METROPOLITAN
CORPORATE
COUNSEL®

VOLUME 24, NO.1 FEBRUARY 2016 WWW.METROCORPCOUNSEL.COM

MCC GUIDE TO IN-HOUSE TECH

Welcome to our first Guide to In-House Tech. We are delighted to present a suite of insightful pieces of special interest to corporate law departments on topics ranging from e-discovery consolidation and collaboration to data-breach incident response to analytic and workflow tools designed to enhance in-house efficiency – plus a directory of leading tech companies. We hope you find the "MCC Guide to In-House Tech" both useful and enlightening.

MCC INTERVIEW: Charlie Platt / iDiscovery Solutions

Data Breach & Incident Response

Assess the cybersecurity priorities keeping you up at night

Businesses are generating and storing great volumes of data using numerous platforms: desktops, laptops, servers, cloud servers, archiving appliances, external storage devices, websites and more. ***Charlie Platt*** *explains how* ***iDiscovery Solutions*** *advises clients from both the prevent and protect side as well as incident response. His remarks have been edited for length and style.*

MCC: Tremendous amounts of data are produced by businesses today, in a variety of forms from multiple sources. Employees are using personal devices and email, as well as other digital accounts, to communicate and store information. How can businesses assess their vulnerabilities and protect their data, whether at rest or in motion? How can they ensure that they can identify a data breach or network incident and do so quickly?

We need to stop thinking about security as a one-stop perimeter defense and start thinking on a more compartmentalized basis.

Platt: It's important to keep in mind that there is no one-size-fits-all solution to cybersecurity and that no solution can guarantee 100 percent effectiveness. With that in mind, some of the best ways to address the issue are non-technical in nature. For example, education, policies and culture can have a more significant impact on the security of your organization than a large purchase of software or hardware.

I'm not saying that technology is not part of the solution; it absolutely is. However, technology is just one part of a multifaceted solution and if we don't address the other facets, no amount of technology can account for the shortfall. Case in point, Target. Target, according to their own press release post-breach, had spent hundreds of millions on cyber defense, and yet it was a failure in policy and culture that ultimately led to the breach.

To be more specific to your question, before we can assess our vulnerabilities and develop defenses, we need to understand our systems and our data. What are we defending and why are we defending it? Are we putting as much effort into defending the office roster as we are confidential business information? Is our data properly segregated or is it all collocated, mingled and unmanaged? Does anyone with access to one piece have access to all pieces?

You'd be surprised by how many organizations set up private and secure network storage locations for employees, but the employees all use a common shared network location to which everyone has full access. They do this because it solves a business need, is cost effective and gets the job done quickly and efficiently. It's also exceptionally bad from a cybersecurity viewpoint. I've seen this at sites where unmanaged network shares hold data going back to the early 2000s and beyond. All staff have full access to all data. When employees leave, the data remains and accumulates over time. No one knows what is out there and what might be considered PII or confidential, or who is accessing what data. This is not really a technology problem, but rather an educational and cultural one. The trick is to make sure to address the business need at the same time we solve the security hole; otherwise it will just pop up somewhere else.

MCC: These days, the common wisdom seems to be that a data breach is inevitable – a matter of when, not whether. Some say protecting the perimeter is a strategy destined to fail. How can businesses best prepare themselves for when that day arrives? Who are the key players who should be involved in planning and responding to such an incident?

Platt: I've heard the argument that given enough time and persistence, an attack will be successful. While I tend to agree, I think that's only half the picture. What we are leaving unsaid is the level of success achieved by the attack. Simply because someone is successful in breaching the perimeter doesn't mean they are successful at breaching critical or sensitive information. We need to stop thinking about security as a one-stop perimeter defense and start thinking on a more compartmentalized basis.

This means we need to defend ourselves in a manner where a successful perimeter breach gives the attacker minimal access and presents them with a whole new defensive surface. In essence, once they've breached the first line, they are faced with having to repeat that success again and again before being able to access anything of importance. All of this secondary attack activity is occurring within our perimeter, which makes it easier for us to detect and address. It also allows us to apply higher levels of resources (budget, technology and staff) to defend critical areas.

Who are the key players? C-suite executives and the company's board. The board needs to address cybersecurity as a strategic priority and should have a cybersecurity committee devoted to the topic. The executive suite needs to embrace security and not sidestep it. Their demeanor will set the tone for the entire organization.

Once leadership is on board, the key players involved in drafting a response protocol should include IT, information security, inside and outside counsel, and the various business units. Outside consultants can also be of great assistance in developing a response plan, but the authority and the final responsibility needs to reside within the organization. This responsible party does not necessarily need to be an IT professional, but does need to have a vested interest in the security of the organization – with the authority and backing of senior leadership to make changes and implement policy.

IT and information security are fairly obvious needs. Inside and outside counsel are needed to provide guidance and understanding of compliance and regulatory needs, as well as help maintain privilege and confidentiality of sensitive conversations. What is often lacking, yet absolutely critical, are the business units. They need to be included in developing incident response plans because they are the ones who not only know the data, but understand its business importance. They are key to developing solutions that work and can realistically be implemented.

As a simple example: locking down USB ports so that thumb drives and autolaunch no longer operate might be a valid and appropriate solution to a cybersecurity problem. However, an organization might very well see a dramatic rise in use of cloud based storage, such as Dropbox and Google Drive, as a result of that action. So, we have just replaced one exposure with another exposure. If we had included the business units up front, we may have understood that private ad hoc file sharing between devices is a critical need and, along with our lockdown, provided a secure alternative to USB drives.

MCC: There is a great deal of talk about "incident response plans." How can businesses ensure that their team can develop and execute such plans when data is so voluminous and varied?

Platt: Like in many problems viewed as a whole, it can appear daunting and insurmountable. However, if we break it down into constituent parts and start addressing individual pieces, before we know it we've achieved our goals. A good start is to document and understand your IT systems. Then, create a risk map of those systems, asking questions about each: Does it contain PII? Does it transfer data in and out of the organization? Does it use encryption at rest? Is it business critical? Get a sense of where you need to act so you can target your approach to the highest need.

MCC: Are there any case studies you can point out to our readers that would illustrate best practices or lessons to learn from a data breach or network incident?

Platt: I'm not sold on case studies as much as a handful of industry documents that I rely on. First to mind is NIST's "Framework for Improving Critical Infrastructure Cybersecurity." This does a great job of pulling together many of the risk areas involved and provides, as the name implies, a coherent framework for developing cybersecurity policy and procedures. Second is NIST Special Publication 800-30, "Guide for Conducting Risk Assessments – Information Security."

These can be a bit dense for non-security professionals. A bit more accessible is Alien Vault's "Insider's Guide to Incident Response." It really provides a good overview for a non-security professional and acts as a great high-level guide for professionals.

Continued on following page

Charlie Platt
Senior managing consultant at iDiscovery Solutions.
cplatt@idiscoverysolutions.com

Let's Play Nice Together

4 benefits to getting on the same page for e-Discovery

By Nadine Weiskopf / AccessData

One of the more intriguing developments with the various changes in evidence rules and judicial expectations that impact e-Discovery is the steady evolution of professional responsibility codes pertaining to client/attorney collaboration. For example, outside counsel is increasingly expected to be knowledgeable about the technology used during e-Discovery, and to articulate to the court how e-Discovery was managed with the corporate client.

"Many discussions of the relationship between in-house law departments and outside counsel take as its unspoken assumption that it's a zero-sum game, where gains for one are losses for the other," said Bruce MacEwen, founder of the legal consulting firm Adam Smith, Esq., and an attorney who has practiced both in-house and at a law firm. "A much more realistic and more business-driven view is that it needs to be a collaboration. While the obvious shared goal is to 'solve legal problems,' the marketplace and client/advisor reality is more nuanced and should create a stronger intrinsic bond. Any law firm that doesn't care about getting closer to its clients, or any client who secretly wants to undermine its preferred law firms, has problems far larger than what's on the legal agenda."

Of course, this conversation is not new in our industry. As far back as 2008, Law360 reported that e-Discovery collaboration between in-house legal departments and outside counsel was improving – and yet we continue to see major cases of process failure that lead to spoliation and failure to preserve evidence sanctions. Why do litigation professionals instinctively understand the importance of properly managing data throughout the e-Discovery workflow and yet continue to struggle with the execution?

Nadine Weiskopf
Vice president of product management, forensic & e-discovery solutions at AccessData.
nweiskopf@accessdata.com

Perhaps one answer is the absence of a comprehensive e-Discovery review software platform on which all parties can collaborate. There are four key advantages to having your in-house legal department and outside law firm using the same e-Discovery review software platform while working on a case:

1. Less Data Movement

A single e-Discovery platform means you will have fewer "data hops" as documents enter the workflow and move across the EDRM continuum. Less data movement inherently reduces the potential for errors in investigation, collections, processing, review and production.

2. Decreased Risk

There is no way to eliminate human error in e-Discovery, but a single review platform significantly decreases the risk of sanctions for failure to preserve evidence, data spoliation and other serious considerations. This is a growing problem that many experts feel is bound to be more commonplace under the new federal electronic discovery rules.

3. Improved Collaboration

The best e-Discovery software tools will provide a real-time review platform that allows secure collaboration, regardless of where any member of the litigation team is located. An in-house/outside counsel team that is better able to work together on e-Discovery is going to be more efficient in their workflow, more accurate in their production and more responsive to each other throughout the process.

4. More Favorable Pricing

When in-house and outside counsel agree to work on a shared platform for e-Discovery, it creates obvious economies of scale. Some software vendors will even offer price breaks and incentives if a corporation wants to provide their outside counsel with a license of their review software to facilitate collaboration.

There is a wide range of reasons why it is important for in-house counsel and law firms to better collaborate during e-Discovery, ranging from the ominous court-ordered pressures and the strategic litigation management considerations, to the important business efficiency factors. One tool to support the effort to step up your collaboration is a single e-Discovery review software platform.

AccessData's AD eDiscovery® software product is an end-to-end platform for in-house legal departments that supports the entire e-Discovery workflow. For more information, please visit www.accessdata.com.

Incident Response

Continued from previous page

Another favorite is Verizon's annual "Data Breach Investigations Report." This contains a great overview of the current state and what is really occurring as it relates to industry and attacks.

MCC: How do businesses know when they should report a data breach or network incident to government enforcement officials? What are the protocols for such an incident?

