Best Practices for E-Discovery

Making E-Discovery the New Deal

How a New Problem Became a New Challenge

By Andy Moore, Editorial Director, *KMWorld* Specialty Publishing Group

There's no way around it: Legal e-discovery is a 21st century, first-world problem. I'm pretty sure there's no one in a village in sub-Saharan Africa wondering if they are adequately protected from civil litigation. It's only a reality in today's multi-faceted, multinational and multi-problematic business world.

Which is still a pretty big deal.

Just to get started, I'll add a little "dictionary." It will come as no surprise that I stole this from the net:

"The processes and technologies around e-discovery are often complex because of the sheer volume of electronic data produced and stored. Additionally, unlike hardcopy evidence, electronic documents are more dynamic and often contain metadata such as time-date stamps, author and recipient information, and file properties. Preserving the original content and metadata for electronically stored information is required in order to eliminate claims of spoliation or tampering with evidence later in the litigation.

"After data is identified by the parties on both sides of a matter, potentially relevant documents (including both electronic and hard-copy materials) are placed under a legal hold—meaning they cannot be modified, deleted, erased or otherwise destroyed. Potentially relevant data is collected and then extracted, indexed and placed into a database."

Basically, what that means is that electronically stored information is raw meat, but it has to be *agreed upon ahead of time* raw meat. So choose your storage strategies wisely.

The other thing about e-discovery is that it is usually preceded by an information governance strategy. Here's how Gartner puts it: "Information governance (IG) is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival, and deletion of information. It includes the processes, roles, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals. As compared to e-discovery, information governance as a discipline is rather new. Yet there is traction for convergence. E-discovery—as a multi-billion dollar industry—is rapidly evolving, ready to embrace optimized solutions that strengthen cybersecurity (for cloud computing). Since the early 2000s e-discovery practitioners have developed skills and techniques that can be applied to information governance. Organizations can apply the lessons learned from e-discovery to accelerate their path forward to a sophisticated information governance framework."

The thing (maybe things) about e-discovery that complicates the water are: (a.) it's still relatively new; (b.) it's totally foreign to all but the chosen few in the legal counsel's office; and (c.) it's really hard to do. The new rules (I still call then "new" because very few people understand there have been massive rule changes) call for a complete reorder of the civil litigation process. And the processes under which businesses now operate—mobile workforces, BYOD, cloud—stir up more silt to make the navigation more treacherous than ever. OK. Enough with the sailing analogies. But it's apt: E-discovery has become a major check-list item on every corporation's to-do list. And the sailing is heady indeed.

We often talk about how knowledge work is a combination of "people, process and things." That pretty much covers the waterfront. (Oh, sorry, I promised no more sailing references.)

But just ask Accusoft. They write in this paper about the "people" part quite eloquently (if not a little aggressively). They say, "Go full or go home. Research shows that when users can't perform every required task of their workflow within the designated application, they start working around the application. They begin performing some tasks on hardcopy or through email attachments, or engage in oral discussions that really should be documented within the workflow." Those dastardly water-cooler talkers. "They begin losing track of document versions and the discussion flow, on top of exposing sensitive legal documents to greater risk or theft or misuse."

There's a lot of truth in that. Workers who have become accustomed to firing off emails and tweets and insta-whatevers are probably more likely to rely on social tools to do their work than the age-old "document" relics that linger still in corporate information repositories. But listen to this: "The 'petrification' of legal documents to TIFF format for discovery review was aptly named—the practice is officially a fossil. Effective review demands access to documents in their native file formats, but the viewer technology in many applications still constrains the user to a short list of supported file formats." Meaning, one has to assume, that embedded technologies are a hindrance to current work, and cause more harm than good. "Reviewers wind up having to convert files just to review them, wasting costly time and potentially reducing the document's discovery value in the process."

