

Cloud Computing

Practice Safe SaaS: Don't Lose Your Head (or Data) In The Clouds.

Katten

KattenMuchinRosenman LLP

UHY Advisors

Tax & Business Consultants

UHY Advisors FLVS, Inc.

Practice Safe SaaS: Don't Lose Your Head (or Data) In The Clouds.

Written by:

Hope Haslam

Principal
eDiscovery & Digital Forensics Practice Group
UHY Advisors FLVS, Inc.

Douglas Herman

Managing Director
eDiscovery & Digital Forensics Practice Group
UHY Advisors FLVS, Inc.

Dara Chevlin Tarkowski

Associate and eDiscovery & Digital Evidence
Practice Group Member
Katten Muchin Rosenman LLP

Martin T. Tully

Partner and eDiscovery & Digital Evidence
Practice Group Chair
Katten Muchin Rosenman LLP

Flying High Again.

Everyone knows of the mythical flight of Daedalus and Icarus. Daedalus fashioned two pairs of wings out of wax and feathers for himself and his son, Icarus. Before they took off from the island of Crete, Daedalus warned his son not to fly too close to the sun, nor too close to the sea. But overcome by the giddiness that flying lent him, Icarus soon curiously soared through the clouds, and in the process, came too close to the sun which melted the wax. Icarus kept flapping his wings, but quickly realized he had no feathers left and was only flapping his bare arms. And so, Icarus fell into the sea and drowned.

One of the biggest developments in recent years has been the stratospheric rise of what has

been fancifully termed "cloud computing." To be sure, this next generation of the internet is a very popular topic. If you type the word "cloud computing" into Google, you will get just a little over 20 million hits, and many important and intelligent computer scientists and influential organizations are contributing to the discussion. For example, Cisco CEO, John Chambers, has been quoted emphasizing that cloud computing is the "next big thing." Likewise, Erich Clementi, general manager of enterprise initiatives at IBM, has stated that "Cloud [computing] is an important new consumption and delivery model for IT and business services." See James Urquhart, "IBM Releases New Enterprise Cloud Portfolio," *The Wisdom of the Clouds*, (June 15, 2009). Even Oracle Corporation is now getting into the space "a little bit," just months after its outspoken CEO initially "described the trend as 'gibberish' and expressed skepticism as to whether companies could make a profit from cloud computing." Jessica Hodgson, "Oracle CEO Ellison Changes Tack on Cloud Computing," *The Wall Street Journal* (June 23, 2009)

To be sure, it is no myth that software as a service (SaaS) and its siblings can offer significant benefits to those that choose to employ it. But like Icarus, can companies that ascend to the clouds for their computing needs suffer from giddiness that can blind them to the practical risks that could bring them plummeting back to earth? In addition to varying views as to what is and isn't "cloud computing," organizations that are considering implementing such an "architecture," but have strong security and privacy concerns or are under the burden of litigation, subpoenas or regulator information requests at regular intervals, face significant challenges.

Cloud Computing Defined: I See a Sailboat, No Wait, it's a Pony!

Like two people who see different shapes when gazing into a cumulus cloudscape on a balmy summer day, there is a threshold question of what exactly constitutes the "cloud." As frequent "cloud blogger" James Urquhart has noted, "the market seems to have come to the conclusion that cloud computing has a lot in common with obscenity – you may not be able to define it, but you'll know it when you see it." James Urquhart, "The Cloud Conversation is Changing," *The Wisdom of the Clouds* (June 6, 2009). That said, "cloud computing" generally incorporates three distinct concepts – infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Different vendors offer one or more of these services. As an example, Amazon's cloud, known as Amazon Web Services, offers storage, computer processing, message queuing, and database management as plug-and-play services, all of which are accessed over the internet. Other examples are likely more familiar. Thus, if you have a Hotmail, Gmail, AOL, Yahoo or other web-based email account, then you are already a cloud computing user. Instead of running an e-mail program on your computer, as you would at work with Lotus Notes or Microsoft Outlook, you log into a Web email account remotely. The software and email storage for your account doesn't exist on your computer – instead it is on the service's computer "cloud."

