to split the final tab for e-discovery with the other parties.

"Cost-sharing is really critical," Theisen said. "You can enter into cost-sharing agreements that can cut costs in half with two parties. Or, in multi-party cases, the party involved only pays a fraction."

She emphasized that controlling costs should be an ongoing effort throughout the entire process of electronic discovery.

"The cost-effective part of e-discovery isn't just one particular point in the process," she said. "It goes all the way from how you ask for or respond to a request, to review and production."

Also, don't be afraid to get help, Jacoby said.

"If you're in a small firm and this is overwhelming, you can bring in a consultant for a half day or day for a fixed price," he said.

Consultants' fees run about $1,500 for a half-day.

Questions or comments can be directed to the managing editor at: reni.gertner@lawyersusaonline.com

E-discovery ruling gives insight on errors, sanctions

By Correy E. Stephenson
Staff writer

Lawyers across the country are looking for insight and guidance on proper sanctions for e-discovery errors in a recent opinion from a U.S. District Court in New York.

In *The Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities*, Judge Schira Scheindlin addressed litigants' failure to follow proper litigation hold and document preservation techniques and established a framework for awarding the appropriate sanctions.

The decision, issued in January 2010, comes six years after Judge Scheindlin's seminal decision in *Zubulake v. UBS Warburg*.

The *Pension Committee* decision "is certainly a successor to *Zubulake* and gives practitioners the next step down the road," explained Michael Hindelang, a partner at Honigman Miller in Detroit, Mich. and chair of the firm's e-discovery group. "Now that we learned the basic ground rules from *Zubulake*, how do we apply them?"

The plaintiffs in the latest case did not engage in willful misconduct, Judge Scheindlin determined – the behavior consisted of failure to issue timely litigation holds, as well as a failure to supervise the production and review of electronically stored information – but the parties still deserved to be sanctioned.

Judge Scheindlin's expertise in the e-discovery world and the lack of existing case law on the issue means that judges and practitioners in all jurisdictions will look to the decision for guidance, said Robert Brownstone, Law & Technology Director at Fenwick & West in Silicon Valley.

Kenneth J. Withers, director of Judicial Education and Content at The Sedona Conference, a non-profit organization in Phoenix that works to advance law and policy in areas like electronic discovery, said the decision is important because it is "a very clear explanation of the intricate relationship between the prejudice a party may suffer as a result of someone else's loss of discoverable data, the culpability with which it was lost and the sanctions that attach."

Duties – and sanctions

The litigation began in 2004 when a group of investors brought suit to recover $550 million stemming from the liquidation of two hedge funds based in the British Virgin Islands. They asserted claims under federal securities laws against former directors, administrators and other officials connected with the funds.

During the discovery process, the defendants discovered substantial gaps in the plaintiffs' document production. Depositions were held and declarations were submitted.

The defendants then moved for sanctions, seeking to dismiss the complaint. They claimed that 13 of the plaintiffs failed to preserve and produce documents – including electronically stored information – and submitted false and misleading declarations regarding their document and preservation efforts.

Judge Scheindlin agreed that each of the plaintiffs should be subject to sanctions, but declined to dismiss the suit.

Instead, she established a framework of culpability and applied it to each plaintiff's behavior.

Judge Scheindlin first determined the various plaintiffs' level of culpability on the continuum ranging from negligence to gross negligence to willful misconduct. Using examples at each stage of the discovery process, she explained the gradations between each level of conduct.

For example, "the failure to collect records – either paper or electronic – from key players constitutes gross negligence or willfulness as does the destruction of e-mail or certain backup tapes after the duty to preserve has attached. By contrast, the failure to obtain records from all employees (some of whom may have had only a passing encounter with the issues in the litigation), as opposed to key players, likely constitutes negligence as opposed to a higher degree of culpability," she wrote.

A litigation hold should direct employees to preserve all relevant records – both paper and electronic – as well as create a mechanism for the collection of preserved records so that they can be searched by someone other than the employee, the decision said.

Sanctions should be determined on the same sliding scale, Judge Scheindlin said, with the most severe sanctions – dismissal or preclusion – levied as a result of willful conduct, while less severe sanctions, like fines and cost-shifting, should be applied in cases of negligence.

Judge Scheindlin found that seven plaintiffs acted negligently and six were grossly negligent, and all should therefore pay for the defense's attorney fees. In addition, she crafted an adverse inference instruction for the grossly negligent plaintiffs, intended to alleviate the harm suffered by the defendants.