They also point out these as guidelines to creating an effective knowledge-sharing base:

- **Mobile device support that's non-responsive…or nonexistent.** When reviewers can perform review tasks at client sites, the courthouse, or wherever else they may find themselves, they're more productive. But not just any mobile support gets the job done. Unless the viewer responsively adapts both the document display and the review toolset to optimize the experience for the device size, users may decide that trying to review on their phones and tablets is more hassle than it's worth.
- **Insufficient document safeguards.** The downside of mobile access is that it exposes documents to greater risk of misuse. Documents must be encrypted both on the server and in transit to devices, and administrators should have the option to

Andy Moore

Andy Moore is the publisher of KMWorld Magazine. In addition, as the editorial director of the KMWorld Specialty Publishing Group, Andy Moore oversees the content of the monthly "KMWorld Best Practices White Paper series," in print and online, as well as assisting with the creation and content of several single-sponsored "positioning papers" per year. He is also the host and moderator of the popular KMWorld Web event online broadcast series.

Moore is based in Camden, Maine, and can be reached at andy_moore@kmworld.com

"Electronically stored information is raw meat, but it has to be* agreed upon ahead of time *raw meat."

stamp a watermark on every page. But more importantly, documents must be displayed in a way that does not require that an actual copy of the source document be sent through the Internet.

Nexidia, also represented in this paper, addresses the "people" part of the equation in a unique way, I thought. There is no question that those "water cooler" denizens play an important role in the dispersal of information in a (typically small) organization. But, as we've noted, globally diverse, time-zone handicapped, sometimes language-barriered organizations can have a challenge meeting that fundamental need. Nexidia thinks it's a challenge more than an obstacle: "Financial institutions and other firms subject to heightened oversight are wise to implement rigorous systems to ensure the compliance and legality of all employee activities. While much of the employee activity is conducted digitally—through emails, trading systems and even personal solutions such as texting—there is still a great deal of activity that occurs through our oldest and most traditional form of communication: the human voice."

Pretty dramatic stuff. But they go on to sharpen the e-discovery edge: "Voice traffic can take many forms, from individual calls made between traders, to 'party line-style' talks on a turret system that connects people to the trading floor, and voicemails which are increasingly being sent and stored as email attachments in a unified messaging system." Here's the important part: **"All of these communications are part of the electronic record of a company's activity, and they are subject to the same review and discovery as any other evidence.** In fact, the 2006 changes to the Federal Rules of Civil Procedure even spelled this out in Rule 34(a), which specifically noted "sound recordings" as a type of electronically stored information (ESI). It is in the review and analysis phases of the EDRM that the differences between voice and textual electronic data really arise. While there have been technical methods for searching electronic text for decades, reliable methods for doing this with voice are relatively new. These technologies do exist today, and they must be considered a vital part of any company's voice compliance system." How'd you like to reveal your employees' telephone calls in a court of law? And I don't mean, the "hey, let's get lunch at Izzy Kadetz's today"-type of conversation… although that kind of noise and inconsequential banter can overburden the best management system. (BTW, if you're ever in Cincinnati, go to Izzy Kadetz for a reuben with slaw and russian dressing and a latke. You will thank me.)

On Being Proactive

You hear this a lot in e-discovery circles (and yes, there are some of those. I have picked up on e-discovery as sort of a hobby, thanks to great mentors such as Jan Scholtes at ZyLab): There's a movement afoot to create an active "activity" within organizations to prepare for litigation in advance. It's pretty much a foregone conclusion that preparation is better than reaction. But it's all too common that organizations wait until they're stung before they swat. In Sherpa's article, they point this out:

"E-discovery search and collection is part of a larger information governance effort. Ideally, policy and process should be in place long before litigation strikes; the more litigious a company, the more important it becomes to establish and document overall policy—especially rules for retention and defensible deletion. Another crucial step is to build a team with stakeholders who can collaborate on strategies for preservation, litigation hold and collection. To avoid last-minute scrambles, keep data maps and system inventory updated. Lastly, the right resources, software, vendors and personnel should already be identified and functional."