Recently, the meaning of the term has warranted the attention from the U.S. Government. A draft definition for federal use of "cloud computing" has emerged from the National Institute of Technology and Standards (NIST), a non-regulatory arm of the Commerce Department. See James Urquhart, "Are the feds the first to a common cloud definition?" *The Wisdom of the Clouds* (May 10, 2009). The current draft definition of "cloud computing" is "a pay-per-use model for enabling available,

convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Draft NIST Working Definition of Cloud Computing v14. The NIST cloud model "promotes availability" and is comprised of five key characteristics: (i) on-demand self-service; (ii) ubiquitous network access; (iii) location independent resource pooling; (iv) rapid elasticity; and (v) measured service. *Id.*

How Does it Work? The Architecture of the Clouds.

Large organizations usually have hundreds of thousands, if not millions, of dollars tied up at any given point in computers and software. Further complicating matters is that the diversity of software needed for a given employee to be productive with his/her assigned computer is endless. Not every computer can have everything installed, as that would be cost prohibitive, yet it is an IT nightmare for each employee to have a completely "custom" software base. Under the SaaS concept, instead of tasking the IT department with installing a suite of software for each computer, only one application has to be loaded. That application would allow workers to log into a Web-based service, in the very same manner they would access the Internet, which hosts all the programs the user would need to perform his or her job. Remote machines, owned by another "servicing" company would run everything from email to word processing to complex data analysis programs. This concept is cloud computing at its heart.

Cloud computing systems are made up of two primary components – the "front end" and the "back end." The front end, more commonly known as the computer on your desk, and the

back end, the “cloud” portion of the system, is connected much like the computers on your company’s computer network, except that the “network” here is the Internet. The front end includes the client’s computer and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface, primarily because there is little as of yet in the way of standards in the cloud industry. Services like Web-based email programs leverage existing Web browsers such as Internet Explorer. Other, more complex systems have unique software applications that must be installed on the client computer, providing network access to clients. On the back end of the system are the various computers, servers and data storage systems that create the “cloud” of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from email to data processing to video games.

Why Enter The Cloudscape?

Some of the benefits commonly-attributed to cloud computing include the following:

- Ability to access corporate software applications and data from anywhere at any time.
- Access the cloud computing system using any computer linked to the Internet. Data is not confined to a hard drive on one user’s computer or even a corporation’s internal network.
- Reduced hardware and infrastructure costs. No need to have the latest and greatest equipment.
- Reduced software costs. Cloud computing systems provide company-wide access to

software applications, at far less cost than purchasing licenses for each machine. SaaS also reduces implementation lag by making new software versions available to users immediately.

- Reduced need for physical and digital storage space.
- Reduced IT support costs. Streamlined hardware, in theory, have fewer problems than a network of heterogeneous machines, each with slightly different operating systems.
- Increased processing power. The cloud computing system would tap into the processing power of all available computers on the back end, significantly speeding up the results of an elaborate query.

The appeal of moving to the cloud is clear—saving money on IT personnel and avoiding capital expenditures on hardware, software, and services, and instead, consuming your computing services like a commodity. Moreover, the applications of cloud computing, at least as we know them today, are limitless. With the breakthroughs in computing technology that are released each year, the power and capacity of creating cloud-based systems, with even more power and capacity than we can imagine, will be possible. With the right network connectivity, a cloud computing system will be able to provide all of the programs a normal computer could run. The cloud could serve up software systems that will have the ability to do everything from generic word processing to customized computer programs designed for a specific need or organization.

Given these benefits, why would anyone want to rely on anything but the cloud to run programs and store data? To begin with, cloud computing is not for everyone. For example, companies with extensive legacy mainframe

systems may find that making them available in a SaaS-like model to be prohibitively expensive. Some companies would have to spend hundreds of thousands of dollars to code these systems so that they could be offered via a SaaS-like model. Another consideration is the regulatory impact of moving corporate systems and applications to the cloud. For companies that have software programs in use within their environment solely for regulatory compliance, much can be at stake. At least for now, many of these regulatory-required systems would never make the transition from standard desktop application to a SaaS system. Furthermore, while the benefits of cloud computing seem convincing, there are risks that all would-be cloud dwellers potentially face.

Threatening Weather?

