Electronic Discovery Update
April 2011

KRAMER LEVIN

In this Issue

Editors

If you have any questions or would like more information concerning any of these topics, please contact:

Norman C. Simon 212.715.7816
nsimon@kramerlevin.com

Norman C. Simon is a litigation partner with significant experience in the area of electronic discovery and chairs the firm's E-Discovery Practice.

Brendan M. Schulman 212.715.9247
bschulman@kramerlevin.com

Brendan M. Schulman is Kramer Levin's E-Discovery Counsel and a member of the firm's E-Discovery Practice.

Samantha V. Ettari 212.715.9395
settari@kramerlevin.com

Samantha V. Ettari is a litigation associate and member of the firm's E-Discovery Practice.

Striking a Balance after *Pension Committee*: Court Emphasizes the Need to Establish Relevant Data Loss Before Imposing Sanctions

Last year, Judge Shira A. Scheindlin's *Pension Committee* decision from the Southern District of New York garnered much attention nationwide for its detailed and stringent analysis of the law relating to document preservation and the litigation hold process. A new Southern District of New York decision issued by Magistrate Judge Francis — also of the Southern District of New York — takes issue with some of the analysis in *Pension Committee*, and holds that the failure to abide by preservation standards "does not necessarily constitute negligence, and certainly does not warrant sanctions if no relevant information is lost." In *Orbit One Comm. v. Numerex Corp.*, 2010 WL 4615547 (S.D.N.Y. Oct. 26, 2010), the court emphasized the need to establish relevant data loss before imposing sanctions, while reiterating the need for parties to continue to take a broad approach in their preservation efforts.

Pension Committee's Stringent Standards

Among the holdings in the *Pension Committee* case was an enumeration of the types of "failures [that would] support a finding of gross negligence, when the duty to preserve has attached: to issue a written litigation hold; to identify all of the key players and to ensure that their electronic and paper records are preserved; to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody, or control; and to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources." *Pension Committee*, 685 F. Supp.2d 456 at 471. A failure of this kind constitutes gross negligence because "that failure is likely to result in the destruction of relevant information." *Id.* at 465. Under *Pension Committee*, a finding that a party acted with gross negligence would lead to sanctions, including an adverse inference instruction to the jury that they may "presume . . . that such lost evidence

continued on page 2

Striking a Balance after *Pension Committee*: Court Emphasizes the Need to Establish Relevant Data Loss Before Imposing Sanctions

continued from page 1

was relevant, and that it would have been favorable" to the requesting party — although this presumption may be *rebutted*. *Id.* at 496.

The framework generally established by *Pension Committee*, particularly when read independently from the facts of that case, is generally perceived as formalistic in nature: the failure to undertake certain steps upon the reasonable anticipation of litigation will invariably result in a finding of gross negligence, an adverse inference instruction to the jury, as well as other sanctions. That the conclusion was considered rebuttable has largely been considered little comfort, as it is plainly difficult to "prove the negative" as to relevance and prejudice of documents that no longer exist.

The *Orbit One* Case: Background and Claims

In *Orbit One*, the court was confronted with plaintiffs who had, like many of the plaintiffs in *Pension Committee*, failed to take appropriate preservation steps. Orbit One, a satellite communications corporation founded by David Ronsen, was acquired in 2007 by Numerex, another company in the same industry. Numerex agreed to an "earn out" provision relating to future earnings targets and entered into employment agreements with Ronsen and other former Orbit One executives. Two years later, however, Ronsen brought an action against Numerex alleging interference with his management functions, the earn-out provision and various violations of the employment and acquisition agreements. Ronsen also subsequently resigned from Numerex, which itself brought claims against him for misappropriation of proprietary information. The specific claims do not appear to play a large role in the outcome of the decision, although it seems plain from their general description that many aspects of Ronsen's management of Orbit One, as well as the company's financial performance, could be the subject of relatively broad discovery.

> The court set out various examples of how *Ronsen* and *Orbit One* failed to take appropriate preservation steps during the course of the dispute . . . These failures repeatedly placed data at risk of loss.

A Series of Preservation Failures

The court set out various examples of how Ronsen and Orbit One failed to take appropriate preservation steps during the course of the dispute. First, when litigation was reasonably anticipated, the initial litigation hold was established without input from information technology (IT) personnel, lacked detailed instructions, was not disseminated to all relevant persons, and compliance was not monitored. Second, once litigation actually was commenced, counsel failed to implement a formal litigation hold. Third, IT personnel were not informed of the litigation hold when information was, for various reasons, deleted from servers, archived or otherwise manipulated. Fourth, during the course of events, primary responsibility for preservation efforts remained with Ronsen, the individual who had the greatest incentive to destroy harmful evidence. Fifth, Ronsen's treatment of information within his control was viewed as "cavalier" –he removed computer hardware from the premises, permitted it to leave his own control, and failed to document his archiving practices. *Orbit One*, 2010 WL 4615547 at * 12.

These failures repeatedly placed data at risk of loss during the course of events. For example, a desktop computer containing potentially relevant data was moved to a home garage and subsequently "cannibalized" by a technician in order to build another one. The original hard drive was recovered only later, when the technician was contacted. In another example, Orbit One's IT administrator undertook an initiative to increase server storage space. As a consequence, over six gigabytes of data were removed from the company's server. That data was later located on an external hard drive that had been used for archiving purposes. Additionally, after litigation had commenced, backup disks were taken out of rotation and stored in Ronsen's office safe. However, Ronsen subsequently took them home and returned them only after he had resigned from Numerex. Also during the relevant period, Ronsen's laptop hard drive failed and was replaced. An examination by a forensic expert in connection with the spoliation motion determined that the laptop had been synced with the company's servers such that data was not likely to have been lost, although the court noted that the possibility of data loss could not be ruled out entirely.

continued on next page

The Key Factor of Relevance

Notwithstanding the failure to implement proper preservation efforts and the various ways in which seemingly relevant data was placed at risk of loss, Judge Francis declined to impose any sanctions. After noting that in the Second Circuit, "a 'culpable state of mind' for purposes of a spoliation inference includes ordinary negligence," the court focused on the issue of relevance. According to the *Orbit One* decision, "a court considering a sanctions motion must make a threshold determination whether any material that has been destroyed was likely relevant even for purposes of discovery." *Id.* at *10. The best approach is to consider preservation failures as only one factor in the analysis and "consider the imposition of sanctions only if some discovery-relevant data has been destroyed." *Id.* at 11.