Sounds like sound advice to me. But they go on: "You cannot search or collect ESI that is not there. Deletion and wiping activities are often scrutinized by the courts in an adverse manner, which could negatively impact your case. Well-documented policies should be in place to outline how both automated and manual deletion will be disabled in the event of litigation. The policy and the applications that support it should be flexible enough to issue legal holds as well as halt deletion based on custodian, data store, date range or all the above. Verifying and assessing of all these steps is central to defensibility.

"Knowledge and planning reduces pain and disruption in the initial stages of e-discovery. Be organized in your approach, and have the correct resources and tools in place while working together with a well-chosen team to create policies specific to your organization. Being proactive and thorough during collections will lead not only to savings, but also will provide peace of mind."

Peace of mind. How cool is that? I'm writing this a few days before Christmas, and the idea of "peace" is an especially meaningful concept right now. There is no doubt that the fear and avoidance of litigation is a painful challenge for corporations. And it's getting worse.

So being prepared for e-discovery is the key to solving the difficult and sometimes business-ending result. So preparation, planning and (yes) having some technology in place ahead of time is key to solving the threat of litigation. It will come, make no doubt. The only question is how well prepared you will be. FTI provides an interesting graphic in these pages that sort of charts out how the e-discovery path takes place in real-life. Follow that graphic to see what steps are necessary to get from the batting cage to home base. It always helps to follow a map. I recommend it.

On the following pages, you will also learn several methods and means to create an e-discovery foundation, and also how to begin a strategy to create a successful e-discovery outcome.

Yes, it does seem like a first-world problem. But make no mistake: Being prepared for civil (and criminal) litigation is a key part of the current operating procedure for any company today. And, besides that, it's more than a "big company" issue. ANY organization is exposed to a variety of threats, from contract negotiations to internal HR and policy issues. So don't think "it won't happen to me." Because it probably will. These solutions partners—Sherpa, Nexidia, Accusoft and FTI—can help you prepare for the worst and best outcomes. ▮

Eliminating Barriers to Full-Workflow E-Discovery

By Ned Averill-Snell, Product Specialist, Accusoft

Predictive coding shows us where e-discovery technology wishes it could go: total automation. Encode a complete legal mind into a software program, load up the discovery portfolio, count to 10, and out pop coded, annotated, redacted production files.

It's a seductive concept, but such technology is a very long way off, and its broad acceptance by courts—which have yet to really say yea or nay even on predictive coding—is farther away still.

In the meantime, legal document workflows will require expert reviewers. And given the state of most current legal technology, those reviewers rarely get the tools and support they require to perform their full-workflow function thoroughly, accurately and efficiently.

Go Full or Go Home

Research shows that when users can't perform every required task of their workflow within the designated application, they start working around the application. They begin performing some tasks on hardcopy or through email attachments, or engage in oral discussions that really should be documented within the workflow.

And then they begin losing track of document versions and the discussion flow, on top of exposing sensitive legal documents to greater risk or theft or misuse.

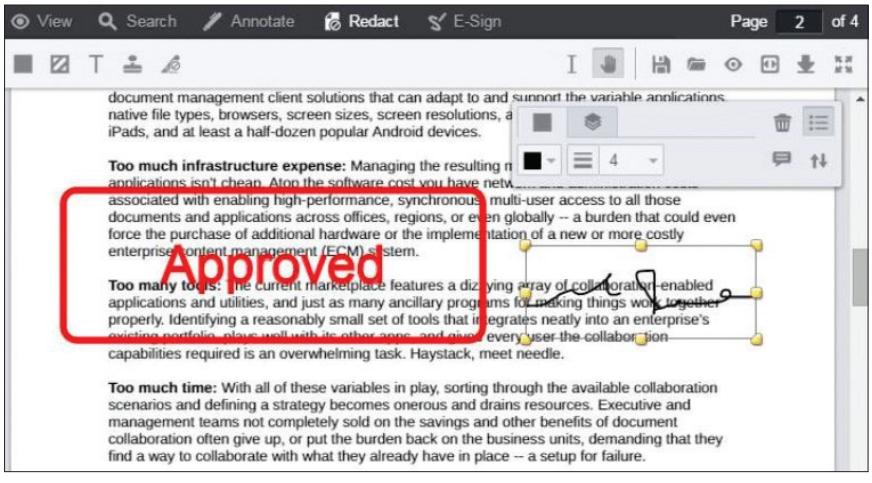
Given the current state of most legal document review technology, reviewers often run up against the following obstructions that may send them running outside their applications:

- **Limited support for native file formats.** "Petrification" of legal documents to TIFF format for discovery review was aptly named—the practice is officially a fossil. Effective review demands access to documents in their native file formats, but the viewer technology in many applications still constrains the user to a short list of supported file formats. Reviewers wind up having to convert files just to review them, wasting costly time and potentially reducing the document's discovery value in the process.
- **Mobile device support that's nonresponsive…or nonexistent.** When reviewers can perform review tasks at client sites, the courthouse, or wherever else they may find themselves, they're more productive. But not just any mobile support gets the job done. Unless the viewer responsively adapts both the document display and the review toolset to optimize the experience for the device size, users may decide that trying to review on their phones and tablets is more hassle than it's worth.
- **Insufficient document safeguards.** The downside of mobile access is that it exposes documents to greater risk of misuse. Documents must be encrypted both on the server and in transit to devices, and administrators should have the option to stamp a watermark on every page. But more importantly, documents must be displayed in a way that does not require that an actual copy of the source document be sent through the Internet. HTML5 viewing technology can reduce the risk by transmitting only a high-fidelity copy that's useful to the reviewer but useless to anyone who might try to steal it.
- **Skimpy annotation toolsets.** Careful document review is a multiuser process, a conversation. At base, legal reviewers need to be able to insert comments in a document. But for the level of engagement a full review demands, they also need to insert comments in comments, to include comment text in searches, and to customize annotation types to match the unique needs of their firm, company or case.
- **Primitive redaction capabilities.** The essential ability to black out nonresponsive and nonrelevant content is the beginning of a useful redaction function, not its end. Reviewers also need to be able to embed a reason in a redaction, and to include redaction reasons in simple and complex searches.
- **No approval/signature functionality.** The review workflow isn't complete until approval, so full-workflow legal review must include a way to sign documents electronically.

Look to the Viewer

Ensuring that legal review technology addresses the full workflow lies mostly in the application's viewing component. It's the platform and enabler for the search, annotation and redaction tools. But more importantly, the viewer component defines the architecture that enables superior security protections and mobile responsiveness.

Developers of legal software are finding that HTML5 document viewing technology supplies a secure, adaptable platform for the full range of document review tools that can keep legal staff productive within applications that meet their full-workflow requirements. ▮



Annotations and signatures are among the tools reviewers require for full-workflow legal document review.

Ned Averill-Snell is an award-winning computer journalist and author. A former contributing editor to *Datamation* magazine, he is the author of "Sams Teach Yourself to Create Web Pages in 24 Hours," among other titles. He works at Accusoft.

Visualization: The New E-Discovery Paradigm

By JR Jenkins, Senior Director, FTI Technology

1. Before the "e" was in e-discovery, legal teams manually separated and clustered relevant documents together to understand the relevant facts.

2. A lot has changed since then. We've moved to online software that provides functionality to do the e-discovery process faster, but not necessarily better.

3. At the end of the day, you're still going through the whole e-discovery process before you find the important materials and understand the key concepts within the matter.

4. But, there is a better way to do e-discovery. Analytics tools enable you to visualize and summarize data. They can present multiple data points and enable you to drill down into important data.