The Cloud Security Alliance (CSA), an ad-hoc, security-focused organization, recently released a whitepaper discussing the security implications of cloud computing. CSA is also addressing, to some degree, the impact that cloud computing will have on electronic discovery. For instance, the CSA whitepaper notes that:

“Legal systems in both developed and developing economies generally presume that a company, as a legal entity, will possess and control the records and information assets that may serve as evidence in legal proceedings in which a company may be involved. Further, there are various important affirmative legal duties for a company to preserve and produce those records and information assets in those legal proceedings, including regulatory reporting (tax records, environmental discharge reports), compliance audits, internal investigations and, of course, civil litigation.”

Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, 41 (April 2009). However, cloud computing business models “challenge the presumption

that a company possesses, or even controls, all of the digital business information for which the law may impose duties to preserve and produce,” and “potentially jeopardize a company’s ability to preserve and produce required records and electronically stored information.” As a result, “companies face substantial barriers to implementing cloud computing solutions if, as a result, their compliance capabilities and legal profiles are compromised.” CSA, *Security Guidance*, at 41.

Indeed, in a presentation at the April 2009 Storage Networking World show, Steven W. Teppler, senior counsel at KamberEdelson, LLC, went so far as to characterize “cloud computing and services” as “a corporate counsel’s [worst] nightmare.” See Marty Foltyn, “Cloud Computing Poses E-Discovery, Legal Risks (April 10, 2009). As Teppler observed, “cloud computing” means that “data may always be in transit, never anywhere, always somewhere.” *Id.* This transience, among other things, creates huge challenges for both corporate and outside counsel.

Cloud Computing’s Three-Headed Dog: Security, Privacy & eDiscovery

Such challenges bring to mind another Greek myth, that of Cerberus, the multi-headed dog that guarded the gates of Hades to prevent those who had crossed the river Styx from ever escaping. As the foregoing section suggests, perhaps three of the biggest concerns about cloud computing, which have the potential for hellish consequences, are security, privacy and its impact upon eDiscovery.

Do you know where your data is?

One of the drawbacks of litigating in the cloud is that you necessarily are relying on a third party to maintain and control your data. It is therefore critical to understand the implications

of moving your data to the cloud. Once there, who has access to it? Who can alter it?

The very idea of handing over important and potentially sensitive or proprietary data to another company understandably worries a lot of people. Corporate executives might well hesitate to take advantage of a cloud computing system because they cannot keep their company's information under lock and key, restricting access in the same ways as today. The counter-argument to this position is that the companies offering cloud computing services live and die by their reputations and their ability to entice clients to renew their service agreements. Just as with Internet website hosting providers, it benefits these companies to have reliable, documented security measures in place. Otherwise, the service would lose all of its clients. In short, it is in their best interest to employ the most advanced techniques to protect their clients' data.

However, even the best of reputations cannot protect cloud computing companies from the ravages of a stormy economy. As one commentator recently noted, "[o]nline storage sites, the toast of the Internet circa 2006, are shutting down in droves, putting the data and images of their users in jeopardy." Tom Spring, "Will Your Data Disappear When Your Online Storage Site Shuts Down?" (PC World, May 14, 2009). Alarming, these are not all thinly-capitalized ventures. On the contrary, "[o]nline storage services that have announced closings in the past ten months include big names in tech: AOL (Xdrive and AOL Pictures), Hewlett-Packard (Upline), Sony (Image Station), and Yahoo (Briefcase)." *Id.* Especially in these instances, lack of control over the physical status of your data and processing can raise serious data protection issues.

Hey, you! Get off of my cloud!

If a client can log in from any location to access data and applications, it is possible that

the client's privacy could be compromised. That can pose a huge headache for highly-regulated industries.