> "[A] court considering a sanctions motion must make a threshold determination whether any material that has been destroyed was likely relevant even for purposes of discovery."

Judge Francis noted his disagreement with court decisions that may be read to omit the relevancy showing, such as the *Pension Committee* decision. "The implication of *Pension Committee*, then, appears to be that at least some sanctions are warranted as long as any information was lost through the failure to follow proper preservation practices, even if there [has] been no showing that the information had discovery relevance, let alone that it was likely to have been helpful to the innocent party. If this is a fair reading of *Pension Committee*, then I respectfully disagree." *Id.* at 10. Judge Francis did agree that once culpable conduct and relevant data loss *are* established, there should be a presumption that the lost data would have been harmful to the spoliator, but "[f]or sanctions to be appropriate, it is a necessary, but insufficient, condition that the sought-after evidence *actually existed and was destroyed*." *Id.* at 11 (emphasis in original).

The court also took issue with the directive in the *Pension Committee* decision that a formal written litigation hold is always necessary: "For instance, in a small enterprise, issuing a written litigation hold may not only be unnecessary, but it could be counterproductive, since such a hold would likely be more general and less tailored to individual records custodians than oral directives could be. Indeed, under some circumstances, a formal litigation hold may not be necessary at all." *Id.* at 11. Presumably, under an application of the *Orbit One* decision, a similarly flexible, context-specific analysis would also apply to the other types of preservation failures identified in *Pension Committee* as constituting gross negligence.

Failure Without Consequence

Applying its relevance standards to the facts before it, the court determined that "there is insufficient evidence of any loss of discovery-relevant information." *Id.* at 12. Data removed from servers was located on an external archival hard drive, data on the desktop computer that had been removed from the company was synchronized with company servers, the laptop drive that failed and was replaced was synced with the servers as well, and the backup disks that were physically removed from the company were later returned. Moreover, "[n]o witness has identified any significant document that has not been produced in discovery." *Id.* at 14. As a result, the motion for sanctions was denied.

Broad Preservation Still Recommended

Notwithstanding Judge Francis' seemingly heightened standards for imposing spoliation sanctions, he rejected the proposition – frequently proposed by e-discovery practitioners and respected institutions such as The Sedona Conference – that concepts of reasonableness and proportionality that are present in the federal rules should expressly apply at the preservation phase. These concepts "may prove too amorphous to provide much comfort to a party deciding what files it may delete or backup tapes it may recycle. Until a more precise definition is created by rule, a party is well-advised to retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches." *Id.* at 6. Indeed, Judge Francis finds it "unlikely" that a court "would excuse the destruction of evidence merely because the monetary value of anticipated litigation was low." *Id.* at n. 10. In a footnote, the *Orbit One* decision indicates that reasonableness and proportionality cannot be assumed to

continued on page 7

Is Social Networking a No-Privacy Zone? The Discoverability of "Private" Social Media Data

Introduction

In the world of social networking, users will commonly choose information-sharing over privacy — often without realizing that they are making such a choice. Facebook alone boasts 500 million active users with an average of 130 friends each, who share more than 30 billion "pieces of content" each month. Facebook, Press Room, http://www.facebook.com/press/info.php?statistics (last visited Feb. 22, 2011). Its founder, Marc Zuckerburg, has opined that "the age of privacy is over." Bobbie Johnson, *Privacy No Longer a Social Norm, says Facebook Founder*, The Guardian, Jan. 11, 2010, *available at* http://www.guardian.co.uk/technology/2010/ jan/11/facebook-privacy. Users of social networks typically share personal information, pictures and videos via user-created profile pages, notes and private messaging services, inadvertently creating a depository of potentially valuable, discoverable evidence for litigants. This wealth of "pieces of content" has recently raised the issue of whether parties are entitled to discovery of an adversary's social networking data, particularly when that data is designated to remain "private."

Two recent decisions have begun to define the contours of social media discovery, with seemingly divergent results. In *Romano v. Steelcase, Inc.*, the New York Supreme Court found that a plaintiff did not have a reasonable expectation of privacy in certain content on her access-restricted Facebook and Myspace pages and ordered discovery. 907 N.Y.S.2d 650 (N.Y. Sup. Ct., Suffolk Co. 2010). Conversely, in *Crispin v. Audigier, Inc.*, a federal court in California quashed defendant's subpoenas to social network providers to the extent they requested private, access-restricted content, relying on the classification of the information under a federal statute. 717 F. Supp. 2d 965, 970 (C.D.Cal. 2010). These cases suggest both the limits of social media "privacy" and also the methods that may be used by parties to obtain social media discovery.

New York State Court: *Romano v. Steelcase*

The plaintiff in *Romano* brought suit against Steelcase for personal injuries and loss of enjoyment of life. Steelcase asserted that the public portions of the plaintiff's Myspace and Facebook pages contained evidence of an active lifestyle, including travel "during the time period she claim[ed] that her injuries prohibited such activity." *Romano*, 907 N.Y.S.2d at 653. After Romano refused Steelcase's discovery requests for additional information from her social network accounts, Steelcase sought an order granting access to plaintiff's "current and historical Facebook and Myspace pages and accounts, including all deleted pages and related information." *Id.* at 651. Romano objected to the application on privacy grounds.

The *Romano* court's ruling on the discoverability of plaintiff's "private" social networking data turned on the presence of material she had placed on the *public* portions of those sites that contradicted her claims. The court explained

> [U]nder CPLR 3101 . . . a plaintiff who "places [her] physical condition in controversy, may not shield from disclosure material which is necessary to the defense of the action."

that under CPLR 3101, which provides for "full disclosure of all nonprivileged matter which is material and necessary to the defense or prosecution of an action," a plaintiff who "places [her] physical condition in controversy, may not shield from disclosure material which is necessary to the defense of the action." *Id.* at 652; CPLR 1301. Thus, "in an action seeking damages for personal injuries, discovery is generally permitted with respect to materials that may be relevant both to the issue of damages and the extent of a plaintiff's injury." *Romano*, 907 N.Y.S.2d at 652.