5. You can also find key facts earlier in the process. This can help you reduce the amount of data to collect, process and review. Overall, this leads to a dramatic reduction in your e-discovery costs.

6. However, reducing cost isn't the only advantage. You will better understand the strengths and weaknesses of your case and be more effective at developing case strategy.

To learn more about how you can use analytics to find important case facts, please visit www.ftitechnology.com.

Be Reasonable, Be Knowledgeable

The Foundation for Effective E-discovery Preservation, Search and Collections

By Marta Farensbach, Director of Product Services, Sherpa Software

E-discovery advice is prevalent throughout legal, information management and technology publications, including varying opinions about the methods in which to diligently preserve and collect electronically stored information (ESI). Common themes focus on finding relevant ESI by understanding how your organization uses its information, locations where data resides, as well as knowing the scope of the collections for specific litigations. This guidance, coupled with the court's requirements, drives the desired outcome of using reasonable and repeatable processes, cost-effective methods and legally defensible practices. To best achieve these goals, consider the following recommended practices:

Be proactive.

E-discovery search and collections is part of a larger information governance effort. Ideally, policy and process should be in place long before litigation strikes; the more litigious a company, the more important it becomes to establish and document overall policy—especially rules for retention and defensible deletion. Another crucial step is to build a team with stakeholders who can collaborate on strategies for preservation, litigation hold and collections. To avoid last-minute scrambles, keep data maps and system inventory updated. Lastly, the right resources, software, vendors and personnel should already be identified and functional.

Collaborate.

The formation of an efficient e-discovery team is essential for collections to work effectively. Members should fill key roles needed to create and implement policy. To that end, the team should be pulled from legal, IT and business units with other departments like compliance, HR or records management supporting overall efforts and being consulted as necessary. In addition to proactive planning, this team should assemble when any legal proceedings can be reasonably expected. It is essential that the members pre-define areas of ESI that are not reasonably accessible (e.g. legacy systems). Once litigation is anticipated, the team should focus on one or more of the following:

- Defining the scope of the matter and information-gathering requirements;
- Initiating and managing legal hold notifications and acknowledgment;
- Implementing preservation and collections processes;
- Addressing outliers such as encrypted files or corrupt data stores; and
- Managing a defensible process.

Communication between team members is critical to keep the collections process running smoothly. To assist this effort, an e-discovery liaison should be appointed. This key resource should work with IT to guide the process, establish parameters and navigate challenges. The liaison should be able to answer questions, work to safeguard defensibility, inform 26(f) meet-and-confer conferences and ensure that collections address other legal and technical concerns.

Preserve data.

You cannot search or collect ESI that is not there. Deletion and wiping activities are often scrutinized by the courts in an adverse manner, which could negatively impact your case. Well-documented policies should be in place to outline how both automated and manual deletion will be disabled in the event of litigation. The policy and the applications that support it should be flexible enough to issue legal holds as well as halt deletion based on custodian, data store, date range or all the above. Verifying and assessing of all these steps is central to defensibility.

Deploy targeted collections.

Document review remains as the largest cost associated with e-discovery and is directly related to the volume of ESI collected; therefore, there is a direct correlation between targeted data collections capabilities and front-end culling capabilities. From the outset, the scope needs to be well-defined by the e-discovery team. This includes:

- Identifying and prioritizing key custodians;
- Pinpointing pertinent ESI storage locations;
- Choosing automated solutions and deciding on methodology;
- Defining the parameters of the search including dates, keywords, file types;
- Clarifying delivery formats for structured and unstructured data; and
- Establishing what is "reasonably accessible" as related to the proportionality of the specific case.

Avoid common mishaps.