For example, the Gramm-Leach Bliley Act ("GLBA"), was passed in 1999 and provides a framework for the affiliation of banks, security firms, and other financial service providers. Three provisions define the privacy provisions of GLBA: (1) The Financial Privacy Rule, 15 U.S.C. §6801, et seq., which requires that financial institutions provide customers with notice at the time their financial relationship is established explaining what information is collected about the customer, where that information is shared, how the information is used, and how that information is protected; (2) The Safeguards Rule, 15 U.S.C. §6801, et seq., which requires financial institutions to develop an information security plan for protecting customer information; and (3) The Pretexting provisions, 15 U.S.C. §6821, et seq., which requires financial institutions to protect unauthorized access to customer information by individuals without access authority. The GLBA specifically names executive officers as personally responsible for misuse of personally identifiable information and imposes fines for non-compliance. Through implementation of various access and security controls, the goal of the GLBA is ensuring the integrity and confidentiality of customer information. Auditing and logging access to certain data is a critical aspect of compliance with GLBA. Systems must be designed to carefully log information in order to construct a clear audit trail because tracing the access patterns of users may uncover illegitimate data use. Questions about the ability of cloud environments to properly log access data to maintain clean audit trails remain. Until these questions are answered, banks and other financial institutions should approach the shift to the cloud with caution.

In certain other cases, regulatory compliance may be impossible if your data is subject to any geographical storage restrictions,

such as the EU Data Protection Directive, Directive 97/66/EC. This directive disallows the transfer of data to third countries (countries outside the EU) that have not adopted all provisions of the directive. While there have been some attempts to institute safe harbor provisions for "third countries," there are still questions about the level of data security in the United States. Without the ability to freely transfer data to data centers located in the United States and around the world, companies may be unable to take full responsibility for certain data (since, of course, the principle behind the cloud is that customers don't need to know or care where their data is). These types of regulatory restrictions may prohibit your company's transition to the cloud. In any event, cloud computing companies will need to find ways to protect client privacy in many environments.

Searching in the clouds.

One of the cost benefits of cloud computing is due to the fact that your company's data is not specifically mapped. Yet, over the past several years, clients have been instructed by counsel and consultants alike that electronically stored information (ESI) maps are a critically-important tool when it comes to eDiscovery preparedness. If a company chooses to move to the cloud, ESI maps will become a thing of the past. The locations of your data will be an unknown and may be on a server/hard drives with other companies, stored without any sense of order (remember, your company essentially buys space like a commodity). Your cloud vendor doesn't necessarily know "where" your data is, but merely has the power to "retrieve it." Part of this shift is the initial obstacle of navigating regulations about where and how your data must be stored and understanding your preservation and discovery obligations as a party to litigation.

Preservation: lassoing a cloud.

The Federal Rules of Civil Procedure require disclosure of all non-privileged "documents" and "electronically stored information" in the party's "possession, custody, or control" that may be sued to support that party's claims or defenses. Fed.R.Civ.P. 26(a)(1)(ii). Once your data is the cloud, is it technically in the possession and custody of your third party vendor? Even if so, who has "control?" The Federal Rules also allow adversaries discovery regarding any information potentially relevant to the claims and defenses at issue, including "the existence, description, nature, custody, condition, and location" of any such documents. Fed.R.Civ.P. 26(b)(1). If your data is no longer controlled in-house, will cloud computing providers be able to implement your company's general document retention policies as well as litigation holds?

Parties have a duty to preserve evidence in their custody and control where it is foreseeable that the evidence may be relevant to threatened or pending litigation. Specifically, parties are under a duty to preserve what it knows, or reasonably should know, is relevant to the litigation, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request. The failure to obtain and preserve evidence or destruction of evidence may result in serious sanctions, including the imposition of attorneys' fees and costs, exclusion of evidence, adverse inferences, in cases involving bad faith spoliation, even dismissal of the action or default judgment.

The documents, information or other potential evidence must be in the party's possession, custody, or control for any duty to preserve to attach. If your company is "movin' on up" to a deluxe data center in the sky and effectively handing over your data to a cloud computing provider, will your company still be considered to have custody and control

over that data? Probably, yes, because control has been construed very broadly. Generally, under Fed.R.Civ.P. 34, "control" does not require that the party have legal ownership or actual physical possession of the documents or data at issue. Rather, documents are considered to be under a party's control when that party has the "right, authority, or practical ability to obtain documents from a non-party to the action." See *In re NTL, Inc. Securities Litigation*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (internal citations omitted). Thus, courts considering the issue of custody and control in other contexts have found that parties cannot relieve themselves of their preservation and production responsibilities by handing over documents or data to third parties if litigation is reasonably foreseeable. For example, a company that relinquishes control over relevant evidence in the context of asset sale will not be relieved of its responsibility for preservation of those transferred documents. If the third party subsequently destroys any relevant documents or data, your company is still responsible. See generally *Centimark Corp. v. Pegnato & Pegnato Roof Management, Inc.*, No. 05-708, 2008 WL 1995305 (W.D.Pa. May 6, 2008). Similarly, a federal court confirmed last year that the obligation to preserve and produce electronically stored information cannot be avoided merely "through the simple expedient of storing it with a third party." *Flagg v. Detroit*, 252 F.R.D. 346, 347 (E.D. Mich. 2008).