Certain plaintiffs were also ordered to conduct some additional discovery.

"While litigants are not required to execute

Continued on page 11

Streamline electronic discovery using a data map

By Correey E. Stephenson
Staff writer

Looking for a way to cut electronic discovery costs and streamline your knowledge of a client's electronically stored information? Try a data map.

Thomas Seymour, an associate in the legal group of Huron Consulting Group in Chicago, said that the best description of a "data map" is "a collection of information about data sources that are likely to contain information potentially relevant to litigation."

"A data map can be anything from a simple diagram of hardware showing what items are connected to what, or it can … show the flow of data through various applications and how custodians have influence over other aspects of the process," explained Michael Hindelang, a partner at Honigman Miller, Detroit, Mich., and co-leader of the firm's e-discovery group.

On the most basic end of the spectrum, a map could generate a picture of anything connected to the network, with boxes designating servers, workstations, printers and back-up drives, with lines showing how each is connected.

Sounds simple? That's the point.

"For e-discovery purposes, what a client has is one of the most important things," Hindelang said. "Lawyers need to know: are there sources of information that perhaps we didn't look at, or don't know about?"

He used the example of old computers tucked away in the back of a spare office where temp workers sat in a better economy, with no one having used them in months or even years.

But "a data map will show those are still active machines and a source of potential information," Hindelang said.

When to use it

A data map is very useful at the conference stage, said Hindelang, because it "lays everything out for you in list or graphic form and … this is an easy thing to show the judge and opposing counsel when you are trying to work out an e-discovery plan."

But it can also be helpful even earlier in the process, noted Charles Ragan, managing director of the legal group of Huron Consulting Group in Chicago.

For example, the map can identify if systems are set to auto-delete. If litigation occurs, the client's attorneys will know that they need to turn off that function, he noted.

A data map can also help at the collection


©iStockphoto.com

and production stages – if a lawyer knows what information is or is not readily accessible, he or she can more easily determine what the cost and burden of producing it will be, said Ragan.

The map can also indicate a contact person for certain subjects or types of data – a valuable tool for lawyers looking for better understanding about an issue later in the litigation process, Seymour said.

With the map, "all those metrics are lined up in advance," said Ragan.

Size matters

The intricacy of a data map will depend upon the size of the company, the frequency that it is involved in litigation and the level of technology.

"Typically, in larger organizations, there will be a much more complicated version that will also be more expensive" to produce, Hindelang explained.

In addition, a regulated business may need a data map for compliance issues, he noted.

For a smaller operation, the network operating system may generate its own map, which may provide the necessary information.

For something more complex, Ragan suggested that companies leverage existing technology in the company to cut down on cost. Some applications can be configured to track the flow of information and even doing piecemeal maps – of just one department, for example – is better than nothing.

"It's better to start small, and cover the [information] that is going to be the biggest issue for the organization," he said.

While some businesses may be hesitant to take on the project, the cost of a data map could translate into major savings, because courts are increasingly awarding sanctions for e-discovery violations or spoliation.

In addition, a company that has to scramble after being sued in order to understand its electronically stored information could end up paying exorbitant fees, Seymour cautioned. "It's always going be cheaper to be proactive."

Privilege issues are another concern.

But Ragan said that a data map should be considered work product, whether it was created in anticipation of specific litigation or not.

"If the client is a manufacturing company and the data map includes information on products, sales and the manufacturing process, but a case involves an injury to an employee in the parking lot, you don't have to turn over the entire data map," he said. "Courts are looking for candid disclosures, but always require that the information be relevant."

Keep it up-to-date

The value of a data map is in its accuracy, so it's important to keep it current.

"The key thing is that the map has to be up-to-date or you run the same risks as working without [it]," Hindelang said. "You may present an incomplete picture to the court or to the other side, you increase your chances of forgetting to look at certain sources of information or data and you increase concerns about spoliation."

Seymour agreed.

"It's important to think of the map as an ongoing business process," he said.

A one-location office with a few employees that has a back-up system and an e-mail server is relatively easy to keep track of for data mapping purposes. So updates may only be necessary when a purchase is made or someone is let go or hired, Hindelang said.

But an organization with multiple offices with hundreds of potential known items on the network – servers, workstations, printers with memory – needs to be updated far more frequently.

"The question you have to ask yourself is, what level of confidence are you looking for?" Hindelang said. "Is it a snapshot of last month, or last quarter, or from six months ago or even last year? Can you put together a complete picture for the judge or opposing counsel?"