Mistakes during the collections phase can cause havoc for a case. Here are a few to avoid:

- ***Modification of metadata.*** Without the correct tools and processes, it is surprisingly easy to change file properties. For example, using Windows Explorer to copy files to a new location can change creation and access dates. Opening documents in native applications can also change "last accessed by," and in some programs, may affect "modified by" properties.
- ***Failing to document methodology.*** Defensibility is one of the main considerations in e-discovery collections. Missing collections inventories and logs can weaken a case. Additionally, some collections are performed using native applications. Care is needed here because some of these programs (e.g. Microsoft Outlook) can alter metadata and are not optimized for establishing a chain of custody or consistently reproducing results.

Using custodian self collections. A common, but highly unreliable, method of collections is to have custodians collect their own data. This is often a recipe for disaster because of the lack of audit trail, inconsistent searching and potential conflict of interest. Trained, impartial personnel should perform the collections, preferably with peer-reviewed and commercially available tools. This helps to avoid mistakes due to lack of knowledge of systems, scope or process.

Review the process.

The best way to avoid difficulties and withstand legal scrutiny is to include a repeatable assessment process as part your collections methodology. This includes several fundamental steps:

- Document the steps that were performed;
- Test software to make sure you can consistently reproduce results;
- Review and validate your preservation workflow;
- Outline the quality control process as part of the initial plan of action;
- Conduct pilot collections on a small set of potential custodians before performing the overall collections effort; and
- Implement and monitor the litigation hold efforts to ensure enforcement.

Knowledge and planning reduces pain and disruption in the initial stages of e-discovery. Be organized in your approach, and have the correct resources and tools in place while working together with a well-chosen team to create policies specific to your organization. Being proactive and thorough during collections will lead not only to savings, but also will provide peace of mind. ▮

Haven't You Heard?

Managing Voice Data is Critical to Corporate Compliance

By Jeff Schlueter, VP/GM of Legal Markets, Nexidia

The headlines capture your attention: "$4 Billion Settlement Reached for FOREX Manipulation!" In November, 2014, six of the largest international financial institutions agreed to more than $4 billion in settlements with both US and UK regulators regarding improper trading activities in the foreign exchange market. According to the *Wall Street Journal*, the regulators cited the banks for "inadequately supervising their traders and other employees and lacking sufficient controls to prevent them from engaging in allegedly improper behavior." (WSJ, Nov. 12, 2014.)

The FOREX scandal is just the latest in a recent stretch that includes investigations into LIBOR trading, credit default swaps and many other activities that regulators have been cracking down on since the financial collapse of 2008. There is now a much higher degree of oversight and activity among regulators such as the CFTC, SEC and United States DOJ, as well as the creation of a whole new agency, the Financial Conduct Authority (FCA) in the UK. In fact, eight months after the passage of the US Dodd-Frank Act in 2010, the CFTC had conducted 93 investigations with 45 settlements totaling more than $155 million in penalties and disgorgement of unjust profits.

In this environment, financial institutions and other firms subject to this heightened oversight are wise to implement rigorous systems to ensure the compliance and legality of all employee activities. While much of the employee activity is conducted digitally—through emails, trading systems and even personal solutions such as texting—there is still a great deal of activity that occurs through our oldest and most traditional form of communication: the human voice.

Voice traffic can take many forms, from individual calls made between traders, to "party line-style" talks on a turret system that connects people to the trading floor, and voicemails which are increasingly being sent and stored as email attachments in a unified messaging system. All of these communications are part of the electronic record of a company's activity, and they are subject to the same review and discovery as any other evidence. In fact, the 2006 changes to the Federal Rules of Civil Procedure even spelled this out in Rule 34(a), which specifically noted "sound recordings" as a type of electronically stored information (ESI).

General counsel and compliance officers need to factor voice traffic into their information management program to provide compliance and to be ready to answer regulatory investigations in a timely manner. However, when compared to email and other electronic forms of communication, voice activity is generally managed by different systems and different people in an organization, and voice data has a unique set of attributes that make it potentially more challenging to manage than regular electronic data.