Platt: One of the first items in your incident response plan should read, "Contact Outside Counsel." Outside counsel absolutely needs to be involved in incident response, both in planning and in execution.

The protocol can vary based on the organization and the type of data involved. Organizations need to clearly identify their data, understand the regulations and compliance to which they are subject and clearly spell out the relevant reporting requirements – including how they will comply in any given situation.

In many cases, we find that while data may have been exposed, there is no evidence of actual breach or access to the data. Various organizations choose to respond to that scenario differently. Some favor reporting with the sense that sharing information can benefit the overall community, while others feel that sharing when not required can damage their reputation and brand, or even encourage future attacks. The important thing is to make these decisions prior to the event, with a calm mind and advice from counsel, rather than trying to make a critical decision under the pressure and deadlines associated with reporting.

MCC: When you are working with clients, what keeps you up at night? What are the risk factors that may be off the radar for most businesses?

Platt: From a small business viewpoint, the two things that scare me the most today are Cryptoware and some of the new multi-pronged "whale" and "spear" phishing attacks.

What keeps me awake at night is a looming shift in focus. When we think about cybersecurity today, we generally think about either confidentiality or availability. Confidentiality: has someone had inappropriate access to read my private information? Availability: has someone been able to prevent me or my customers from accessing systems or data? From breaches of our private data (e.g. PII, HIPPA, CBI) to attacks designed to deny access (e.g. DDoS and Cryptoware), confidentiality and availability have been a core focus of cybersecurity in the recent past.

In the future, I see integrity moving to the forefront. The question will not be, 'Has someone seen my private health information?' but instead, 'Has someone altered my private health information?' As we become more and more reliant upon these systems as final authorities, we become much more vulnerable to alterations in that data – the subtler the alteration, the scarier. Consider the business data that you rely on daily to operate your business. Now consider that someone has had access to maliciously alter that data for the past month, the past quarter, the past year, and you've been relying on it to make critical business decisions. Would that keep you awake at night?

MCC INTERVIEW: The Williams Companies / Crowe & Dunlevy / Inventus, LLC

E-discovery Is About More Than the Tools

The project management team is the key to effective large-scale reviews

Energy corporation ***The Williams Companies****, its outside counsel* ***Crowe & Dunlevy*** *and discovery management firm* ***Inventus*** *form a productive trio in meeting the company's e-discovery needs. Representatives from each arm of the partnership –* ***Amy Sellars*** *of The Williams Companies,* ***Christopher B. Woods*** *of Crowe & Dunlevy, and Clint Williams and* ***Stephen Kennedy*** *of Inventus – share their successful tactics. Their remarks have been edited for length and style.*

The most important part is the project manager. Tools are tools. People think and are smart and are invested in the outcome.
–Amy Sellars

MCC: How long have your firms been working together and what are some of the key elements of your collaboration? Chris, do you want to start us off?

Woods: Crowe & Dunlevy and The Williams Companies have enjoyed a long relationship – as long as I have been at the firm, and that's more than 15 years. That type of a relationship benefits us as outside counsel in being able to learn a lot about the client – not only various aspects of their business, but also understanding how they approach matters. In the e-discovery context, it provides us an understanding of their systems and processes – not to the degree that Amy has, by any means, but a familiarity that is very useful. Our relationship with Inventus is a newer relationship. This is the first case on which I have worked with them.

Sellars: This is also the first time that The Williams Companies has worked with Inventus. The Crowe-Williams association does go back. In fact, I think that Crowe has been our e-discovery counsel on every major complex litigation involving large volumes of ESI. It's a pretty big history.

MCC: How do you manage one of these highly complex matters?

Woods: There are similarities that cut across all these matters, but each matter also stands on its own. When we receive a new case, we evaluate not only the substantive issues, but also the data that will be implicated, the number of custodians implicated, what types of systems and databases might be involved, and things of that nature. Each case is handled a little bit differently depending on those aspects and other factors, including the size of the matter and the anticipated schedule.

As Amy mentioned, Crowe has worked with Williams on quite a few cases with large volumes of ESI. But a "substantial amount of data" itself is variable and often requires different approaches. What we do from the beginning is take a look at those issues. We take a look at the key people involved, including their roles, duration of involvement and whether they are current or former employees. We look at what databases might be implicated. Williams has many different systems for different areas of its business. But one of the great things about our relationship with Williams, and having someone with Amy's expertise as a client, is that they've done a lot of work before they ever call us. They have a good handle on things.

Sellars: That's true, but I think Crowe really helps us refine the scope. One thing that I've loved about working with Crowe is that scope is a continual issue. It's not that we define the scope of the case based on the face of the complaint knowing we will never revisit it.

As with most companies, our goal is to retain as little as we are obligated to retain but still meet our obligations. Crowe has been very thoughtful in working with us on figuring out: Who are truly the key custodians? Who do we really need to collect from early? What are the date ranges? Are we pushing some things to the side for the moment with the idea that there is no real danger of spoliation, and if we have to get to it, we will? They are very helpful in helping us be as targeted as possible so that the ultimate cost of review is as low as possible. Sometimes you work with outside counsel who feel like you will start with the entire world and narrow down from there, rather than thinking about the case as it progresses and modifying your scope as you move through it.

MCC: Given all of that, how can a company go about developing a data retention strategy that makes sense?

Woods: What Amy said is the key. As with other aspects of any case, as you review documents and talk to witnesses, you learn more about the case. Some of that information bears on the e-discovery process and retention/preservation issues. Certainly, Williams does a wonderful job at the outset of talking to individuals, finding out who was involved, where the data is, and making sure it's preserved. But as you get deeper into the matter, you might find, for instance, that a certain person didn't really have a significant role in the case. After you've collected the data, you also are able to run analytics and conduct searches to evaluate custodians' involvement, date ranges and the like. You can talk to the witnesses to assess whether certain custodians can be released.

Likewise, as the case progresses, you may learn about people that you didn't anticipate. It's an evolving process, but always with the objective of making sure that we're not collecting and reviewing any more data than is necessary, because it is so costly and such a burden on the trial team to get through this additional material to prepare the case. Focusing on the key custodians and date ranges – making sure you have the right data – is the foundation for making sure that you're complying with your obligations and have what you need. You don't want more data than you need, as that bogs you down.

MCC: Talk about how you collaborate to develop strategies going into the e-discovery process and how your teams design your approach to project management. It sounds like, in this situation, we have three groups that work well together.

Sellars: It's a hard question to answer. It's like asking us to do improv comedy.

If the team understands what you're trying to achieve, they can help you know what you missed and what you have that you don't need and why, so you have a defensible trail of how you came to decisions in terms of scope.

Continued on following page

Amy Sellars
Senior litigation attorney at The Williams Companies. Also serves as the company's discovery subject-matter expert.
amy.sellars@williams.com

Christopher B. Woods
Shareholder and director in Crowe & Dunlevy's Tulsa office with substantial experience in large-scale e-discovery projects.
christopher.woods@crowedunlevy.com

Clint Williams
Managing shareholder of Inventus' Oklahoma City office.
cwilliams@inventus.com

Stephen Kennedy
Project Manager at Inventus, LLC.
skennedy@inventus.com

E-Discovery Is About More Than the Tools

Continued from previous page

Chris and I have had experiences where we look at each other with blank faces and then turn to the vendor and say, "If you have suggestions, can you help us?" We get equally blank faces, and that's part of the reason we're on the phone with Inventus. Having somebody who can offer you suggestions, things you could try, things they've done before in other cases where they had a similar problem, is great.

I always joke with Chris about how we hate to say, "I don't know." But when you find someone who will, that's great because rather than making up an answer or letting something go completely wrong, they'll go find the person who does know the answer, or they'll find what you need to do by relying on folks with more knowledge about that area. This is such a vast area. It goes far beyond law. You could get into project management, technology, linguistics, data intelligence. No one person can be all that. That's why you have to have a team, and that's why you have to collaborate. It's just that in each case, the facts and circumstances are different, and your process has to be flexible.

You don't want more data than you need, as that bogs you down.
– Christopher B. Woods

Woods: I suspect of those of us on the call, I'm the one who knows the least about the technical aspects of the tools. That's OK, because we all bring different experiences and different expertise, and we have different roles. The key is to put together the right team. As Amy said, we feel that the greatest value we can get from our e-discovery firms is that they share their experience and make suggestions. They see this every day. They see counsel who try different approaches, and through their experience, they know some things that maybe we haven't thought of. They also have seen things that didn't go so well. They know some functionality that exists within their tools that I might not have used.

While I think it's important for outside counsel to be educated enough that they can understand the issues, talk intelligently with their team, and make informed decisions and recommendations to their client, I don't need to be the expert. What I really look for are project managers who understand my objective and give me options, and tell me the pros and cons of things that I might suggest. We have had a number of vendors in the past who do what you ask of them, but they don't suggest alternatives.

The wonderful thing about working with Steve is not only is he incredibly responsive, he understands our objective. He shares that objective. So, if we present him with a problem, he'll tell us the advantages and disadvantages of certain approaches and let us make that decision. Also, if we ask him to do something, he has the knowledge and experience to do it consistent with our objectives. It's been really refreshing, and it makes my life a lot easier as outside counsel, to have a partner like Inventus and a project manager like Steve who I can rely on to do those things.

Kennedy: A lot of times in these relationships, there can be kind of an "us and them" dynamic. It's almost combative. "What's our vendor doing to us? What are they going to do to us today?" Where you get the most traction is when, as Chris said, you're a team. We don't know all the legal strategies, but our job is to support those strategies. Our job is to understand what you want to do. There may be two or three different ways to do it, and we may think one is the best, but it's always important to remain open to other ideas, as there may be things that we aren't privy to. You have to keep an open mind and be as flexible as possible, but always with the understanding that our goal, like Chris said, is to make our clients' lives easier – to kind of take away the headache of e-discovery so that they trust us and trust that things are going to get done properly and in a timely fashion. We want them to think, "They are there for us. They are listening." That's what we can do to build the relationship so we are a team and not sinking, but hopefully, mostly swimming, together.

Woods: It's also nice that they are patient when I ask stupid questions.

Kennedy: There are no stupid questions.

Sellars: What I really like about Chris is that Chris will ask a lot of questions. He's like a five-year-old. He asks until he understands it. Again, I urge people who are reading this and thinking about getting into large-scale e-discovery projects, you have to be willing to learn a whole lot as you go. I learn a whole lot more in every project, and continue to learn, and the technology continues to change and the rules are changing. It's a great comfort to be a part of a group of people sharing ideas and strategies. I'm relying on Chris to ask questions until he is satisfied that we're doing this in the most efficient way and with the best results.