For some companies, it may be too expensive to update frequently, if there is a constantly changing IT structure, for example.

But the "more complete picture you can present, the better you can communicate information to opposing counsel and the judge," Hindelang noted.

Questions or comments can be directed to the writer at: correy.stephenson@lawyersusaonline.com

E-discovery ruling gives insight on errors, sanctions

Continued from page 9

document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation. All of the plaintiffs in this motion failed to do so and have been sanctioned accordingly," Judge Scheindlin wrote.

Lessons for practitioners

Withers noted that the decision may surprise many lawyers because the *plaintiffs* were sanctioned.

The last thing on most plaintiffs' minds is that they need to preserve data, but their obligation to do so may actually be greater than the defendant's, Withers said, because they have a better awareness of the total scope of the potential claims and defenses, at least in the early stages of a case.

Other important guidance from the case is contained in Judge Scheindlin's discussion of the levels of culpability, Withers said.

The levels range from negligence to willful activity and each level has its own standard, requiring the party that feels wronged to demonstrate the prejudice they suffered – which is then used to determine the appropriate sanctions.

"If something was lost through mere negligence, then the party claiming it was prejudiced has a pretty high burden to show that the information was both relevant and material and would have favored it," Withers explained. "If, however, the action is determined to be grossly negligent, then the trier of fact may presume that the lost material was relevant and the loss was prejudicial – and the scale goes up from there."

Because the decision deals with a common problem – litigation holds – it provides even more value for practitioners, Hindelang said.

"There are a lot of cases where litigation holds aren't perfect, or there are problems with the collection," he said.

Brownstone, who also teaches e-discovery at the University of San Francisco Law School, said he gleaned valuable points from the decision.

First, he noted the emphasis on following through with clients on a regular basis, even in cases where the litigation may be put on hold or move slowly.

"The lesson is that even if nothing is happening in the trenches, counsel should not be lax and should be in touch with clients on a periodic basis," Brownstone said. "It is very important to have ongoing communication, and to memorialize the content of that information."

Having a policy for preservation and collection in place, following it and documenting it – even if information that is deleted is later deemed relevant to litigation – will offer a company some protection.

Whether in a memo to the client or to the client's file, "memorialize, memorialize, memorialize," Brownstone stressed.

He also highlighted the portion of the opinion dealing with one plaintiff's failure to collect electronically stored information from an ex-employee.

"Not making sure that preservation and collection reaches a key player who is an ex-employee, or failing to follow up with an ex-employee, could [lead to] sanctions for gross negligence purposes," Brownstone said. "It is very helpful for any organization to have a 'time out' window whenever anyone leaves the employ," where that person's hard drive and e-mails are stored for a set time period, like 30 or 60 days.

Questions or comments can be directed to the writer at: correy.stephenson@lawyersusaonline.com

Misspellings can create issues for the e-discovery process

Continued from page 6

Ken Withers, director of Judicial Education and Content at The Sedona Conference, a nonprofit organization in Phoenix that works to advance law and policy in areas like electronic discovery, noted that the issue of misspelling words or alternative spellings can be addressed with different types of searching.

"Computer scientists and others have developed methods of training computers to be much smarter than using brute force word searching," he said. "Sophisticated search and information retrieval now involves criteria that go way beyond character strings that appear in a text database, and now include relationships between various communicants, having the computer identify whole concepts, not just words, and involving the proximity of words and concepts to each other."

For example, in a case about gemstones and searching for the word diamond, the computer could exclude discussions of baseball or wedding planning. Using mathematical probability, the computer could also look for things that don't exist in the database – such as at what point in time people stop talking about an issue, which could be very important in a case, Withers said.

The new methodologies allow litigants to maximize two variables: recall and precision, he explained. While the use of alternate spellings and misspellings may expand recall, it will decrease precision, he said, which is why courts and litigants are increasingly turning to new types of searching.

For the best results, Withers said attorneys should take a small sample of the ESI collection and run a search with a few keywords or data concepts in collaboration with the opposing party.

Then, both sides should examine the results and determine how successful the first run was, he said, before refining the search parameters to increase accuracy.

"The parties might do this two or three times before they press the button and do the final search of the complete ESI collection. They will have a much narrower, much better-defined search that will maximize precision and recall," Withers said.

Questions or comments can be directed to the writer at: correy.stephenson@lawyersusaonline.com