The court found that the plaintiff's public profile page contained information contrary to her claims and deposition testimony, in that it depicted 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." *Id.* at 654. Accordingly, the court granted Steelcase access to the private portions of Romano's social networking site pages. Justice Arlen Spinner explained that because the public portions of those sites contained content material necessary to the litigation, there was a reasonable likelihood that the same would hold true as to the private portions.

continued on next page

The *Romano* court then turned to whether there is "a right to privacy regarding what one posts on their on-line social networking pages such as Facebook and Myspace" (*Id.* at 656) — an issue of first impression in New York. Because there was no New York case law directly on point, the court looked to other jurisdictions (including international) for guidance. Specifically, the *Romano* court relied on a personal injury case from the Colorado District Court in which the court granted a subpoena to obtain information from the public access areas of plaintiff's social networking sites. *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018 (D. Colo. Apr. 21, 2009). Justice Spinner also looked to a Canadian case that reached the same conclusion, emphasizing that individuals should not be allowed to hide behind "self-set privacy controls" on a site designed to share information with others, as this would deprive the adverse party of information that could be necessary to ensuring a fair trial. *Leduc v. Roman*, No. 06-CV-3054666PD3, [2009] O.J. No. 681 (O.S.C.J. Feb. 20, 2009). The *Romano* court found these cases instructive and adopted their reasoning. *Romano*, 907 N.Y.S.2d at 655. Justice Spinner held that to deny the defendant an opportunity to access the private pages "not only would go against the liberal discovery policies of New York favoring pre-trial disclosure, but would condone Plaintiff's attempt to hide relevant information behind self-regulated privacy settings." *Id.*

Justice Spinner concluded that the plaintiff in *Romano* had no reasonable expectation of privacy in access-restricted areas of her social network pages, in part, due to the very nature of Facebook and Myspace, which exist so that users may share information about their personal lives. The court looked to case law addressing analogous facts in the electronic information context which had concluded that there was no reasonable expectation of privacy in sent email (*United States v. Lifshitz*, 369 F.3d 173 (2d Cir. 2009)), or in shared electronic posts (*Beye v. Horizon Blue Cross Blue Shield of New Jersey*, 2008 WL 3064757 (D.N.J. July 28, 2009)). The court also examined Myspace's and Facebook's privacy policies, which provide that, notwithstanding a user's privacy settings, complete privacy is not guaranteed. Because the plaintiff knew that her private information *might* become publicly available, the court decided she could not claim she had a reasonable expectation of privacy. The court also cited commentaries regarding privacy and social networking sites, which explain that, "[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking." *Romano*, 907 N.Y.S.2d at 657.

Finally, the court found that the defendant's need for access to the content on the social networking sites outweighed plaintiff's privacy concerns. The court concluded that without access to this information, Steelcase would be "at a distinct disadvantage in defending this action." *Id.* Accordingly, because *Romano* did not have a reasonable expectation of privacy in the material, and the social media content was material and relevant, the court granted Steelcase's application.

[P]laintiff . . . had no reasonable expectation of privacy in access-restricted areas of her social network pages, in part, due to the very nature of Facebook and Myspace, which exist so that users may share information about their personal lives.

It is important to note that New York courts have emphasized the need for a factual predicate with respect to the relevancy of the data on social media accounts and will not permit parties to conduct "a fishing expedition." *McCann v. Harleysville Insts. Co. of New York*, 78 A.D.3d 1524, 1525 (4th Dep't 2010). In *McCann*, issued a few months after *Romano*, the Fourth Department held that a litigant is not entitled to another party's social network information without an adequate showing of relevancy, and found that defendant failed to make such a showing for discovery of plaintiff's Facebook account. The court permitted defendant the opportunity to renew its request at a later date.

continued on page 6

Is Social Networking a No-Privacy Zone? The Discoverability of "Private" Social Media Data

continued from page 5

California Federal Court: *Crispin v. Audigier, Inc.*

In *Crispin*, the plaintiff brought a copyright infringement claim against defendant Audigier, alleging that Audigier violated the parties' oral license agreement and sublicensed artwork to others without the plaintiff's consent. The defendants served subpoenas on Facebook, Myspace, and webmail provider Media Temple, to obtain, among other things, Crispin's subscriber information and all communications that referred or related to Audigier, including private social-networking messages. Audigier asserted that these communications were relevant in determining the nature and terms of the alleged agreement.

Crispin brought a motion to quash the subpoenas on the ground that they sought private electronic communications that internet service providers are prohibited from disclosing, pursuant to the Stored Communications Act of 1986 ("SCA"), 18 U.S.C. §2701 *et seq*.

The *Crispin* court first explained that the SCA created "a set of Fourth-Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." Crispin, 717 F. Supp. 2d at 972. The SCA prohibits electronic communication services (ECS) and remote computing services (RCS) from voluntarily disclosing users' private messages, such as electronic mail, to outside entities and individuals, absent a statutory exception. *Id*.

The *Crispin* court then evaluated whether a user's private communications sent through and held by social networking sites are afforded protection from disclosure under the SCA, an issue of first impression. Judge Margaret M. Morrow reviewed provisions of the SCA that apply to "providers" of communication services and the information in their custody concerning individuals and companies. The SCA defines an ECS provider as "any service which provides to users thereof the ability to send or receive wire or electronic communications" and RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." The court reasoned that Facebook and Myspace are hybrid providers that allow several types of communications, with varying levels of privacy. Because these social network sites "provide private messaging or email services," they were deemed to be qualified as ECS providers. *Id*. at 980. Thus, those features of the sites are protected under the SCA in the same manner as traditional web-based email providers.

Judge Morrow also found that Facebook and Myspace "wall postings" and comments also rendered these sites as RCS providers because their content is stored on the service providers' website, and can be kept private by restricting them to a limited number of others. The court cited to a case from the Southern District of New York, *Viacom International Inc. v. Youtube Inc.*, which found that because YouTube encouraged individuals to post videos to its site, yet also had restricted-access features limiting who can view the videos, it qualified as an RCS provider with respect to the restricted postings. 253 F.R.D. 256 (S.D.N.Y. 2008). The court analogized YouTube's restricted-access features to the postings and comments on Facebook and Myspace that can be posted and marked by the poster as private. Judge Morrow concluded that because Facebook and Myspace provide private messaging or email services, as well as electronic storage, they qualified as both ECS and RCS providers.

The *Crispin* court first explained that the SCA created "a set of Fourth-Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information."

The *Crispin* court quashed the subpoenas served on Facebook and Myspace to the extent they sought to compel disclosure of electronic messages, as well as Facebook wall and Myspace postings and comments, that had been marked as "private" by the plaintiff and that were not accessible to the general public. With respect to the portion of subpoenas that sought information from the plaintiff's other Facebook wall and Myspace comments and wall

continued on next page

postings, Judge Morrow found that there was insufficient evidence to determine whether these wall postings and comments constituted private communications, as the user's privacy settings for them were not clear. The court ordered further fact investigation to determine what privacy settings, if any, the plaintiff had employed.