Kennedy: Some vendors would maybe get frustrated, but frankly, I think it's always great when clients want to educate themselves about the process. It really helps if you're all speaking the same language. Large-scale e-discovery is not going away, so the more you know, the more it can help you moving forward.

MCC: Energy infrastructure is kind of a niche area. What, if anything, is different about data and e-discovery in your cases?

Woods: I don't view it as being substantially different. If I have a case that involves a substantial amount of data, it doesn't really matter if it's an energy company or a financial company. There will still be a whole lot of email with attachments, and there will be noncustodial sources that we need to identify, collect and review. When it comes to large amounts of data, it's the same questions regardless of the industry. For instance, what data needs to be collected? How am I going to go about reviewing it in the most cost-effective manner? What does the schedule look like? I find that volume, your opposing counsel and your schedule are much more important factors in the e-discovery process than the industry from which the documents came.

Sellars: The only thing I would say about a regulated industry is that people get accustomed to the idea that things have to be saved for what are sometimes inordinate periods of time. They get used to that as a practice and don't differentiate between data subject to regulation and all data. I think, however, that this is probably a universal problem with people overpreserving stuff regardless of industry, because storage is cheap and the time to go back and clean up is hard to find.

The other thing is that in our industry, we have sensors on everything. We are collecting data at a ridiculous rate all day long at every site, every fractionation plant, every processing plant. There are sensors everywhere sending data constantly. Some of that data is immediately overwritten, and some of it is captured and stored in other databases. If you had an incident at a plant, for instance, there is the potential to have literally hundreds of thousands of lines of sensor information coming in, which is something we are struggling to understand how to deal with. Most people are struggling to understand how to deal with mass volumes of data. A lot of it's raw, but it's there. You have to figure out what it is and deal with it even if it should have been disposed of long, long ago.

Kennedy: I wouldn't say there is anything different. Like you said, it's primarily email and attachments. I know that we have other oil and gas projects that,

Continued on following page

E-Discovery Is About More Than the Tools

Continued from previous page

depending on the size and the scope, can involve a lot of scans – nonelectronic data that's scanned in – which can be a challenge to work with. Just as you might be working with a lease from the 1980s that was almost handwritten. There can be challenges getting searchable text and things like that. Otherwise, the data is pretty similar to any other large-scale litigation – primarily email and attachment data with some loose files.

It's about taking a consultative approach and leveraging the expertise and experience of the vendor to the benefit of the client.
– Clint Williams

MCC: What are some of the essential tools that your teams are using to collect and analyze data?

Kennedy: The primary tool we use is Relativity as a review tool. Within Relativity, I think the most useful tools that we have are analytics. Whether that's email threading, deduping technologies, assisted review, all of those work together to streamline the review process. One of the most expensive aspects of large-scale litigation is review time – having contract attorneys go in to look at individual documents. Using technology, whether it's de-duping in your processing environment, email threading to sort threads so that you don't have people looking at different parts of an email thread at different times, works to cut down that review bill, which I think is of great benefit to clients.

Williams: Like Stephen said, we primarily utilize Relativity for review. However, we have many proprietary custom developments within the tool which were all built based on client feedback. Our focus has always revolved around delivering exceptional value to our clients by reducing cost and risk. We achieve this goal by leveraging our unique combination of best-in-breed technology, customized workflows, and most importantly, people. Those are the necessary ingredients for success, but the secret sauce is all about the people.

MCC: Do you anticipate any changes to your strategy or approach to project management given the recent changes to the Federal Rules of Civil Procedure?

Woods: I am cautiously optimistic, but in terms of preservation, I would take a wait-and-see approach. Until we see how the courts apply the rules, there is potential to get yourself in trouble if you get too aggressive when it comes to preservation obligations.

I do think, however, there will be some immediate changes in how lawyers approach and conduct a Rule 26(f) conference and try to limit the scope of discovery. I think we will have stronger grounds to seek, and likely be able to obtain agreement regarding, reasonable limits on the scope of discovery. In my experience, there has been a trend toward that anyway. E-discovery has become so overwhelming that opposing counsel doesn't want to receive more documents than they can handle. If you have another large company on the other side of the case, they are feeling the same burdens that you are. Counsel has been increasingly willing to agree to some scope limits, and I think that the recent changes to the rules will continue that trend.

Sellars: I completely agree with that. I'm hopeful this will substantially lessen the review burden. At a recent EDI conference, I asked a panel of judges whether proportionality would apply to preservation. The answer was, essentially, "no" and/or "you won't know what proportional preservation is because the judge gets to tell you." Chris is right that while we may have to save email and documents for 100 custodians, in a 26(f) we might get down to an essential 10 and focus efforts in a more proportional way, but I don't think the preservation burden will change. The rules are only codifying developments in the case law over the past few years. Our strategy won't change substantially, but I think other people may begin to understand better how to appropriately scope discovery in large cases.

Kennedy: If this helps clients reduce the scope of what has to go into a database or get reviewed, then this will help us help them by reducing discovery costs.

MCC: What's your advice to other in-house lawyers looking to collaborate with data management experts such as Inventus?

Woods: As we discussed, the key is putting together a good team and finding project managers who understand your objectives and concerns, and are proactive in offering their advice and expertise. As lawyers, we need to be educated enough to make sure we can meaningfully contribute to the discussion and evaluate strategies that comply with our obligations and develop our case, but also which manage costs based on what's appropriate for this litigation. Lawyers don't have to be IT experts. If you put together a good team, the better that they'll make you look in the end.

Sellars: Amen to all of that. Chris and I have said many times that there are lots of vendors out there and lots of products. The most important part is the project manager. Tools are tools. People think and are smart and are invested, and when you've got a project manager from a vendor who works with you and is invested in the outcome, it's a very different experience from some of the other experiences we've had.

Woods: Amy and I have worked together for a long time on a lot of large cases. This is our first case in which we've worked with Inventus. That tells you that clients will continue to look for a vendor that helps them until they find it. We're on the phone with you today because we've had a very good experience with Inventus, and we feel that Steve has really set the bar in terms of what we're looking for from a project manager.

Williams: Being open to the vendor's suggestions and the expertise that they bring to the equation is extremely important. One of the things that stuck with me when this engagement began was Amy's statement that the project managers make or break the value of any engagement. That's 100 percent true. You can have the technology and the workflows, you can even have all of the "tools" necessary for success, but if you don't have the right people asking the right questions, the value that you can bring to the engagement will be negated. The vast majority of our project managers are lawyers who have substantial experience managing complex litigation and document reviews in various aspects of law. There is a tremendous amount of value to be had by our clients in leveraging that experience. One of the things that I ask of all my project managers is to really challenge our client's way of thinking. If we see a better way we will "challenge" our clients to take a different approach. It is great when we get to work with clients like Chris and Amy who allow us the freedom to bring different thoughts and creative ideas to the discussion. It is through those consultative conversations that I feel we are able to deliver significant value to our clients.

New Tool, New Efficiencies

Practice Point brings together the best of Westlaw and Practical Law to streamline legal department work flows

By Emily Colbert / Thomson Reuters

The system is designed to deliver the most relevant content, along with the tools to quickly and efficiently accomplish the task at hand, in a single search.

Emily Colbert
Vice president of global workflow solutions for the legal business of Thomson Reuters.
practicepoint@thomsonreuters.com

As demand increases for counsel to handle more work in-house while also better managing outside counsel, there's a clear need for greater efficiency in handling matters. One avenue for achieving this goal is by streamlining those in-house workflows, especially as counsel are asked to take on new and complex situations.

The complexity and time required of legal work can vary tremendously from task to task, particularly if it's an area, matter or issue that is less familiar to the legal department. Quickly identifying and assembling on-point legal guidance to form a solid grounding on an issue is essential whether the matter is to be handled in-house or sourced to outside counsel. One key to this is to have the most relevant information and appropriate tools readily accessible in one place.

One of the more intriguing approaches combines authoritative legal research, legal know-how and assistive tools into a single solution. Thomson Reuters recently unveiled Practice Point, which brings together the best of Westlaw and Practical Law, along with time-saving tools and a slew of other helpful resources.

Practice Point users can seamlessly access both Westlaw and Practical Law content, placing key information from both at their fingertips without the need to continually switch back and forth between applications. Building on Westlaw content and functionality and Practical Law legal know-how, Practice Point delivers highly relevant, curated legal content, organized around the ways in which in-house counsel works. It's uniquely arranged by practice area, project and task, with proprietary task-based menus that make it easier to focus on what needs to get done without having to sort through extraneous information.

Practice Point is organized around typical corporate counsel workflows. For example, users can browse by a practice area such as labor and employment, or by project, such as launching a new product.

The system is designed to deliver the most relevant content for a specific matter or issue with a single search, along with the tools to quickly and efficiently accomplish the task at hand.

It provides access to Westlaw's authoritative primary law, analytical materials, practice area insights, public records and other legal research resources. Users can also utilize Westlaw organizing features, such as foldering and search history.

Furthermore, Practice Point is integrated with Practical Law know-how resources including practice notes, standard documents and clauses, checklists, toolkits, legal updates, global content and state-specific guidance. This can be particularly useful for getting up to speed quickly and providing a starting point for highly specialized or unfamiliar practice areas.

Practical Law content is authored and continually updated by expert attorney-editors. These editors bring significant experience from the world's leading law firms, companies and public organizations across practice areas, ensuring that content is up-to-date and reliable.

Key workflow tools are accessible anywhere from within Practice Point. These include Business Law Center, information on public and private deals and filings, public and private company information, document drafting tools, West LegalEdcenter and other CLE resources.

One example of how Practice Point brings these resources together to improve workflow is Rulebooks, a browsable online collection of federal laws, rules, regulations and related materials organized in a format exclusive to Practice Point. For capital markets and corporate governance practitioners, Rulebooks makes it easier to pinpoint and track changes in the rules and regulations covering securities offerings, SEC disclosures and reporting requirements, proxy solicitation and more. Plain-language searching allows users to find statutes, rules and regulations by popular name without the need to look up USCA and CFR citations.

Practice Point was developed through extensive research and feedback from leading corporate counsel and Thomson Reuters internal attorney-experts to supply the most relevant content, analysis and tools for a given task.