Components of a Successful Voice Compliance Solution

Using the Electronic Discovery Reference Model (EDRM) as a guide, the preservation and collections of voice data is the first issue companies must address. Many institutions already have call recording or "logging" systems in place, and these loggers capture not only the call but any metadata about the call, including the data/time, agent or custodian, calling party ID or customer number, etc. Still, companies must be diligent with their call recording vendors to be certain the system permits rapid access to their calls, and that they are not restricted by proprietary database or encryption schemes that prevent them from exporting and analyzing calls in a timely manner.

It is in the review and analysis phases of the EDRM that the differences between voice and textual electronic data really arise. While there have been technical methods for searching electronic text for decades, reliable methods for doing this with voice are relatively new. These technologies do exist today, and they must be considered a vital part of any company's voice compliance system.

The most important aspect of voice compliance technology is accuracy; in other words, does the system index the content and allow systematic or ad-hoc review so that companies can accurately track and monitor what's being spoken? As a search medium, audio is traditionally more difficult to search than text; it is subject to accents, quality issues like background noise and file compression, and other variables that can make the same words sound very different when spoken. A voice review system that uses phonetic indexing and search—in which the audio is broken down into its component parts, or phonemes—has shown to be the best method for accurately searching large amounts of unstructured audio. This is the system that has been adopted by all the major regulators including the CFTC, SEC, CFPB and DOJ.

Also critical is a system that can economically analyze compliance across 100% of a company's voice content. In this day of heightened regulatory oversight and heavy penalties, companies must be able to analyze every single voice data record they produce. Measuring a small sample is no longer sufficient to satisfy regulatory demands for proper behavior. Here again, a phonetic indexing and search approach has proven to handle even the largest voice compliance projects, with some systems indexing nearly 100,000 hours of audio per day with just a few servers.

Finally, a voice review system cannot be an island; it must fit within a company's overall compliance monitoring function. Voice data must be analyzed in concert with emails, chats and other electronic records, to track the journey of these different employee interactions across the organization. The system must automatically discover potential violations across all these data sources, route suspected communications to the appropriate reviewers, and track the final disposition for each potential violation through the system.

With voice as a vital component of a total compliance monitoring solution, financial services and other companies can take a vital step toward ensuring that their employees' behavior stays within the guidelines established in this new age of regulatory oversight. And this, in turn, should help those companies stay out of the headlines. ▮

Jeff Schlueter is the VP/GM of legal markets for Nexidia. He is responsible for developing and executing the company's audio discovery solutions targeting law firms, corporate counsel and regulatory agencies.

For more information on the companies who contributed to this white paper, visit their websites or contact them directly:

Accusoft
4001 N. Riverside Drive
Tampa FL 33603

PH: 800.875.7009 or 813.875.7575
FAX: 813.875.7705
Contact: info@accusoft.com
Web: www.accusoft.com

FTI Consulting
925 Fourth Avenue, Suite 1700
Seattle WA 98104

PH: 1.866.454.9305
Contact: ftitechsales@fticonsulting.com
Web: www.ftitechnology.com

Nexidia
3565 Piedmont Road NE
Building Two, Suite 400

Atlanta, GA 30305
PH: 404.495.7220
FAX: 404.495.7221
Contact: info@nexidia.com
Web: www.nexidia.com

Sherpa Software
456 Washington Ave., Suite 2
Bridgeville PA 15017

PH: 412.206.0005
Fax: 412.206.0018
Contact: information@sherpasoftware.com
Web: www.sherpasoftware.com

Produced by:

KMWorld Magazine
Specialty Publishing Group

Kathryn Rogals
561-483-5190
kathy_rogals@kmworld.com

Andy Moore
207-236-8524 Ext. 309
andy_moore@kmworld.com

For information on participating in the next white paper in the "Best Practices" series, contact:
kathy_rogals@kmworld.com • 561-483-5190