Conclusion

Crispin and *Romano* provide important guidance to potential litigants seeking content from individuals' private social networking accounts. *Romano* suggests that — notwithstanding privacy settings — litigants may be ordered to disclose information or communications on social networking sites that may be relevant and material to a litigation because such discovery fulfills the mandates of liberal civil discovery rules. On the other hand, the *Crispin* decision suggests that civil parties seeking communications directly from a social networking site via subpoena may be prevented from obtaining much of this information by virtue of the Stored Communications Act. Access to adversaries' social networking pages and accounts will become increasingly important in personal injury, employment and fraud cases, where plaintiffs may post pictures and messages that contradict their claims. Arguably, the lesson from these cases for a party seeking discovery is to seek materials in the first instance from an adverse party, rather than a social networking provider. Moreover, it is prudent for potential litigants who can expect to receive discovery requests to exercise discretion in their communications on social networking sites even when "privacy" settings are utilized. ■

[T]he lesson from these cases for a party seeking discovery is to seek materials in the first instance from an adverse party, rather than a social networking provider.

Striking a Balance after *Pension Committee*: Court Emphasizes the Need to Establish Relevant Data Loss Before Imposing Sanctions

continued from page 3

create a "safe harbor" in the absence of "a court-imposed preservation order." *Id.*

Thus, parties may continue to be well-served by negotiating the scope of preservation with adversaries or, when that is not possible, approaching the court at an early phase when preservation issues promise to be complex or burdensome in a particular case. Additionally, Judge Francis' suggestion that a "rule" containing a "precise definition" is needed should encourage the nascent discussion on that very point within the Federal Rules Advisory Committee and other rulemaking bodies. In the interim, the best practice remains broad preservation and appropriate record-keeping. "In order to avoid sanctions, parties would be obligated, at best, to document any deletion of data whatsoever in order to prove that it was not relevant or, at worst, to preserve everything." *Id.* at 11.

With so many potential avenues of data loss, it might be said that plaintiffs in *Orbit One* were simply luckier than other parties whose lax preservation efforts have resulted in data loss and the award of sanctions in numerous other recent decisions. The *Orbit One* decision was an "easy" one in the sense that every source of data placed in jeopardy by plaintiffs ultimately turned out to be duplicated elsewhere or returned. In other cases, a renewed focus on relevance promises to entangle litigants in protracted disputes about what kinds of data may have existed on a data source that has been lost. Judge Francis' decision to place the burden of showing relevance upon the moving party before entertaining any form of sanctions reflects the continuing effort by sophisticated judges to balance the stringent preservation standards with the practical impact of lost data upon the merits of a case. ■

This article was originally published in Digital Discovery & E-Evidence, 11 DDEE 02, 1/20/11.

SDNY Ruling Requires Government to Produce Metadata in Response to FOIA Requests

Last month, Judge Shira A. Scheindlin of the Southern District of New York took yet another step in advancing e-discovery jurisprudence by ruling that metadata (that is, "data about data" which is often hidden from plain view) must be produced by the United States Government as part of its electronic records, in a usable format, when responding to requests under the Freedom of Information Act ("FOIA"). *National Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency*, 2011 WL 381625, at * 5 (S.D.N.Y. Feb. 7, 2011). This is the first federal court to have issued such a ruling. The decision highlights the increasing scrutiny courts are paying to the production of metadata and the provision of electronic documents in a usable format.

Background – Unclear and Unfulfilled Requests

Plaintiffs submitted identical FOIA requests to four governmental agencies asking for information pertaining to Secure Communities, a program that enlists the help of states and localities in enforcing federal immigration law. *Id.* at *1. After a minimal substantive response from the Government, Plaintiffs submitted a shortened request, requiring production of specific documents on an expedited basis. *Id.* Plaintiffs asked the Government to produce responsive records on a CD, to provide each document as a separate file, and with Excel documents in native format. *Id.*

After receiving an incomplete and tardy response to this abbreviated request, Plaintiffs moved to compel the production of documents. *Id.* The court ordered the Government to produce certain key records within three months. *Id.* Plaintiffs then sent the Government a Proposed Protocol Governing the Production of Records ("Proposed Protocol"), specifically requesting load files and metadata fields. *Id.* at *2. The Government subsequently produced five, unsearchable PDF files, consisting of an undifferentiated mix of electronic and hard-copy documents, without load files or metadata fields. *Id.* Plaintiffs found the production unusable and moved the court to order the Government to provide the records per the Proposed Protocol. *Id.* The Government defended its January 12 production, faulting Plaintiffs' failure to make a timely or explicit request for metadata and arguing that its production was sufficient because governmental disclosure under FOIA is not subject to the federal rules governing document discovery. *Id.* at *5.

ESI Treatment Under FOIA Similar To Rule 34

Judge Scheindlin dismissed the Government's timeliness defense as a "lame excuse for failing to produce the records in a *usable format*." *Id.* at *4. The court noted that Plaintiffs' email months earlier — requesting spreadsheets in native format and asking that each text record be produced as a separate file — sufficiently notified the Government of the form of production. *Id.* Instead of properly fulfilling Plaintiffs' requests, the Government not only failed to produce the records in a usable form, but actually provided records in a manner that was burdensome for Plaintiffs to use. *Id.* Judge Scheindlin also criticized the Government's failure to contact Plaintiffs concerning the method of production, observing that, "any ambiguity as to the nature of the requested format would have been resolved" if they had done so. *Id.* Indeed, a major refrain of the *National Day Laborer* decision is that parties must cooperate and use common sense when ESI discovery disputes arise. *Id.* at *8.

The decision highlights the increasing scrutiny courts are paying to the production of metadata and the provision of electronic documents in a usable format.