The result is legal guidance, research and know-how, plus time-saving tools – all integrated into one solution. It uses proprietary task-based menus tailored to the way in-house counsel actually works. It helps users navigate new or unfamiliar matters and practices, and see issues from a broader legal perspective. This, in turn, helps counsel to better understand related issues, and advise, negotiate and draft more effectively. The task-based organization provides clear paths for accomplishing a project, whether done in-house or managing outside counsel work.

Having the right information, tools and other resources needed for a specific task delivered all in one place at the right time can yield tremendous benefits. It can mean more effective work product achieved with greater confidence and efficiency. Multiplied across the numerous tasks and matters that a typical corporate law department faces, the advantages of such an approach are clearly manifold.

Thomson Reuters is continually innovating to bring content, tools and other resources from across its business in new ways to help their customers manage their organizations better and handle matters more efficiently.

MCC INTERVIEW: Hal Marcus / Recommind

Choice, Control and the Cloud

Survey: E-discovery consolidation benefits companies, but resistance persists

*Hal Marcus, Director of Product Marketing for **Recommind**, a leader in data analytics and e-discovery technology, discusses the company's recent survey of Corporate Law Departments, including their openness and resistance to an e-discovery consolidation strategy. His remarks have been edited for length and style.*

MCC: Recommind's 2015 Corporate Legal Survey delves into how legal operations, analytics and the cloud are reinventing the corporate law department. What were the most surprising and important takeaways from the survey?

Marcus: Most surprising for me was the counterpoint between the concerns over data security around e-discovery, with 72 percent concerned about sharing data with outside law firms and other service providers, and the very low number that reported ever conducting audits of their outside counsel regarding their technological competencies. Put those two side by side and it's hard to reconcile them. It's one of those great poster children for the challenges facing an industry that can't turn on a dime and has a lot of overhead associated with the things being done. Despite that, I've worked with some large firms that indicate anecdotally that they're receiving more security audits then ever before. What this shows is a trend toward law departments taking matters into their own hands.

MCC: What was the single most important thing that came out of the survey?

Marcus: Most important for us, as we look at our strategy and where we apply our energies, is the benefits of consolidation of e-discovery. We saw a lot of things we expected, but it's great to have it fleshed out. This was as much a qualitative survey as a quantitative one, more so perhaps on the qualitative side. These were full interviews, so we got a lot of candid, anonymous remarks. We saw that those that have done consolidations have accrued great cost savings and other benefits. They noted challenges as well, and those tend to relate to things like being locked into certain service providers, communication practices, billing practices and the like. That speaks to the model we're pursuing and what cloud technology is making more readily available today, which is that corporations can control their data and still have a variety of choices around service providers and outside counsel.

MCC: There seems to be a shift underway as many corporate law departments follow their companies, which are adopting the cloud for many purposes. So while some are getting over their fear of the cloud, plenty continue to be scared. What's driving this tension?

Marcus: We should probably start with the resistance. Some of it makes sense based on history. Some companies are concerned about lack of control, security and being beholden to others. These concerns are not necessarily valid in the current environment, but they persist. For some of our clients, among the best technology companies in the world, it makes sense that they want to manage their own data given how well they know their own security parameters. That's logical. Regarding the other side of the equation, the openness to moving forward despite those concerns, that's because the best options are available in the cloud, and that's increasingly the case.

Hal Marcus
Director of Product Marketing at Recommind.
415.394.7899

Moreover, organizations are being pulled there whether they want to be or not. There's a forced paradigm shift underway. End users within corporations are leveraging consumer chat systems and consumer sharing systems such as Box and Dropbox. They're doing this to collaborate and have easy access to data whether their organizations support them or not. The corporations, for the most part, are coming around to providing support and institutionalizing things so there's more consistency. As they're being pulled in, they're becoming more open to the cloud. On the security front, there's a growing recognition that it may be best to leave security to cloud providers that live and die by it and focus on it night and day. They're evolving their solutions and providing the tightest security available. Relying on them gives companies a degree of accountability.

One additional point worth highlighting is that as we see more cloud usage in businesses generally, that means the data is already there. Keeping the data in the cloud for a review and production process makes sense. That said, not all of the data is in the cloud and this point sometimes gets lost. Even with high-end tech companies that are very well set up with technology, there will still be a real need for hybrid solutions for the foreseeable future. You need to be able to collect and cull from on-premise sources. That touches on both resistance and openness, if you will. The legal department needs to find a way to straddle both.

Companies don't want to be forced into settling early on unfavorable terms because of the expense of e-discovery.

MCC: E-discovery is top of mind for inside and outside counsel, especially with the changes to the federal rules that took effect in December. To what extent is that the driver shaping attitudes toward moving to the cloud?

Marcus: A couple of things have happened with e-discovery that are forcing a broader recognition of the cloud. One part is that all of us in e-discovery that have been providing hosted solutions over the last couple of years and hosting large cases in that environment are giving corporate legal departments a reason to begin using cloud solutions. That's especially the case when no other approach allows for the same level of collaboration by getting outside counsel, other services providers and themselves on the same page with the best solutions. They're coming to recognize that the cloud is a good way to go.

Now we're seeing that mature. Corporate counsel are starting to consolidate their providers, including outside counsel, so they can benefit from standardized best practices. One example would be prioritization of review – using analytics, machine learning, search and other tools to streamline the review process and not go document by document. With consolidation, they're reaping economies of scale. It delivers more predictable, lower costs, and it lets them reuse data stores from matter to matter. You commit to an amount of data and leverage it as you see fit. It's a much more efficient and cost-effective way to go.

MCC: Given that security is top of mind for corporate law departments, they're not auditing outside counsel the way you would expect given the level of concern. What are the companies that are addressing this doing to minimize risk, to make things more efficient and to reduce costs? Is there a set of best practices emerging?

Continued on following page

Choce, Control and the Cloud

Continued from previous page

Marcus: Not to be a broken record, but the first answer is consolidation. Or maybe it's better to say they're addressing it through adoption of a centralized provider. Having a centralized provider system, where you've conducted your audits and you're monitoring and tracking them, reduces the burden of trying to keep track of a dozen different service providers, a dozen different outside counsel and many different parameters. Consolidating makes this a much more manageable process. Those that are leveraging the best-in-class systems rather than creating their own stacks can point to a higher degree of security.

The other aspect is standardizing on better platforms. A big part of knowing your security, knowing your data, knowing what's out there is having the visibility into the data systems. That comes from leveraging platforms that give you great analytics, let you leverage the tools for better review efficiency, and give you earlier insights into your data. The more you standardize on those kinds of tools, the more you can keep track of your entire case portfolio and know where it is in real time at any given moment.

MCC: Many companies you surveyed reported they hadn't yet consolidated data, yet three out of four of that nonconsolidation group said they're considering it. If I'm in that group and I have to articulate the benefits and risks of an e-discovery consolidation strategy, what should I focus on?

Marcus: You could break down the benefits into three core benefits. The first is security. That means leveraging the best data centers you have, the best business continuity, things like being sure that your data is encrypted both at rest and in transit, and knowing that that's the case across the board. Another would be predictability. That's a fairly obvious one from a cost perspective, but it's a bit more nuanced than that. It's also about knowing you can adjust and adapt very flexibly, as needed, by scaling up, scaling down and leveraging services wherever and whenever you need. You can work on a self-service basis where you'd like, bringing in third-party providers when you'd like, and do all of that very flexibly. The flexibility that's emerging is a bit of a change from what we've seen in the past. The third would be visibility. That means being able to really look right into your data, into the practices of your outside counsel and other services providers, into the efficiencies they're achieving, the tools they're using, and see all that without hounding them for static reports on a monthly or quarterly basis.

On the risk side, some of the feedback in the survey and from other sources shows receptivity of the consolidation model from a cost perspective, but challenges with a particular service provider. Since they don't want to be locked in, having the flexibility to manage the data and choose outside counsel and service providers as needed offers the opportunity for much more control, which is a way to get around that risk. If the data is really under the corporation's control, the rest flows from there.

MCC: Many corporate law departments are deploying metrics to manage their work, which in part is being driven by the proliferation of in-house legal operations professionals. Corporate counsel have long focused on outside counsel spending, but they're extending beyond that. What should corporate law departments measure to drive real improvement, something noticeable to the GC and the board? If they could measure only one thing, what should that one metric be?

Marcus: This touches on one of the other interesting things that came out of the survey. Of all the metrics that were being tracked around e-discovery, efficiency was the aspect focused on by the fewest law departments. It was 30 percent while all the others were considerably higher. That's telling. The one thing that they should be tracking is review efficiency, as long as they have the right definition. Everything else pretty much flows from it. The definition I would propose is: How much irrelevant data do you have to review to find the relevant data that you actually need? There are different goals for every matter – an investigation is different from a review for production in a massive litigation – so the goals change in terms of what you need to review and what you need to find. But for any kind of matter you can look at a very simple metric of irrelevant content versus relevant content in what was reviewed. It could be one to one – one irrelevant document reviewed for every relevant document found – or it could be far worse than that, or it could be better. If you're tracking that number across all of your matters, and you can visualize those down to the type of matter, the service provider, the counsel that worked on it, and compare and contrast, you're going to see what kind of practices are in place. Everything else flows from that: early data analysis, prioritization of review, staffing choices, outsourcing, choosing the right analytics and technologies, leveraging search effectively. All of these things come together in the level of efficiency you're achieving.

MCC: Why aren't companies using this metric more? Is it just too hard? Are they worried what they're going to find?

Marcus: At the risk of overstating it – this did not come out of the survey – I'm pretty confident that one key reason is that review efficiency is not consistently defined. It's not entirely clear what it means to people to track review efficiency. For some, it's where we stand on budget. If we're on budget, we're efficient. For some, it's whether we turned it around on time. If we turned it around on time, we were efficient. For some, it's that we only looked at 10 percent of the data because we effectively leverage technology. That's undeniably efficient if it got you the results you needed, but there are so many other factors that go into it.

MCC: One takeaway from the survey that litigators especially should find interesting is the impact e-discovery costs are having on litigation strategy. In many ways, this is the most compelling reason why a strategy such as consolidation, with real potential to drive down costs, is attractive.