In another example, *Columbia Pictures Industries, et al. v. Justin Bunnell, et al.*, the defendants were involved in litigation concerning possible copyright infringements. No. CV 06-1093FMCJXC, 2007 WL 2080419, at *1 (C.D.Cal. 2007). Plaintiffs filed a motion asking the court to order the defendants to preserve and produce certain server log data. *Id.* The defendants opposed, contending that the server log data was not within their possession, custody, or control as defined in Fed.R.Civ.P. 34(a)(1). *Id.* Critical to the litigation was certain log server

data. While the defendants did not affirmatively retain the server log data, the data was stored in the random access memory ("RAM") of the defendants' website server for approximately six hours. *Id.* at 3. At some point in time, the defendants altered the method through which their website operated. *Id.* In order to increase the processing and delivery of the content on their website, the defendants contracted with a third party vendor. *Id.* Consequently, the defendants' server log data was routed to the vendor's servers located geographically proximate to the users making the requests. Because the "defendants have the ability to manipulate at will how the Server Log Data is routed", the court held that the defendants were in possession, custody, and control of both the data that had been formerly temporarily stored in the defendants' website's RAM and the data which was being routed to the third party vendor, and ordered to produce the data. *Id.* Furthermore, the court noted that the data in issue may have been within the defendant's possession, custody, and control by virtue of the defendant's contractual relationship with the third party vendor. *Id.* at 3.

As these decisions indicate, courts are not willing to relieve parties of their preservation and discovery obligations simply because data is in the possession of a third party vendor. Consequently, if your company is contemplating a move to the cloud, understanding how your cloud computing vendor will work with you during litigation is critically important.

Are the clouds reasonably accessible to mere mortals?

Under Fed.R.Civ.P. 26(b)(2)(B), a party need not produce discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. If a company chooses to store its data "in the clouds," how accessible will the data be? How will it make a showing that

the clouded data is “not reasonably accessible”? If your data is no longer “reasonably accessible,” how will a court respond? Courts will likely not look kindly upon a party who appears to have affirmatively made their ESI inaccessible. Under the rule, moreover, if the opposing party makes a showing that the discovery is necessary, a court nevertheless may order discovery from the “inaccessible source” (in this case, the cloud), with no guarantee of cost-shifting.

In *W.E. Aubuchon Co., Inc. v. Benefirst, LLC.*, for example, an employer, sponsor, and administrator of employee medical benefit plans covered by ERISA brought action against plans’ third-party administrator, alleging it breached its fiduciary duties. 245 F.R.D. 38, 40 (C.D.Cal. 2007). The third-party administrator, BeneFirst, moved for reconsideration of the discovery order that it produce all medical claims files in its custody or control. *Id.* At the time of the order, BeneFirst was no longer in operation. *Id.* at 41. As a result, BeneFirst would have had to hire personnel to retrieve the claims sought by the plaintiffs. *Id.* Also, for parts of the relevant years, BeneFirst used an outside vendor to process its claims. *Id.* Furthermore, BeneFirst’s files were not indexed in any way and could only be searched by date. *Id.* Due to the lack of search criteria, BeneFirst claimed that the documents were not reasonably accessible because the cost of their production would far outweigh their value to the plaintiffs. *Id.* at 41. BeneFirst estimated it would cost approximately \$80,000.00 and take almost 4,000 hours to retrieve the requested documents.