Judge Scheindlin explained that the underlying goals of the Federal Rules and FOIA are the same and "common sense dictates that the parties incorporate the spirit if not the letter, of the discovery rules in the course of FOIA litigation." *Id.* at *5 n.33. The Government defended its production on the grounds that metadata had not been

continued on next page

recognized as an integral part of an electronic record for FOIA purposes and, as such, metadata are separate records that Plaintiffs failed to request. *Id.* at *5. Responding to that argument, and recognizing that she was applying federal civil discovery rules to a statutory scheme that is silent on these issues, Judge Scheindlin wrote that "Rule 34 surely should inform highly experienced litigators as to what is expected of them when making a document production in the twenty-first century." *Id.* Judge Scheindlin then explicitly held "that certain metadata is an integral or intrinsic part of an electronic record. As a result, such metadata is 'readily reproducible' in the FOIA context." *Id.* Aware that the same metadata may not be available for all types of electronic records, Judge Scheindlin offered the following rule-of-thumb: "metadata *maintained* by the agency *as a part of an electronic record is presumptively* producible under FOIA, unless the agency demonstrated that such metadata is not 'readily reproducible.'" *Id.*

Finally, Judge Scheindlin addressed the Government's failure to produce properly separated documents with an associated load file. *Id.* at *7. Even if production formation was not specifically demanded as part of a FOIA request, the production of static images of ESI without "any means of permitting the use of electronic search tools is an inappropriate downgrading of ESI." *Id.* Judge Scheindlin noted the production was deficient precisely because Plaintiffs had no way of using an electronic search tool to review the material — the records had no metadata and were "lumped" together in five large PDF files. *Id.*

Far from simply outlining the general production protocol, Judge Scheindlin next furnished a blueprint for the Government's ESI productions. She listed by name twenty-three specific metadata fields that the Government is required to include in its future productions, such as "Source Path" and "Modified Date". *Id.* at *6-7. These fields "are the minimum fields of metadata that should accompany any production of a significant collection of ESI." *Id.* at *6 n.41, *7 n.41 (emphasis in original). Judge Scheindlin pointed out, however, that she was not suggesting that this protocol "should be used as a standard production protocol in all cases" and that static images may be appropriate for smaller productions.

In reaching her conclusions, Judge Scheindlin attempted to set a universal rule of thumb for parties everywhere. She wrote, "it is no longer acceptable for any party, including the Government, to produce a significant collection of static images of ESI without the accompanying load files." *Id.* Moreover, the court also admonished the parties for bringing issues before that court that "could have been avoided had the parties had the good sense to 'meet and confer,' 'cooperate' and generally make every effort to 'communicate' as to the form in which ESI would be produced." *Id.* at *8.

Judge Scheindlin held "that certain metadata is an integral or intrinsic part of an electronic record. As a result, such metadata is 'readily reproducible' in the FOIA context."

Conclusion

On a basic level, the *National Day Laborer* case clarifies the Government's document production obligations under FOIA. The larger picture, however, is the practical ESI discovery guidance provided by Judge Scheindlin as to the types of metadata that typically ought to be provided in any large document production, regardless of the underlying rules, as well as the need to produce ESI in a reasonably usable format. *National Day Laborer*'s guidelines promise to facilitate the production of usable ESI in a variety of contexts and to encourage parties to cooperate before bringing discovery disputes to the court. ■

Introducing Kramer Levin's E-Discovery Counsel, Brendan M. Schulman

Brendan A. Schulman serves as Kramer Levin's E-Discovery Counsel. In that capacity, he advises clients on the preservation, collection, processing, review and production of electronic information, with an emphasis on early case assessment and other cost-effective and defensible strategies. He also counsels attorneys and clients on effective discovery strategies and advocacy, with a view to emerging developments in this rapidly-evolving field. Here, Mr. Schulman shares his insights and experiences in the area.

Q: How did you become interested in electronic discovery?

Schulman: I have had an interest in computer technology since I was a teenager. In the late 1980's, as a hobby, I ran a BBS (bulletin board system), a dial-in computer message forum that was a local-level precursor of the internet. When I was in college, although I was an English major, I had a part-time job as a "Computing Assistant," helping fellow students fix computer problems. That was back when hardly anyone had an email address and before there were web browsers. My interest in technology continued in law school, where I was Executive Editor of *The Harvard Journal of Law & Technology* and wrote a published article on the copyright implications of MP3s and digital music — before anyone had heard of either Napster or the iPod. So for a long time, I've been intrigued by the impact of emerging technology on various aspects of society. As electronic discovery began to emerge as its own field, it was a natural fit as an area of focus within my commercial litigation practice.

Q: What does your role as E-Discovery Counsel involve?

Schulman: I am the firm's point person for legal issues relating to the preservation, review and production of electronic documents, and I act as a resource for both attorney teams and clients who have questions about legal standards and obligations. So, when there's an e-discovery dispute in a case, I may be brought in to help with a brief or a deposition of an IT representative. I consult with clients on novel e-discovery issues as they arise. In more complex or time-sensitive projects I might take the lead on designing and executing a discovery protocol. I also stay current with the latest developments in the field, write articles in legal publications, and speak at e-discovery events and conferences. I am an active member of The Sedona Conference, an organization dedicated to developing e-discovery law in a just and reasoned way. Another aspect of my role is to coordinate with our Legal Technology Services group to make sure we continue to make available cost-effective, state-of-the art tools for our lawyers to use in the discovery process.

Q: Given the integral role of IT specialists in the e-discovery process, how important is technological savvy to the practice of commercial law today?

Schulman: If you look at an average case, upwards of 50 percent of the time and money expended on prosecuting or defending a commercial action involves the collection, processing, review and production of documents in response to discovery requests, and related tasks such as privilege logs. The relevant documents are no longer found in warehouses or filing cabinets. They are on computer data systems and on an increasingly large collection of portable electronics. People are using new software platforms and tools to conduct business. Whether it's Facebook, instant messaging, Twitter, Salesforce, or the next new thing, the business communications that tell the story of "what happened and why" are increasingly found in computer data collections. In a recent high-profile corruption prosecution in New Jersey, the government was sanctioned for not preserving text messages sent between a confidential informant and FBI agents during the course of the investigation. You may have thought that teenagers were the only ones texting each other; it turns out that secret agents are doing it too. E-Discovery issues now impact every type of litigation, in every field of law. In the past

> "I am excited to be moving to the point where electronic discovery is something we do strategically, to win cases or settle on favorable terms, rather than just being a burdensome and expensive stage of the litigation process."

continued on next page

couple of years, courts have ordered the production of text messages, Facebook accounts, webhosted email files, and other seemingly esoteric electronically stored information ("ESI"). Understanding the technology that lies behind the tools people are using to conduct business is critical to formulating discovery strategies and also making sure the legal team has uncovered all the evidence that is important to defending or prosecuting a client's case.

Kramer Levin is one of the few firms that has a dedicated E-Discovery Counsel to consult with litigation teams and enhance our ability to respond to these demands with authority and efficiency. For example, not many attorneys know that you only need to examine a random sample of about 1,500 documents out of a very large set in order to speak with statistical confidence about the contents of the *entire* collection. That can be a tremendously useful way of trying to work through enormous volumes of documents.