Marcus: I'm an ex-litigator from a Wall Street firm and I'm always intrigued by how people think, based on what they see on TV, that lawyers, especially litigators, are big risk-takers and adventurists. My take is quite different.. Generally speaking, and with good reason, they're actually quite risk averse. We went back into the survey data specifically to see what we would find if we broke it down by those that had consolidated and those that hadn't. Was there a delta in terms of impact on litigation strategy? We were pleased to see there was a significant delta. That's pretty telling. It's more than about saving money. It's also about the autonomy of the legal department to do what it sees fit. They don't want to be forced into dealing with an action, or settling early on unfavorable terms, just because they have to bear the expense of e-discovery.

Microsoft Office E5 Compliance Center

Changing the in-house discovery toolkit

By Laura Kibbe / RVM Enterprises, Inc.

2015 saw a lot of developments on the eDiscovery front – amended Federal Rules, the Safe Harbor downfall, further crazy acquisition consolidation in the service provider space, and many changes in the technology we rely on. If you are corporate counsel charged with keeping up with all of this, you might be feeling a bit overwhelmed right about now. Will any of it make your job easier? Are you going to need to learn some new crazy technology that hasn't been tested in the courts? How will your company's IT initiatives impact your eDiscovery process and budget?

For those of you whose organizations have moved to, or will move to, Microsoft's Office 365 Enterprise Edition (E5 specifically), your life may get just a bit easier, and your eDiscovery budget just might see a little relief. With E5, Microsoft enhanced the Compliance Center in Office 365 by integrating the Equivio advanced analytics functionality into Office 365 Advanced eDiscovery. So, good news for all of you Zoom fans, all that functionality is now a part of Office 365.

What does that mean to your eDiscovery process? All the stuff many of us have come to take for granted as routine in our discovery workflow, like deduplication, email threading, near duplicate detection, predictive analytics (or predictive coding), and conceptual organization or clustering for review (themes), is now part of Office 365 and can be done BEHIND the firewall (the cloud firewall that is) BEFORE you send data to your service provider.

Imagine running your searches, identifying e-mail threads and near duplicates, suppressing non-inclusive emails, non-unique attachments and exporting only the resulting subset to your service provider in a load-ready format for any of the industry standard review tools. You could also use predictive coding for early case assessment in internal investigations and smaller matters in which you may not want to incur traditional discovery charges (processing, hosting, etc.). The result? Better, more accurate information found more quickly in internal investigations. Processing and hosting costs would dramatically decrease. Review costs would similarly decrease as only inclusive emails and unique attachments would actually be reviewed (you know we lawyers can't help ourselves; if it's there, we'll review it). Assuming appropriate review workflow and quality control measures are employed, review calls should also be more consistent and intuitively more defensible. Now that's good news!

From an information governance standpoint, you might also find some interesting uses for the Advanced eDiscovery functionality. Imagine using some of the predictive coding and themes features you relied on in the litigation context proactively to predict non-compliant behavior in close-to-real time? Legacy data also continues to be a challenge as repositories grow larger and more unstable. If you know that at least some of the custodians are absolutely not subject to hold, and their data can be disposed of, maybe Office 365 and Advanced eDiscovery can help there too.

Assuming you can defensibly determine what to retain and what to discard, migration of legacy mailboxes and documents for some set time period into Office 365 might make that legacy data more manageable for discovery and investigation purposes, and ultimately easier to manage at disposition. Being able to leverage the power of analytics where the data resides opens the door to myriad information governance opportunities at a far more economical price point than ever before.

Sound like utopia? Not quite yet. Today, because corporate data lives in many places other than Office 365, and will continue to for some time, Advanced eDiscovery won't be a panacea for solving all your discovery problems, but it can certainly be a powerful tool in your discovery arsenal as you look to manage your ever-shrinking discovery budgets and ever-expanding data volumes. As you would with any new tool, you need to make sure you understand the total impact on your current internal and external discovery processes, so that any necessary changes to your current processes continue to ensure defensibility. The good news is that the underlying technology is not new – it's a use case for tested functionality that has now been incorporated into another mainstream technology tool – Microsoft Office.

Laura Kibbe
Managing Director of Client Services for RVM Enterprises, Inc.
lkibbe@rvminc.com

> ***Leverage the power of analytics where the data resides.***

What does that mean for you? Here are a few considerations you should be mindful of when you embark on your first Office 365 Advanced eDiscovery project:

Multiple Workflows. Remember that all of this only works on data that is residing within Office 365, so you need to establish a cohesive discovery plan that accounts for both Office 365 data and non-Office 365 data. You may choose for efficiency purposes to migrate non-Office 365 data into Office 365 first, or maintain two (or more) separate workflows. If you choose to maintain separate workflows, ensure that each is properly documented, and that the tools used for things such as deduplication and threading are consistent (or at a minimum identified so you know what you can compare and what you can't—apples to apples and all that). It is important to remember that the new rules haven't changed the fact that defensibility is still the hallmark of any discovery exercise, so you want to be able to explain what you did if you ever need to defend your process.

File Types. Right now, not every file type can be migrated into Office 365. If your case involves one of those, you will have to maintain a separate workflow. The types of files that can be migrated are always expanding. Check that your file type can be migrated, or determine if you need to convert to an accepted file type before you can migrate (e.g., Lotus Notes to Outlook .pst).

OCR. Have any non-searchable .tiffs or .pdfs? At the moment, there is no OCR capability incorporated into Office 365, so be sure to have a downstream plan for OCRing. But with Microsoft, I'm sure OCR can't be that far off.

Data Privacy. Even the cloud has to respect data privacy rules. If your company has gone to Office 365 globally, you need to consider the logistics of using potentially separate Advanced eDiscovery workflows in each of the areas in which you do business, just as you would if your data were sitting in good old fashioned brick and mortar data centers. Currently, Microsoft is utilizing 24 data centers for its cloud, with two more German data centers coming online soon. Keeping abreast of what data is where, and what can or cannot be searched together, is essential in managing a global discovery project.

Size. Even though the Office 365 cloud is vast, right now the Advanced eDiscovery functions do not scale to the entire cloud all at once. There is a size limitation to how many documents can be analyzed at one time. As that capacity increases in future releases, scope your project accordingly, particularly if you will be utilizing the predictive coding technology and need to plan for training time.

Personnel. From a personnel standpoint, bringing more of the traditional culling work behind the firewall, while saving cost, can also increase risk for the company. Thought should be given to the best way to approach and staff this new workflow. Many companies have handled collections and pre-processing in house for years, and have extensive in-house teams of highly technical staff who, with appropriate training, will find this new workflow very easy to assimilate into their discovery procedures. Others may have moved to Office 365 precisely because they do not have strong in-house technical support. Most will fall somewhere in the middle. In order to achieve maximum cost efficiencies and maintain defensibility, work with counsel and a Microsoft eDiscovery Partner to design workflows and assign appropriate staff, internal or external, for each function, to ensure a smooth transition to the downstream discovery functions. While the technology facilitates, it's the project management that will make or break your discovery project.

We may not have reached utopia yet, but the future looks definitely brighter with products like Office 365 Advanced eDiscovery in our toolkit. Armed with a solid roadmap and a well-thought-out strategy, we could be permanently changing the way we think about eDiscovery from the in-house perspective, and that's a good thing. Now is the perfect time for in-house counsel to reignite its partnerships with the business, with IT and information governance colleagues, and to explore what benefits and efficiencies can be achieved. Office 365 Advanced eDiscovery just might be the platform legal, IT and the business need to demonstrate that managing legal risk, protecting vital information assets and achieving business goals can be accomplished at the same time.

MCC INTERVIEW: JR Jenkins / FTI Consulting

Seeing Is Believing – and Understanding

FTI's new Radiance platform visualizes your entire information ecosystem

*JR Jenkins is a member of **FTI Technology,** the e-discovery and information governance practice within FTI Consulting. Jenkins helps drive product development priorities, particularly in relation to Ringtail, FTI's e-discovery software platform. Here, he introduces Radiance, a new data analytics tool that can serve as an upstream partner to Ringtail, and highlights its unique visualization capabilities. His remarks have been edited for length and style.*

MCC: Tell us, what is Radiance?

Jenkins: Radiance is our brand-new visual analytics software platform that helps organizations make sense of their enterprise data. It's a highly scalable, flexible platform designed to assist with compliance projects, risk assessments and activities ahead of e-discovery. It allows organizations to connect with, enrich, analyze and visualize a tremendous number of documents, millions of documents, from a wide variety of sources from a single user interface.

MCC: What kind of data can Radiance connect with and analyze?

Jenkins: This is one of the most important parts of the application. Corporations today are dealing with well-documented and well-discussed increases in traditional documents – email, business documents, etc. In addition, corporations are rapidly adopting cloud-computing technologies for storage as well as the creation of business information. In our regular day-to-day work on e-discovery matters, we're seeing an increase in Google Docs and Office 365 file types.

Google Docs and Office 365 are just the tip of the iceberg, though. Think of the various collaboration applications, structured data software, temporary storage applications – names like Slack, Dropbox, etc. Corporations are using these new cloud-based tools, and often without the central IT team permitting or even knowing about the use. This poses a huge challenge for organizations.

Critically then, Radiance has been designed to connect to the key repositories inside the firewall, the Exchange servers for your email, the file shares where you may be dealing with Word documents, Excel spreadsheets, etc. It can also connect to and then aggregate cloud repositories – the Google Docs, the Office 365 and applications that are dominating headlines today in terms of the business trades, like Slack and Trello. These tools are becoming a primary form of communication amongst teams inside a lot of big organizations.

The ability to bring together not only the traditional output of knowledge workers but also these cutting-edge sources and resources is a critical part of the Radiance story. It's a primary concern for lot of organizations that may have established workflows on how to preserve, collect and then review some of their email and docs but find themselves scrambling right now as to how to preserve, collect and review Slack data or things in Google Docs.

MCC: Tell us some of the problems that Radiance is trying to solve.

Jenkins: At a high level, Radiance allows users to quickly look at 100 million documents and make sense of that information. You can see the data in aggregate and pick out trends, or you can hone in on a few documents or interactions between employees. We're able to do this because of visual analytics. The other day I was thinking about the famous saying "A picture is worth 1,000 words." A visualization, then, illuminates 1,000 data points. It's really about trying to provide an environment in which somebody can take a look at everything and narrow down the corpus in a quick and elegant way. It is providing a visual analytics dashboard to your information ecosystem.

We live in a data-drenched world, and compelling visuals help us make sense of it.