The district court held that “... the records sought by the Plaintiffs are stored on a server used by BeneFirst in Pembroke Massachusetts, which is clearly an accessible format. However, because of BeneFirst’s method of storage and lack of indexing system, it will be extremely costly to retrieve the requested data.” *Id.* at 43. Because of this expense, the court found that the retrieval would involve an undue burden or cost. *Id.* Accordingly, the court held that the

images were not reasonably accessible within the meaning of Fed.R.Civ.P. 26(b)(2)(B). *Id.* However, because the plaintiffs’ document request was specific, the documents requested had been narrowed and the documents requested were clearly an integral part of the litigation, the court found that the plaintiff had shown good cause and ordered production of the materials at BeneFirst’s own expense. *Id.* at 44.

As illustrated above, it is important to know how your cloud computing provider can assist you in parsing out your information. Will the cloud computing provider be responsive to discovery requests and subpoenas? And what about legacy data? When using cloud computing storage, does data ever get “archived” in the traditional sense – is old data just as accessible as new data?

Admissibility of clouded data.

Both courts and legal practitioners have emphasized in recent years, particularly when dealing with electronically stored records and information, that the rules of evidence require that they be authentic and reliable in order to be admitted as proof of a matter. *See, e.g., Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007); *In re Vinhnee*, 336 B.R. 437 (9th Cir. 2005). But how can the authenticity and reliability of clouded data be established effectively? The question demonstrates that “[i]t is vital to assuring the long-term success of cloud computing that information security management be a strong feature of the varied service agreements, in order that the records and information in the custody and control of the service provider align to the standards for authenticity and reliability required by their customers and the surrounding legal environments.” *CSA, Security Guidance*, at 41.

Finally, a great deal of litigation involves the forensic examination of hard drives and other storage devices, specifically when companies are

dealing with spoliation allegations. Will it be possible to investigate evidence of inappropriate or illegal activity in the cloud? Some seriously doubt it. A 2008 report by Gartner Consulting warned that: "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation – along with evidence that the vendor has already successfully supported such activities – then your only safe assumption is that investigation and discovery requests will be impossible."

Future is Cloudy, Please Ask Again Later.

Plainly, the potential benefits of moving to the "cloud" are enormous. However, the risks, eDiscovery challenges, and security issues are also very real and show that much work has yet to be done before the cloud will be a safe place to dwell. Companies would do well to carefully consider whether their circumstances truly make it advantageous for them to move their data or functions into the cloudscape, either in whole or in part. It may be wise to first test the waters with less critical data or operations before jumping without a chute.

For those companies that do decide to ascend into the cloud, experts advise that they should first closely scrutinize their SaaS vendors' security and privacy practices, data protection and segregation practices, and authentication and access control procedures. Users of cloud services will also need to insist on service level agreement (SLA) terms with their providers to ensure legal and regulatory compliance, searchability, demonstrable customer care (security), provably persistent data integrity and reliability, and demonstrable storage security and integrity for electronically stored information

in the cloud. It may be, after all, possible to comfortably live on Cloud Nine.

About the Authors

Hope Haslam is a Principal with UHY Advisors FLVS, Inc. based in Dallas. She serves as the Director of the firm's Corporate eDiscovery Group. Ms. Haslam has been involved in the discovery and electronic discovery space since its infancy. She earned her Juris Doctorate in 1991. She focuses on helping corporations address electronic discovery issues.

Douglas Herman is a Managing Director with UHY Advisors FLVS, Inc. based in Chicago. He leads the firm's eDiscovery & Digital Forensics Practice Group. Doug has an MBA, MS in Computer Science and is MCSE and MCDBA certified. Doug focuses on litigation issues and has served frequently as an expert witness.

Dara Chevlin Tarkowski is an associate with the law firm of Katten Muchin Rosenman in Chicago. She concentrates her practice in litigation matters and is an active member of the Firm's Electronic Discovery Practice. She is admitted to practice in Illinois and before the U.S. District Court for the Northern District of Illinois. Ms. Tarkowski earned her Juris Doctor degree, cum laude, in 2007.

Martin T. Tully is a partner in the firm Katten Muchin Rosenman in Chicago. Mr. Tully is a veteran trial lawyer with comprehensive, national experience in complex commercial litigation. Mr. Tully is the national practice chair of the firm's Electronic Discovery & Evidence Practice and has counseled various clients on eDiscovery preparedness and compliance. He is also a frequent speaker in the areas of e-discovery and digital evidence.