Q: What is the greatest challenge in the e-discovery world?

Schulman: Document preservation remains a challenging issue for clients because it is so easy and inexpensive to preserve vast quantities of data, but so expensive to deal with that stored data in discovery. Relevant data is increasingly located in more obscure locations: on smartphones, on "cloud-based" repositories like Dropbox, on social media networks, or internal collaboration tools like Sharepoint. It can be difficult to balance the cost and effort of preserving those data sources with the relative importance of doing so, especially because you usually do not yet have a judge assigned who can provide guidance, and often your adversary has little incentive to be helpful. Organizations like The Sedona Conference are advocating for a new federal rule of proportionality to be applied to document preservation, and a few courts have already invoked that principle in the absence of a rule. Broad preservation still remains the safest practice.

Q: We often read about e-discovery sanctions cases. What are the real risks of being sanctioned?

Schulman: Unfortunately, the nature of our system is that courts usually don't articulate a standard or issue a discovery-related decision unless there is a serious dispute and something has gone terribly wrong. As a result, much of the e-discovery jurisprudence has developed around cases where things have really gone awry. In spoliation cases, it often isn't even the original spoliation that drives the sanctions decision, it's the failure to disclose the problem early on, and subsequent attempts to hide the problem. There is little appellate guidance in the area because discovery orders are rarely appealed and cases often settle after adverse discovery rulings.

In the Second Circuit, a party can be culpable and sanctioned for data loss even in the absence of bad faith. That means litigants with cases in the New York courts ought to be especially cautious. Cases in this jurisdiction have held parties to increasing standards, and recent studies have shown that the number of e-discovery sanctions decisions is on the rise nationwide, so it is important to be vigilant.

Q: Is there a case from the past year that is particularly noteworthy?

Schulman: A lot has been written about Judge Scheindlin's *Pension Committee* decision from last year. That decision articulated a very high standard for preservation, including the need to issue a written litigation hold upon the reasonable anticipation of litigation. It's a very important decision. But that was a case that involved parties who had made no effort at all to preserve documents. More noteworthy to me is the more recent *Harkabi v. SanDisk* case from the Southern District of New York. In *SanDisk*, which was the subject of an Electronic Discovery Alert we issued in September, the General Counsel of SanDisk had issued four preservation directives and had taken other steps to direct the preservation of sources of relevant ESI, including securely storing former employee laptop computers. A year later, the company's IT department wanted to reissue the laptops by copying the data to a server, a request that the IT personnel claimed was approved by the General Counsel's office. When the imaged data later was unable to be located, Judge Pauley imposed severe sanctions. The decision suggests a very high standard for in-house counsel even after the issuance of preservation instructions. Even if the attorneys do all the reasonable things required to preserve ESI, if you have a technical

continued on page 16

The Second Circuit Upholds Default Judgment for Spoliation

A handful of trial courts in the past few years have imposed the "ultimate sanction" of a default judgment against a spoliating party. That severe outcome was recently upheld by the United States Court of Appeals for the Second Circuit. *In Southern New England Telephone Co. v. Global NAPS Inc.*, 624 F.3d 123 (2d Cir. 2010) ("SNET"), the Court reviewed the conduct of defendant Global NAPS, Inc. ("Global") and its related entities, including its failure to comply with various discovery orders throughout the litigation and affirmed the granting of a default judgment against Global. *SNET* is one of the few cases to provide federal appellate guidance on the outcome of e-discovery sanctions and suggests that in circumstances involving bad faith, severe penalties may be upheld on appeal.

A History of Noncompliance

In *SNET*, plaintiff sought payment for services rendered to Global between 2002 and 2004. *Id.* at 130. During the course of discovery, the District Court for the District of Connecticut ordered Global to disclose its property and assets. *Id.* Additionally, Global was ordered to disclose "cash, stocks, bonds[,] . . . bank accounts and investment accounts, . . . real or personal property," and any debts owed to the company. *Id.* at 139. Over the course of two years, Global failed to comply with these orders, claiming that the relevant records were not in its custody. *Id.* at 140. The district court next ordered Global to produce any financial records *in the custody of third parties*. *Id.* The court warned that Global's failure to comply "[would] likely result in the entry of a default judgment" against it. *Id.* Again, Global failed to comply. *Id.*

During the course of these disputes, plaintiff amended its complaint to add the Global entities as defendants and to attempt to pierce the corporate veil, alleging that the "purported corporate structure of Defendants [was] a sham" because the companies were in fact one company. *Id.* at 130-31. Plaintiff sought discovery regarding those allegations. *Id.* at 141. The district court ordered Global to produce "the books of the company," including "balance sheets, cash statements, registers, journals, ledgers" in "the form in which the records are kept." *Id.* The court also ordered Global to produce other financial documents that had to be gathered from third parties. *Id.* Global produced very little new material, however, explaining that it was "unable to locate copies of all the ledgers from the relevant time period." *Id.* Global's Vice President of Regulatory Affairs attested in an affidavit that he had personally "searched the hard drive of the computer used by [Global's outside bookkeeper]," and that "[a]lthough the hard drive had [accounting] software, there was no data relating to a Global entity, merely the program." *Id.*

Forced to do an end-run around Global, plaintiff acquired excerpts of Global's financial documents by issuing a third-party subpoena to Global's tax accountants. *Id.* at 142. Many of these documents had not previously been produced, despite falling within the scope of the district court's previous orders. *Id.* Deposition testimony from a representative of the tax accountants contradicted Global's earlier claim that it did not have custody of its own financial records, leading the district court to conclude that Global's statement had been "a lie intended to delay the production of financial records in compliance with [plaintiff's] discovery requests and the court's discovery Orders." *Id.* at 140.

SNET is one of the few cases to provide federal appellate guidance on the outcome of e-discovery sanctions and suggests that in circumstances involving bad faith, severe penalties may be upheld on appeal.

Spoliation of Electronic Documents Using Anti-Forensic Software

In light of Global's failure to comply with the court's discovery orders, the parties jointly hired a forensic expert to investigate the computer that Global allegedly had searched. The computer belonged to the president and owner of Global's outside bookkeeping agent, Select & Pay, Inc. — who was a former employee of Global. *SNET*, 624 F.3d at 142. The forensic experts revealed that numerous files from the computer had been destroyed using a program called "Window Washer." *Id.* This application can be used with a separate "Shred" utility, allowing the user of a file to overwrite the content of the file, scramble the name, and delete without the possibility of forensic recovery. *Id.* Another function of Window Washer is the "Wash With Bleach" function, which allows the user to overwrite deleted

continued on next page

files. *Id.* at 143. Both the Shred and Wash With Bleach utilities are not default settings; a user must affirmatively choose to use them. *Id.* at 142-43.