JR Jenkins
A senior director at FTI Consulting based in Seattle.
jr.jenkins@fticonsulting.com

As you can imagine, there are a number of needs for this technology, especially if it's fast to deploy and easy for organizations to use, like Radiance is. As we go to market with Radiance, we're focusing on a couple of uses: early case assessment, early data assessment and investigation. These continue to be huge challenges for organizations, especially as data volumes continue to grow. With Radiance, you can quickly get to the meaning of this data by helping you isolate and focus on the smaller subsets of your data, such as around specific people, issues, date ranges and other variables.

MCC: Can you tell us more specifically how Radiance helps with investigations?

Jenkins: The thing that's most dazzling about the Radiance workflow is its ability to filter down the data in a way that you can go from looking at thousands of custodians and millions of documents to, within just a few clicks, a single custodian, a single person, a single day's worth of activity, what emails they sent or received that day, and what documents were part of those communications. Investigations are all about trying to identify and isolate a unique set of activities, a pattern of activity. In many cases, investigations start with a couple of facts, a couple of threads, and upon those facts and threads, we weave a more complete story.

Because of this, the Radiance home page is a chronology visualization. It shows a date range along with a list of custodians, and investigators can then very quickly select the timelines they are interested in, filter it even further by selecting one or a few key people and interact with these documents. And with a single click, they can be delving into the social networks and communication patterns of these people. From here, the user can intelligently expand their investigation using the custodians' own communication as the guide.

Another important tool within Radiance is concept analysis. During enrichment, Radiance analyzes text and catalogs all concepts – nouns and noun phrases – found in the content. The result is a rich index of "meaning" which the investigator can browse, visualize and analyze quickly. This reduces the burden on the user to know every detail and, instead, accelerates their understanding of the key fact patterns and themes inside the data. We often talk about investigators who are saddled with keywords as their starting point, and where and when keywords are useful. We know that keywords can be used as a way to get you going, but rarely can they be used exclusively to get you across the finish line.

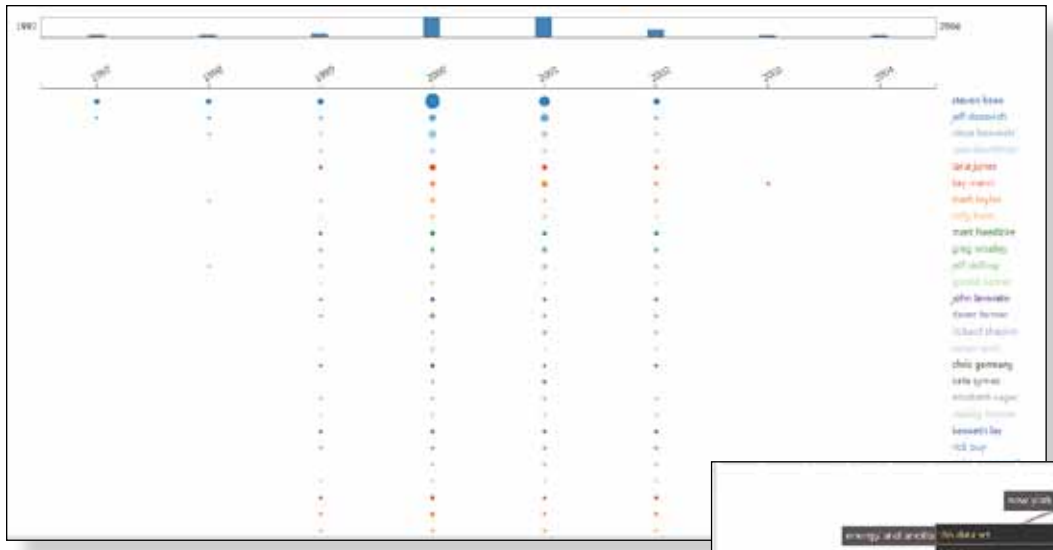
Armed with those small bits of facts – a couple of custodians, maybe a range of dates and a few ideas of what may be at the heart of the issue of the investigation – you can quickly find and isolate critical documents and, in the case of searching across multiple repositories, where they reside. And once identified, Radiance makes it easy to tag documents and ready them for the next phase of the project, which can include export into an e-discovery application, like Ringtail where they can be reviewed with the workflow amongst the team.

MCC: Tell us how Radiance helps with ECA?

Jenkins: ECA, or early case assessment, isn't a new term for lawyers, litigation support teams or e-discovery professionals. The problem is that as it hasn't really lived up to its promise. Inside corporations, ECA is, in many cases, seen as a culling exercise. It's all about eliminating as many documents as you can before review starts in a traditional e-discovery workflow, but very little analysis of the documents takes place. Sure, culling documents is a positive, but what if you can cull and truly do an analysis? With Radiance you can very quickly set aside tremendous volumes of data and do some really rich analysis of the remaining documents, custodians and trends. You can actually get down to looking at the documents.

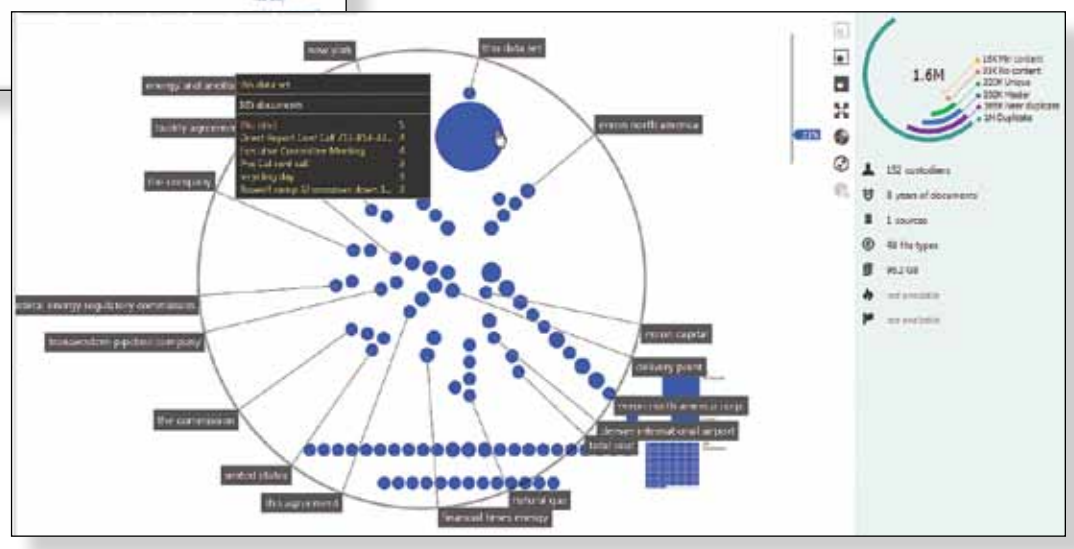
How do we do this? One of the really cool things about Radiance is that when

Continued on following page



Chronology

An easy starting point within Radiance is the chronology dashboard, which allows you to hone in on custodian documents across specific date ranges.



Document Mapper

Like Ringtail, Radiance provides concept clustering so you can quickly find important themes and accelerate your investigation

Seeing Is Believing

Continued from previous page

documents are brought into the system, there's a robust enrichment process. That means the documents are extracted and put through a robust text analysis process. This enables us to identify duplicates, near duplicates, threads, file types and size, and a host of other metadata. This metadata is transformed into facets that users leverage as they explore the data set. As an example, language analysis is one of the facets in the enrichment process. A great example of ECA use is that once you have found the 10,000 or 5,000 documents that you're interested in as part of an early case assessment, you can see how many have foreign languages included. Radiance will tell you not only what types of languages are included in those documents – Portuguese, Spanish, what have you – it will tell you what percentage of those documents are comprised of various languages and even highlight those for you within the document.

You can very quickly find out what your document volumes are going to be. You can see what the document variety is going to be or the file type variety. You can see what languages are being used. You can prepare much more strategically for a better review because you'll understand the characteristics of your ecosystem. Plus, Radiance offers a number of dynamic reporting features so this information can be shared at each stage of the project.

MCC: What are some of the visualizations Radiance can offer to users?

Jenkins: The Radiance visualization library includes 10 visualizations that can be used individually or in tandem. They can quickly illuminate millions of data points and support multiple starting points – date, organization, people, issues, languages, etc. – meaning subject matter experts are never at a loss about where to start.

In addition, Radiance comes with search tools that allow people to leverage traditional keyword approaches, if they have certain ideas that they're interested in, and you can quickly visualize a search result.

But we've found that investigators find the visualization-first approach truly liberating, as it allows them to interact with the actual document content, not what they think is in the document set.

So our visualizations start with the chronology visualization – it shows the distribution of content across time – as constraining dates is a logical starting point for investigation.

In addition, we have our innovative Document Mapper concept-clustering tool, which helps investigators identify batches of documents that contain similar ideas and terms. We use this in Ringtail for document review and coding, and inside Radiance, the document map and visualizations can be used to look at groups of documents and the concepts that are associated with them.

Also of critical use is the ability to look at someone's social network. We know that this is a significant component in a lot of analysis. Whether the investigation is around some notion of internal improprieties or whether it is along the lines of IP, having the ability to analyze somebody's social network, with whom they are communicating, both inside the domain and outside, with Radiance you can see what the communication patterns look like, what kinds of information are being sent back and forth.

The social network and the ability to look at visualizations across time and see the relationships between people and the information are critical.

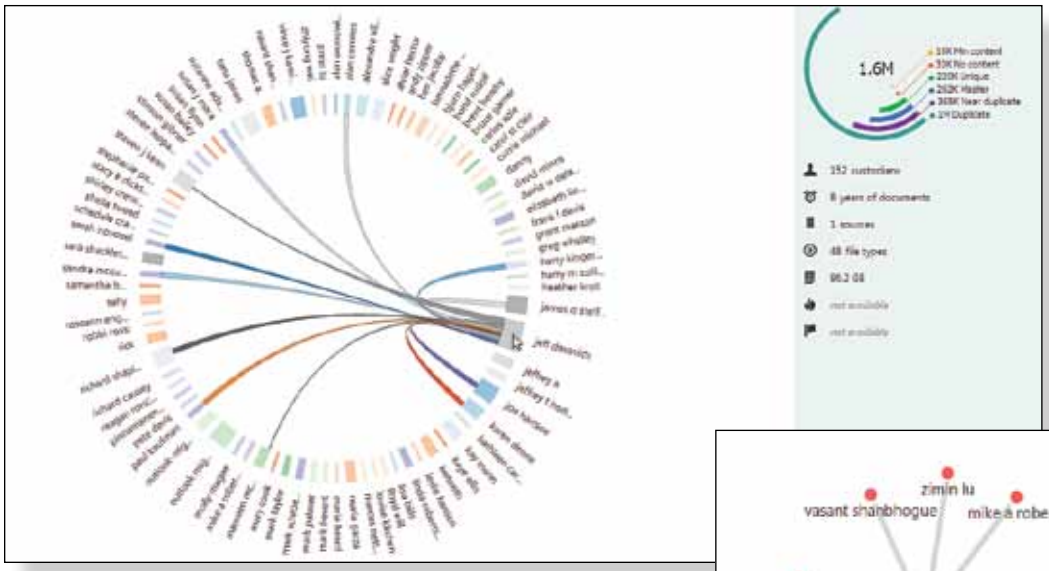
MCC: Tell us how Radiance is different from other software applications that are currently on the market.

