We understand you were ranked number one in a national survey, New York Law Journal and were named as a Relativity Orange-Level Best in Service partner.

Bendel: CDS Legal is an end-to-end e-discovery service provider with one of the largest e-discovery footprints in the U.S. Our clients range from the very large to the very small, and our services include collecting, organizing, reviewing and distributing electronically stored information (ESI). We are experts in more than 25 e-discovery tools, including our proprietary cloud-based review platform, Nytrix, which was just unveiled at the 2012 ILTA conference (International Legal Technology Association).

We have offices in New York, Washington, San Francisco and Chicago as well as three highly secured national data centers. Our processes have just been successfully audited under the requirements of AICPA SSAE 16, Service Organization Control (SOC) 1 Type II, which replaced SAS 70 and is an international standard.

Editor: On what discovery-related issues should increased attention be paid in the development of e-discovery solutions?

Bendel: Currently, predictive coding, social media, cross-border discovery and data security seem to be inspiring the most discussion. These issues are shaping the industry, and legal teams are concerned about their effects, particularly as they relate to controlling costs, managing big data and developing the most thoughtful approach to the e-discovery process.

Predictive coding, or technology-assisted review, has really excited interest as a recent technology aimed at reducing costs, and cases like Da Silva Moore v. Publicis Groupe have provided high-profile commentary from judges and outside counsel as to what constitutes “relevant data” and “collections.” However, no matter how good this technology may be, it is not a cookie-cutter solution in all situations.

The challenge with social media is the complexity it creates in e-discovery, similar to the impact of email just a decade ago. The question is how to manage and review social-media-generated ESI is a source of great anxiety for our corporate clients. And there are not many solutions currently available. There’s talk about “bring your own device” (“BYOD”) – a policy enabling employees to use their own mobile devices to access privileged company systems. Questions remain as to how to handle it from an e-discovery perspective, and solutions are at the infancy of development. Your e-discovery strategist can look at a company’s specific environment and help shape policies for information governance.

Editor: What legislative or judicial developments point to the need for innovation, both in terms of solutions with respect to information governance?

Bendel: The Federal Rules of Civil Procedure were amended in 2006 specifically to include the term ESI, forcing the need to address the issue. For our purposes, the most significant amendments are Rule 26, 26, 33, 34, 37 and 45. Highlighting the last three – Rule 34 affirms that all existing information is discoverable from a person, device or where it is stored, including in the cloud. Rule 37 clearly sets the way for sanctions, and Rule 45 affirms that ESI is evidence, i.e., a discoverable document.

Recent decisions such as those in Da Silva Moore and Global Compensation Landow Aviation, have supported the latest assisted-review technologies, highlighting technology and information governance entities. The message is clear: corporations must address these issues now or face the threat of sanctions.

Editor: What are the key components of effective corporate information governance schemes?

Bendel: Beyond technology, the first step is to develop a master data governance process or approach, and a critical component here is senior management buy-in. When looking at new technologies like this, one must be aware of how to ensure compliance, as the price of technology always does over time, a corporate policy of saving everything doesn’t work and merely creates a mountain of information to store and manage.

Companies should establish an IT steering committee to develop a comprehensive map of the IT system. As companies grow and employees come and go, many corporations lose track of information, and even companies that keep track don’t systematically understand what it means. So in addition to the urge to collect everything, companies need a remediation strategy that is uniform and can formalize the process of eliminating information from their systems. Proper remediation is even more critical in companies that are being merged or acquired to ensure consistency across the company and individual business units.

Bendel: To comprehend that there is no legal requirement to save all data, unless and until data relates to an imminent litigation, a company enters the picture. So it’s an expansion on that. We work with large storage companies – such as EMC – which are responsible for managing and indexing data. Such data processing enables intelligent searching toward producing relevant documents during litigation.

Most existing technology focuses on the data archiving stage, so corporations that don’t have a formal information governance policy naturally will feel obliged to save everything and worry later about data de-duplication, reducing and otherwise processing it. We are now seeing more analytics technologies that actually crawl through and index the data, enabling better and more cost-effective business practices around information governance.

Editor: What are the key elements of data security and privacy policies that enable companies to engage productively in e-discovery in cross-border disputes?

Bendel: Multinational corporations doing business in the U.S. face a unique dilemma whenever they are up against compliance with a Rule 26 discovery obligation. Do I comply with U.S. preservation and production demands but face potential violations of local laws and regulations where non-U.S. relevant data resides, or do I fully comply with the non-U.S. legal framework and risk sanctions from a U.S. court?

Any data security or privacy policy should be firmly grounded in a respect for the history underlying non-U.S. legal frameworks. Cross-border companies have developed an adequate protection of personal and corporate data as required by the EU Data Protection Directive. In the U.S., employee data is property of the employer, whereas in the EU, this data belongs to the employee and is subject to strict privacy laws. Custodians in the EU have to collect and filter data locally, and individuals have the right to opt if the data is private and they don’t want to share it. That’s the framework of Safe Harbor compliance.

Internationally, discovery processes must support a party’s claim or defense in order to minimize conflict with data privacy laws and their impact on custodians. As a result, CDS Legal created a technology called Digital Customs, which essentially is a mobile unit that can process data in a secure environment that is not in any one company’s infrastructure. For example, a German company hired us to identify, collect, process, culled, review and load data into its facility, but still detached from its local infrastructure, thereby preserving data privacy and security.

A similar situation in the U.S. would have found us connecting directly to the company’s infrastructure, performing a targeted collection, then processing data for processing outside the facility. With the German company, we removed unprocessed data from the network and loaded it into our appliance. We worked with the IT director to collect the data internally and with the international compliance officer to make sure we had access to information from custodians. Next, the general counsel reviewed and approved the results, which were then exported to the U.S. for review and production.

Our Digital Customs product really differentiates CDS Legal in allowing us to disengage from the company’s systems – we never touch its infrastructure – which adds a substantial layer of security and objectivity to the process. The German client was very happy with the service and the results.

Editor: Should companies consider using e-discovery service providers to help more broadly with litigation readiness and cost control?

Bendel: The right e-discovery expert can provide results-driven solutions that map how to manage risks, reduce costs and build a standard process before a complaint is even filed. Today’s e-discovery strategists delve into detail to determine the specific needs of a case to produce relevant documents most useful to human review and production. Practically speaking, and really in all cases, our clients want policies that are auditable and forensically tested for effectiveness in actual situations, such as when a court issues a pretrial order, produces a litigation hold letter. Also, document retention and destruction policies must be standardized, reviewed and monitored on information relevant to the business.

Editor: What does it mean for an e-discovery service provider to be compliant with the U.S. Department of Commerce U.S. Safe Harbor Framework (“Safe Harbor”)?

Bendel: Compliance with Safe Harbor Frameworks and international frameworks have developed to provide an adequate protection of personal and corporate data as required by the EU Data Protection Directive. In the U.S., employee data is property of the employer, whereas in the EU, EU

Please email the interviewee at gbendel@cdslegal.com with questions about this interview.