The president of Select & Pay testified at a deposition that she had run the program only once, solely for the purpose of removing her personal information. *Id.* at 89. Forensic analysis, however, revealed that the president used the program *three* times, using both the Wash With Bleach and Shred utilities. *Id.* at 143. Out of 93,560 items stored in a database on the computer that held the metadata of all files that had once existed there, the forensic experts discovered that nearly 20,000 had been erased using the anti-forensic software, including shortcuts to files that bore names appearing to relate to financial records. *Id.*

Sanction: Default Judgment

The district court granted plaintiff's motion for a default judgment against the Global entities, including the veil piercing defendants, imposing liability in the amount of $5.89 million on all defendants jointly and severally. *Id.* at 131, 139. Among its findings, the court explained that defendants had "willfully violated the court's discovery orders," by among other things, "failing to turn over records," "lying to the court about the inability to obtain documents from third parties," and "destroying and withholding documents that were within the scope of the court's discovery orders." *Id.* at 143. The default judgment order incorporated the court's two prior discovery orders, including an order for Global to pay plaintiff's fees and costs in connection with litigating the contempt motion. *Id.* at 128, 131.

The decision in *SNET* is noteworthy . . . because it upheld the rare and extreme sanction of a default judgment against parties who intentionally spoliated electronically stored information.

Second Circuit Affirms Default Judgment

The Second Circuit reviewed the district court's imposition of the default judgment under an abuse-of-discretion standard. The court cited Federal Rule of Civil Procedure 37, which provides that:

> If a party or a party's officer, director, or managing agent . . . fails to obey an order to provide or permit discovery, . . . the court where the action is pending may issue further just orders. They may include the following: . . . (vi) rendering a default judgment against the disobedient party . . . .

Id. at 143 (citing Fed. R. Civ. P. 37(b)(2)(A)). The Second Circuit used four factors to analyze whether the imposition of the default judgment pursuant to Rule 37 was a proper exercise of the district court's discretion.

First, it noted that Global acted willfully and in bad faith. *Id.* at 147. The record showed that the deletion of electronic documents was intentional rather than merely negligent. *Id.* at 147-148. That the president of Select & Pay was not an employee of Global was not viewed as a defense because the evidence indicated that she had "acted on the defendants' behalf." *Id.* at 148 n.10. Second, Global's conduct was not isolated, but rather was part of a "prolonged and vexatious obstruction of discovery with respect to . . . highly relevant records. . . ." *Id.* at 148 (citation omitted). Third, a lesser sanction was deemed to be ineffective at achieving compliance, as Global had already been sanctioned for failing to comply with earlier discovery orders. *Id.* Finally, Global was on prior notice that noncompliance could result in a default judgment, as the district court had warned Global that failure to produce documents could have such a result. *Id.*

Conclusion

While district courts throughout the Second Circuit have produced an abundance of opinions on a wide variety of electronic discovery matters, the Court of Appeals for the Second Circuit has not often weighed in. The decision in *SNET* is noteworthy in that regard, and also because it upheld the rare and extreme sanction of a default judgment against parties who intentionally spoliated electronically stored information. Although the misconduct described in *SNET* is extreme, the outcome of the case suggests that other harsh discovery sanctions imposed by courts in circumstances involving bad faith might also be upheld if tested on appeal. ■

Court Updates: New York State Supreme Court, Civil & Commercial Divisions

In our August 2010 Electronic Discovery *Update*, we highlighted a report by the New York State Unified Court System (hereinafter, the "Report"), released in February 2010 by Chief Judge Jonathan Lippman and Chief Administrative Judge Ann Pfau. *See* New York State Unified Court System, *Electronic Discovery in the New York State Courts* (February 2010), *available* at http://www.courts.state.ny.us/courts/comdiv/PDFs/E-DiscoveryReport.pdf. The Report aimed to reduce the costs and amount of time spent on e-discovery by proposing several ways to make the process less expensive and more efficient for both the courts and practitioners.

Late last year, the New York Uniform Rules for the Trial Courts were amended to adopt one of the Report's recommendations for addressing the e-discovery process at the Preliminary Conference (the "PC"). There are two key enactments. First, Uniform Rule 202.12(b) and Uniform Rule 202.70(g) (Commercial Division Rule 1) now require lawyers appearing at the PC to be prepared to address e-discovery issues. Specifically, counsel appearing at the PC must be

> . . . sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery.

22 NYCRR § 202.12(b); 22 NYCRR § 202.70(g)(1). The changes to Commercial Division Rule 1 are meant to be consistent with Commercial Division Rule 8(b), which already codifies similar requirements. Rule 8(b) additionally provides that counsel confer with each other prior to the PC regarding nine enumerated e-discovery issues. *See* 22 NYCRR § 202.70(g)(8)(b).

These additions are intended to improve attorneys' abilities to engage in a productive conversation about the e-discovery process. They reflect the Report's findings that e-discovery disputes are best addressed at the outset of a case, with the oversight and involvement of the court. The Report proffers that the changes will prevent future delays and the waste of limited court resources that occur when attorneys do not consider e-discovery issues in advance of the PC.

Second, as recommended by the Report, the new rules provide that "[c]ounsel may bring a client representative or outside expert to assist" in the e-discovery discussion. 22 NYCRR § 202.12(b); 22 NYCRR § 202.70(g)(1). The purpose of this addition is to expand options for resolving e-discovery issues at an early stage. The Report notes that participation of client representatives (such as IT personnel) or outside experts at the PC may lead to quicker resolution of e-discovery issues because these individuals often have in-depth knowledge about the technicalities involved in retrieving electronically-stored information. An attorney choosing this option should make sure that his or her client representative or outside expert is thoroughly prepared for the hearing in order to provide an accurate representation of the client's abilities to retrieve and produce electronic data in a manner that will be usable for litigation purposes.

The Report proffers that the changes will prevent future delays and the waste of limited court resources that occur when attorneys do not consider e-discovery issues in advance of the PC.