Jenkins: From an engineering perspective, Radiance is really focused on high-speed performance and rapid feedback. The software feels nimble even when interacting with hundreds of millions of documents. This was accomplished through very thoughtful and innovative software design decisions that emphasize performance at the database, enrichment and presentation layers. We are keenly focused on visual data analytics at a massive scale, so we were merciless during testing to ensure that any feature or action in the user interface would not slow things down.

The other thing that makes Radiance different and unique is it is lightweight, meaning that it's not bolted to something much larger, much more grandiose. One of the things that really stops corporate teams from making investments in the world of big data is the big price tag that comes along with it. We're talking about multimillion dollar, multiyear contracts that take forever to install and train people on. We know that people want something fast and easy so they can get their heads around issues inside their own ecosystem.

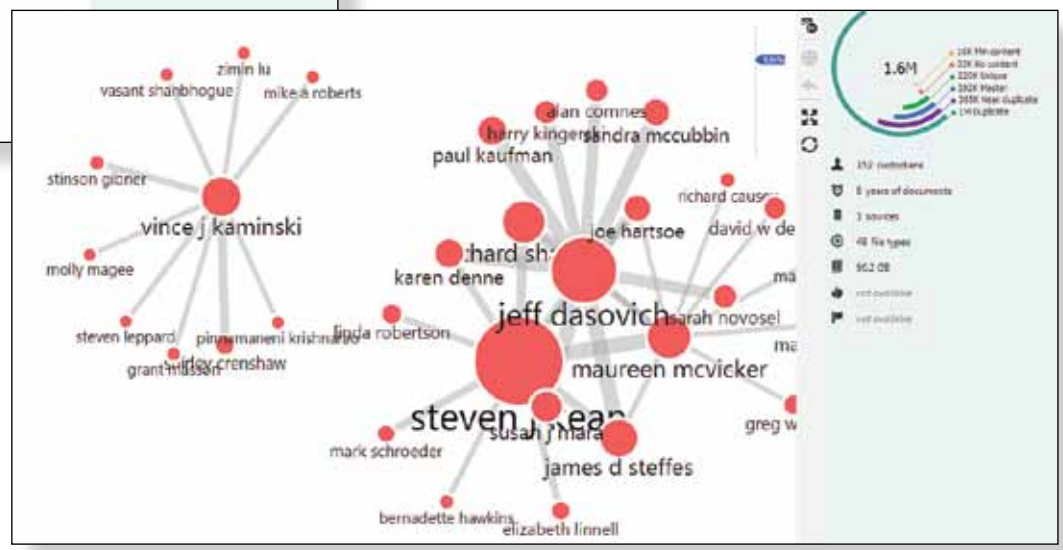
What we've designed here is something that's very fast, very flexible. It's designed to solve the set of problems of a big data repository so to speak. And it moves with you into some of the work flows that in many cases are mandated, whether it's the litigation or legal obligations that come along with being attached to e-discovery or inside compliance and risk offices to identify and isolate the data that may be at most risk.

Continued on following page



Relationship

Radiance reveals the communication exchanges between custodians so you can focus on important interactions.



Social Network

Radiance's social network view provides another tool for you to understand relationships and interactions among custodians

Seeing Is Believing

Continued from previous page

It's easy to come in with Radiance, get your data loaded and analyze it without having to make a multimillion dollar investment in consultants who are spending years inside your ecosystem trying to help you understand your data.

MCC: Who should be interested in Radiance?

Jenkins: Those who are involved with compliance, risk and e-discovery should be interested in Radiance. They may be working inside of legal departments, compliance or GRC teams, and even IT. Anyone tasked with investigation. Also, any organization that's made a move into a cloud environment within the past year should evaluate Radiance for its ability to connect with Office 365 and other tools.

What's interesting is that if you were in this market three years ago, there was a lot of trepidation about movements to the cloud. There was concern about data breaches, obviously, and the feeling that data inside your firewall may be more secure than data in outside repositories. With some of these incredible investments by Microsoft and Google and others, we've seen that what they can offer up in terms of protection is certainly on par with what corporations are offering.

Now, people have now made that switch over to the Office 365 world, to the Google Doc world, to using Slack, but they don't have any idea of how they're going to interact with that data for any of the aforementioned projects. We know those people are concerned about the lack of the workflow around those data types. Those are the primary candidates for taking advantage of Radiance's capabilities.

MCC: This is another FTI Technology software offering visual analytics to cut through big data. What role do you see visual analytics playing in e-discovery and information governance moving forward?

Jenkins: I think it will continue to grow. I think the simple answer is that visualization is, in many ways, the only way that you can get your head around the document volumes and the variety of data that you're looking at today. One of the exciting things about the time we live in is that there's been a real emphasis on charts and graphs and making sense of data. We see it in the use of infographics, which have become such a hot thing. We live in a data-drenched world, and compelling visuals help us make sense of it.

I joined FTI technology almost 10 years ago, and I came to the company because of the visual analytics, because of Document Mapper and its unique visual approach to what was the document review problem of 10 years ago. It is one of the most engaging, innovative and fun uses of visualization that I had ever seen.

I'm fond of saying that what makes our visualizations different than most is that ours are interactive. They're dynamic. You are asked to engage with the visualizations, to work with and shape them. While you're doing that, it's shaping your understanding, shaping your knowledge of the information you're working with. At the end of a four-hour review session with the visualization, you have a much deeper connection to the themes, to the people, to the trends that are part of that data than you do if you're just looking at long static roles, like we see in our email clients.

Every year we've had to tell the story about growing data volumes, and it's true. One of the interesting things that we're dealing with is not only are data volumes growing but data types are changing. I mentioned cloud-based applications, Office 365, Google Docs. That's a migration of a traditional data type to a cloud environment. What about Slack? What about Trello? What about some of these other things that we see as part of business communications, part of business intellectual property? What is a Slack post? Is that a document? Is that spreadsheet? How do we account for that in some of our investigations? Visualization of information breaks down all of these types. It continues to give everybody the edge they need when they walk in and need to make sense of the data quickly.

We've seen in e-discovery that the notion of visualization of data has grown in the last few years. It's no mistake that when we decide to build a brand-new platform that visualizations are at the very heart of it. The visualization experience was first and foremost in our mind. Our users are often subject matter experts who have a deep understanding of their business, about the notion of their unique business activities. They're not technologists. If you put certain visualizations in front of them, you're going to overwhelm them. We have a great deal of experience helping nontechnical types, lawyers, make sense of and review massive amounts of data. It's transforming that metadata and content into recognizable themes and patterns. It was no mistake that our foray into moving left of e-discovery was going to be highly visual.

That's the real opportunity for people using Radiance: to make sense of their data much more quickly. Radiance doesn't impose a structure on the data so much that it allows you to come in and build your own structure around the data, depending on whatever project you're working with. To do that visually means you're going to have a quicker understanding, I think, and more confidence in your decision making. As we like to say, there's this notion of finding facts fast. When you find facts fast, inevitably the strategy becomes *your* strategy. You own it. You have a much clearer sense of how you want to approach projects versus just reacting to either deadlines or the other side's demand for information.

MCC INTERVIEW: Jessica Lockett & Alison Wisniewski / Epiq Systems

Identifying the Implications of the *Schrems* Decision in Canada

Connecting the dots on data transfers between Canada, the EU and the U.S.

On October 6, 2015, Europe's highest court, the European Union Court of Justice (CJEU), issued the Schrems *decision, invalidating the EU Commission's Safe Harbor program, which had allowed for legal data transfers between the EU and the U.S.* ***Jessica Lockett*** *and* ***Alison Wisniewski*** *from* ***Epiq*** *– a leading global provider of technology-enabled solutions for eDiscovery, document review, bankruptcy and class action administration – explain the decision's immediate effects on Canadian organizations, as well as contemplate the likelihood of disruptions down the line. Their remarks have been edited for length and style.*

> ***Privacy protections in Canada were deemed adequate enough by the EU such that Canada didn't need to be a participant in the Safe Harbor program.***
> – ***Jessica Lockett***

MCC:* Schrems' *immediate impact in the U.S., a party to the Safe Harbor program, was significant, particularly for technology and other companies that relied on Safe Harbor. Canada, however, was not a party to the program. Does that mean data transfers are permissible and the decision has no impact in Canada?

Wisniewski: Correct, the EU decision doesn't currently have any impact on Canada or data transfers in Canada. There may be some issues if the data being transferred from Canada to the U.S. contains personal information of EU citizens.

Lockett: It is important to understand why Canada was not a party to the Safe Harbor program. The privacy protections in Canada were deemed adequate by the EU such that Canada didn't need to participate in the Safe Harbor program. That's the reasoning behind Canada's nonparticipation and the lack of impact of the *Schrems* decision in Canada.

MCC: Can you clarify how transfers between Canada and the U.S. are undertaken?

Wisniewski: Canada already has its own data protection act, the Personal Information Protection and Electronic Documents Act (PIPEDA), whereby there are certain requirements in the U.S. that must be followed in order to transfer personal information from Canada into the U.S. It is similar to what is needed in the EU, such as consent from the parties from whom we're collecting personal information, and sometimes consent to transfer such data into the U.S., actual explicit consent. Under Safe Harbor, the U.S. was able to conduct transfers from Canada into the U.S. without obtaining consent. However, even when Safe Harbor was recognized, clients in Canada typically would require that we obtained consent from the data subjects prior to the transfer of personal information from Canada to the U.S. Therefore, the requirements to transfer personal information from Canada into the U.S. haven't changed, unless Canada is transferring EU-specific personal information. In such an event, certain other precautions are needed in order for Canada to make that transfer.