Practitioners must be aware of these two important changes, as they greatly increase and magnify an attorney's obligation to focus on e-discovery from the outset of a litigation. Judge Pfau has warned that failure to comply with the new rules may result in a default (a consequence set out in Commercial Division Rule 1). The full text of the amendments can be found at http://www.dos.state.ny.us/info/register/2010/aug18/pdfs/courtnotices.pdf. ■

Court Updates: Delaware Chancery Court

This past January, the Delaware Chancery Court issued guidelines, predicated on standards of "reasonableness" and "good-faith," for the preservation of electronically stored information ("ESI"). The purpose of the guidelines, as stated by the Court, is "to remind all counsel appearing . . . before this Court of their common law duty to their clients and the Court with respect to the preservation of [ESI] in litigation." Court of Chancery Guidelines for Preservation of Electronically Stored Information, *available* at http://courts.delaware.gov/forms/download.aspx?id=50988 (the "Guidelines"). The Guidelines stress counsel's need to affirmatively address preservation issues, as preservation problems are often difficult to remedy after the fact.

Preservation Guidelines

The Guidelines indicate that the Court will evaluate the adequacy of preservation processes on a case-by-case basis. Notwithstanding the individualized nature of the Court's analysis, parties and their counsel are advised of certain minimum requirements to develop and oversee a preservation process that entails the dissemination of litigation hold notices to custodians of potentially relevant ESI. Failure by parties and counsel to take reasonable steps to preserve ESI may result in serious court sanctions. Counsel are reminded that the duty to preserve is triggered not when litigation commences, but rather when it is "reasonably anticipated." And, finally, reasonable and good-faith preservation efforts by parties and their counsel, although not dispositive, will be taken into consideration in cases where potentially relevant ESI is lost or destroyed.

Opt-Out Option

Although intended to caution litigants of the potential consequences for the failure to preserve ESI, the Guidelines include a safe-harbor provision for cases where the production of ESI is not warranted, for example, in a litigation where the amount at stake is relatively modest. They provide that parties may agree "to limit or forgo" discovery of ESI. Such a determination is best made at the outset of a litigation, consistent with the Guidelines' suggestion that parties confer regarding ESI preservation and production timing and methodology at the outset of a matter.

E-Discovery Guidance from the Bench

Even before the Guidelines were published, one Delaware Chancery Judge made a record of his increased expectations in the e-discovery realm. Vice Chancellor Laster of the Delaware Chancery Court garnered attention for his ruling in an April 8, 2010 teleconference concerning a discovery dispute. Transcript of Telephone Conference, *Roffe v. Eagle Rock Energy, Gp, L.P.*, C.A. No. 5258-VCL (Del. Ch. April 8, 2010), ECF No. 67. During the conference, the Vice Chancellor admonished counsel not to rely on a client to search its own email system, ruling that counsel must be physically present during the collection of ESI from his or her client. See *Id.* at 10. A client-generated search, the Vice Chancellor feared, could result in a collection that is too limited. He cautioned that counsel's use of "lackadaisical" discovery practices, such as relying on an in-house search of ESI, could lead the Court to reject proposed settlements outright. *Id.* at 9-10.

The Guidelines stress counsel's need to affirmatively address preservation issues, as preservation problems are often difficult to remedy after the fact.

Conclusion

As Vice Chancellor Laster's admonitions and the Guidelines demonstrate, litigants in the Delaware Chancery Court should take reasonable and precautionary measures to ensure the complete preservation and thorough discovery of potentially relevant ESI. Although the Court has yet to propose rules regarding the preservation of ESI, it should not come as a surprise if the Guidelines are codified in the future. Furthermore, given the Court's activist stance on e-discovery, it certainly is possible that guidance on matters beyond preservation of ESI also may be forthcoming. ■

Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Phone: 212.715.9100
Fax: 212.715.8000

47, avenue Hoche
75008 Paris
Phone: (33-1) 44 09 46 00
Fax: (33-1) 44 09 46 01

www.kramerlevin.com

Introducing Kramer Levin's E-Discovery Counsel, Brendan M. Schulman *continued from page 11*

failure or an IT department that acts on its own, a resulting data loss may still trigger sanctions.

Q: What are some ways to address clients' cost concerns with regard to producing and reviewing the massive amounts of potentially relevant ESI located in corporations today?

Schulman: One of the best ways to address the cost issue is to encourage clients to focus on electronic discovery issues early in the case. That can be challenging because for decades parties didn't really to focus on discovery until after the defendant lost its motion to dismiss.

The wait-and-see approach doesn't work any more. Now, the federal rules require early conferencing on e-discovery matters, and there can be tremendous strategic advantages in how one handles that early opportunity. For example, learning early on, by conferring with a client's IT personnel, that email received before a certain date is located on a legacy system and will be very expensive to collect and process can help the attorneys guide the proposed cutoff dates during discovery negotiations with an adversary.

Similarly, using advanced software tools to get a quick handle on the most relevant documents can be very helpful at deciding whether to pursue a quick settlement, or to dig in for a battle and ultimate victory. Those are insights that were never possible before, in a world where thousands of paper documents had to be reviewed manually before any conclusions could be drawn about the strength of the case. Having sophisticated e-discovery advice at an early stage can make a tremendous difference in both the cost of dealing with the case and even the outcome.

Q: E-Discovery is often viewed as a "necessary evil." What are some of the new developments in the field that have you excited?

Schulman: Computer technology once promised us a "paperless office." That obviously hasn't happened, and instead technology has brought us huge volumes of electronic data that are expensive to deal with in discovery. This can be very frustrating to a client who wants an efficient substantive resolution of the dispute. However, over the past couple of years I have seen the emergence of increasingly sophisticated software that promises to help. These software tools are designed to focus and prioritize a document review project, to use what's known as "predictive coding" to pre-sort documents into relevant categories, to find near-duplicates that can all be treated in a similar fashion, to assist in the negotiation of effective keywords, to automatically generate concepts and "topics," to gather relevant conversation threads, and to provide other strategic insights into an electronic document collection.

These tools are unquestionably powerful when used to conduct internal investigations, pre-discovery case analysis, and the review of large document sets produced by adverse parties. They are increasingly being used by parties to streamline their document review process as well. So, a challenge that has been created by technology now looks like it may one day be solved — or at least greatly ameliorated — by technology. I am excited to be moving to the point where electronic discovery is something we do strategically, to win cases or settle on favorable terms, rather than just being a burdensome and expensive stage of the litigation process. ■

For their contributions to this issue of the Electronic Discovery *Update*, we recognize and thank Kramer Levin associates **Clinton N. Daggan, Nicole S. Eisenman, Matthew B. Moses, Lisa Neunder** and **Lynda M. Tricarico.**