MCC: The EC's* Schrems *Safe Harbor decision affects the transfer of personal data from the EU to the U.S. What does that mean for Canadian organizations that transfer EU citizens' data to U.S. territory or store or host it within the U.S.?

Wisniewski: Canadian organizations that transfer, store or host EU citizens' data could face some issues when transferring such data into the U.S. because Safe Harbor is no longer recognized by the EU. If we were transferring EU personal data into the U.S., the Safe Harbor protections would not apply. We have started entering into standard contract clauses with clients in the EU that allow the transfer of personal information back and forth; we sign that as a data processor. This might be something we would now need to consider with Canadian organizations in order to transfer personal information into the U.S. Epiq currently has a facility in Canada to host and process data, though, so EU citizens' data could remain within Canada and not have to come into the U.S. for any service that we provide.

Lockett: I agree. Generally, organizations such as Epiq that have the capability to host, store and process data within Canada are going to be able to work around that concern with respect to the transfer of EU personal information into the U.S. If they're able to hold data in Canada, the personal information protections currently afforded by Canada's laws are deemed adequate by the EU.

MCC: Are there specific steps that Canadian organizations transferring EU citizens' data should take in anticipation of what some observers say could be ripple effects from the* Schrems *ruling?

Wisniewski: For Canada, because its privacy act was drafted with the EU Data Directive in mind, and because it was not affected by the *Schrems* ruling, EU organizations can continue to transfer personal data to Canada as they have been without any impediment, unless and until the EU decides to take a look at PIPEDA and make changes.

Lockett: The ripple effect could be a concern in terms of a potential re-examination into Canada's privacy laws. It's been almost 15 years since PIPEDA was deemed adequate protection by the EU. It hasn't happened as of yet, but it leaves open the possibility that the EU could re-examine Canada and other countries' privacy laws to determine whether they still maintain adequate protection for EU citizens' data.

MCC: Although PIPEDA, which as you mentioned was motivated partly by the EU Data Directive, was determined to provide an adequate level of protection for the purpose of data transfers from the EU to Canada by the EU Commission in 2002, the European Parliament Committee on Civil Liberties, Justice and Home Affairs called for a review of Canada's privacy protections during its membership in the Five Eyes Alliance. It remains to be seen whether Canada will be challenged on the basis that it no longer provides adequate protection for EU citizens' data. What might the implications be?

Wisniewski: We would have to see how they rule. If they don't re-approve it, like they didn't approve Safe Harbor, then either Canada would be in the same position as the U.S. when it comes to personal data transfers to the EU, or Canada could revise the PIPEDA to reflect whatever comments the EU had in order to remain in line with the EU Data Directive. It depends on the decision.

Continued on following page

Jessica Lockett
Director of Document Review Services in Toronto at Epiq Systems.
jlockett@epiqsystems.com

Alison Wisniewski
Vice President, Corporate Counsel at Epiq Systems.
awisniewski@epiqsystems.com

Schrems in Canada

Continued from previous page

MCC: Is there any talk in Canada about trying to get in front of a prospective review?

Lockett: The *Schrems* decision is still new, and I haven't heard of any discussion, at least from policymakers, on its specific effect on legislation in Canada. However, the federal Anti-terrorism Act, 2015, Bill C-51, was recently passed by Parliament. The act has potential impact on the Canadian government's reach into personal data within Canada, and also makes some changes to Canada's broader privacy laws. Companies should be aware of these issues and get a plan in place on how to deal with different outcomes with respect to any re-examination of PIPEDA by the EU. It's a little too unknown at this point, but being mindful and watchful is important.

Epiq has a facility in Canada so EU citizens' data can remain within Canada for any service that we provide.
–Alison Wisniewski

MCC: Some experts have cautioned against underestimating the implications of the CJEU's judgment in* Schrems*, which they say could undermine mechanisms sanctioned by the EU to transfer data to the U.S., including contractual language and even the ECU's decision that Canada's federal data protection law adequately protects EU citizens' personal data. Are we on a slippery slope here, given the EU's hardline approach to privacy?

Wisniewski: By not allowing a reliance on Safe Harbor, it makes it much more difficult for the U.S. to conduct business in the EU. There are lots of different contractual requirements that will be required under agreements, as well as other requirements such as having a data center locally, having the capability to provide all of the services that a technology company provides locally, and actually being physically located in the EU. For Canada, that's not much of an issue right now, because they're not affected by Safe Harbor. In the event Canada is affected by an EU ruling of PIPEDA, more organizations will have to focus their services locally in the EU, adding expense and resources, rather than conducting a more global business.

Lockett: That's a great point. Europe appears to lead the pack in privacy protection, and they're coming out with a hard stance. It's not necessarily a bad thing, in my opinion, but legislators will somehow need to strike a balance between promoting commercial activity in a global market, and upholding the privacy protection of individuals.

MCC: For the companies doing business in Canada that you're working with, are you involved in any contingency planning right now for any disruption if things do change? The expectation is that changes need to be executed fairly quickly when working with the EU.

Lockett: There's been no discussion with clients of mine, but like I said before, people should be alive to the issue. There may be less of a concern with our clients, because we do have operational capabilities for hosting and processing in Canada, so Epiq currently has an extra protection there for our clients.

AccessData® has pioneered digital forensics and e-discovery software for over 25 years. More than 130,000 customers in corporations, law firms, law enforcement and government agencies worldwide trust AccessData across the EDRM. It has the only single platform and shared database built on Forensic Toolkit® (FTK®).

More information is available at
www.accessdata.com

iDiscovery Solutions, Inc. (iDS) is an award-winning, global, expert services firm that has been positively influencing the intersection of law and technology since 2008. Founded by industry veterans with more than 50 years of litigation and consulting experience combined, iDS delivers customized, innovative solutions for legal and corporate clients' complex challenges. iDS' subject matter experts testify and consult in connection with electronic discovery (e-Discovery), digital forensics, data analytics, information governance (IG), processing and hosting of electronically stored information (ESI) and enterprise applications.

More information is available at
www.idiscoverysolutions.com

Inventus is a leading international discovery management provider focused on helping clients reduce the costs and risks associated with the discovery process through the effective use of technology solutions. Its Luminosity technology provides an overlay to industry –standard software to provide unique analysis and insights, creating a more strategic, lasting relationship with its 1,200 clients. Since 1991, Inventus has been providing litigation support services to corporate legal departments, law firms and government agencies. Inventus currently has over 240 employees and operates in 16 cities internationally, with operational headquarters in downtown Chicago.

More information is available at
www.inventus.com

FTI Technology helps clients manage the risk and cost of e-discovery and information governance with confidence. FTI's market leading Ringtail® e-discovery software is well known for its scalability and performance, powerful review and analysis capabilities, the ability to search across millions of documents in seconds, and for having the most flexible production capabilities available. FTI Technology also collaborates with clients to deliver strategic solutions tailored to their unique legal requirements – from forensic data collection to cross border e-discovery to fully managed document review services.

More information is available at
www.ftitechnology.com

RVM Enterprises, Inc. has been the preferred provider of eDiscovery and consulting services to leading global corporations and Am Law 100 firms for twenty years. RVM's experienced professionals can assist around the world, across industries and in both the private and public sectors. RVM is proud of receiving certification as a woman-owned business.

A leader in technology, RVM was one of the first to be awarded kCura's Relativity Rating of Best-in-Service, and has achieved Orange-Level Certification. RVM is also the only company to achieve Equivio Partner STAR certification.

Its eDiscovery strategic consulting and expertise on the design and implementation of analytics technologies is geared toward defensibility and cost-savings.

What sets RVM apart? Building on Relationships • Unique Workflows • Strategic Partnering

RVM Services

Advanced Data Analytics

RVM's eDiscovery strategic consulting and expertise on the design and implementation of analytics technologies is geared toward defensibility and cost-savings.

- **RVM Structured Review™** (RSR) leverages advanced analytics, such as predictive coding, concept-based categorization and search to fill the gaps in current discovery practices.

- **Fact Discovery First™** is designed as a low-cost, deep knowledge triage to help you get to the information you need quickly.

Data Processing and Hosting

RVM has the capability to process and host the largest, most complex collections of electronic legal evidence. RVM provides unparalleled data processing services using its portfolio of eDiscovery products combined with deep technical knowledge..

- **Data Processing**
- **Data Hosting**

Forensics and Data Collection

RVM Certified Forensic Engineers can help your company walk through each step of forensic data collection from the initial consultation to providing expert witness testimony regarding the integrity of the collection process.

- **Data Collections**
- **Forensic Examinations**
- **Quality and Cost Control**
- **The RVM Tracer™**
- **Expert Testimony**

Managed Document Review

RVM's Managed Review and Analytics experts work together as a team of trusted advisors who will craft a customized solution to help you get to the most important data more quickly. RVM provides the guidance and training appropriate for your specific needs using our tried and true workflow models based on reliable, repeatable and defensible industry best-practices, along with your know-how about the specific matter at hand.

RVM Consulting

RVM experts provide a broad range of consulting services. RVM's goal is to ensure that it provides the best service possible in a consistent, legally defensible, and cost-effective manner. RVM's Consulting Team helps corporate legal departments and law firms assess, plan, develop and implement information governance through trial support programs.

- **Information Governance**
- **Litigation and Investigation Projects**

Corporate Enterprise Solutions

RVM's Corporate Enterprise Solutions encompass a broad range of solutions tailored to meet the unique needs of the corporate buyer. RVM understands that in addition to state-of-the-art technologies and best practices workflows, Corporations need greater visibility into combined metrics and trends as well as proactive consulting solutions. RVM's Corporate Enterprise Solutions include:

- **RVM Dashboard™**
- **RVM Audio Discovery Analytics**
- **RVM Tracer™**
- **Global Reach and Mobility**
- **Industry Experts**
- **Microsoft Office eDiscovery Partner Services**

New York • Chicago • Cleveland • Los Angeles • London

www.rvmediscovery.com • @RVMEntInc

ContractExpress
PART OF THOMSON REUTERS

Trusted Self-service Contract Creation

REDUCE DELAYS
REDUCE COSTS
REDUCE RISKS

IMPROVE SERVICE
IMPROVE EFFICIENCY
IMPROVE COMPLIANCE

Cloud

salesforce AppExchange Program **PARTNER**

DocuSign

On-prem

THOMSON REUTERS