Deloitte.

Discovery insights

5 questions about emerging digital threats to eDiscovery

An interview with Patrick McColloch, Director, Federal Discovery, Deloitte Transactions and Business Analytics LLP

The march of technology continually increases the potential sources of and challenges associated with discoverable information in legal matters. Electronic data exists in ever-evolving forms, from spreadsheets and emails to texts, and social media posts, quite possibly sent from a mobile device or stored in the cloud. Today, the same issues that attorneys face in acquiring such data during discovery could soon arise with data generated through other sources, including from an array of new technologies that seemingly come on line every day.

What are some of the new and emerging technologies that will affect litigation?

The "Internet of Things" (IoT) is one of the most recent, combining sensors and communications technology to continually connect devices to the Internet and one another. It enables the creation, sharing, and analysis of information, usually about the connected device's use, largely without human intervention. Health and fitness trackers, thermostats, appliances, truck fleets, and industrial controls are among the myriad and growing array of IoT-enabled devices and equipment. As one example of how the IoT might be a discovery target, consider a set of sensors installed along a river to monitor for water pollution. Data generated by these sensors could be important in an environmental action brought against a company or a government authority.

"Big data" is another relatively recent phenomenon that continues to impact legal discovery in a significant way. With data being generated in such large volumes and from so many sources both within and surrounding government agencies, traditional information systems can no longer keep up. New, more powerful, and highly sophisticated tools and techniques for data analysis come on the scene each year for a variety of purposes, from homeland defense to operational effectiveness to customer experience. A close-to-home example for litigation attorneys is technology assisted review, or predictive coding, in which teams of human attorneys are largely replaced by computers and "machine learning" analytics software that enable amazing efficiency gains and speed in the review of the giant data sets often present in today's litigation.

Are there any other trends that counsel should be aware of?

There are two other trends within information technology that counsel should also be aware of, regardless of being either commercial or government. The first is “Shadow IT”. As the promises of cheaper, faster and more robust cloud service offerings have started to become realized, this has created an environment where with a credit card and phone call or click of the mouse someone can standup a new infrastructure in the cloud in hours. The possibilities are limited only by imagination…..email servers, document sharing platforms for collaboration and storage, even e-discovery tools. Many times these systems are not inventoried in the CIO’s catalog, yet they may contain vital information responsive to a litigation matter. Even if they are inventoried and known to exist, the extent to which the data is under the owners control for preservation and collection purposes is further complicated.

The second trend is the growing presence of bring your own device or “BYOD”. In a BYOD environment, the agency or company is allowing individual users to access and potentially download or store data on devices that do not belong to the agency. Common issues such as “how do we know where all to look for data” “how can we preserve data” “who has this data” is now exponentially multiplied.

What issues may counsel face in adapting these emerging technologies into discovery?

New technologies that create so much discoverable data, whether structured or unstructured, present new issues when it comes to discovery and litigation. For instance, a key consideration for IoT is data management, starting with identification of sensor locations and what data those sensors can provide. Depending on the application, some sensors may only send anomalous data – triggered when something out of the ordinary happens – while others transmit data continuously, such as the sensors along the river as described above. Also, as with other types of data, spoliation claims are possible. Once it is established that sensor data needs to be collected and analyzed in a case, it is the attorney’s job to ensure the data is preserved. Working cooperatively with IT, the team must ensure that old data is not being discarded or overwritten, and new data continues to flow and be preserved as well. After analyzing the data to determine relevance, the team must also decide whether to produce the raw data, produce a summary report, or perhaps even produce the sensor. IoT data may also become subject to Freedom of Information Act (FOIA) requests. And, of course, the IoT’s potential impact on information privacy and security will be an ongoing priority.

Information security and privacy are other growing concerns. For example, consider the growing use of smart phones for social media, texting, and remote control of devices in homes, offices, and automobiles. What happens if a person is in Europe or Asia on a business trip and he or she is watching security footage from their home or office in the US? Could legal issues arise around that? Or what if a court case involves a business traveler, and part of the dataset that the litigating attorney is looking for is from the person's smart phone and apps that were used overseas? First there is likely to be a question about where the data resides and how it can be accessed for discovery purposes. There could also be issues with strict data privacy and security laws in various governing access and movement of the data across borders. Then there is the issue of security – once litigators have access to the data, is it handled in a secure way that prevents cyber attack or inadvertent access to unauthorized persons? These types of questions are coming up with increasing frequency, and counsel at least needs to have some familiarity with them going forward.

How can counsel help their agency better understand the potential impact of new and emerging data types on litigation and promote a strategic approach to it?

Counsel has a key role to play in championing the treatment of data as a strategic issue with stakeholders beyond the information technology (IT) department and information security function. Those organizations are not likely to be as attuned to regulatory and legal issues, and they may not think to ask about them. At the same time, legal doesn't always know what the technologists are doing. Educating executive management about the potential relevance of new data types as they are brought on line by the agency, is especially important; dealing with litigation may not be a top priority for them at the moment, but that obviously could change overnight. And, amid tight budgets, informing leadership about potential issues related to discovery could have a major influence on crucial funding decisions.

What can counsel do to increase their own awareness and understanding of the new data types potential impact on legal proceedings and litigation planning?

When cloud computing emerged as an attractive option for data storage and processing, many organizations entered into provider contracts without considering the potential need to later collect and produce data for litigation and other legal purposes. Similarly, field engineers could install IoT sensors in an assortment of devices and processes, and not think to bring legal into the loop. Legal may not use the sensor, but eventually it may have to deal with whatever the sensor puts out. Because of this, it is as much a stakeholder in IoT implementation as IT, records management, and the field engineer who installs the sensor.

The potential for disconnects makes it imperative for counsel to build relationships, stay alert to possible developments, and keep discovery concerns front and center as plans unfold. At the same time, counsel can factor these and other considerations into litigation plans, such as identifying stewards of sensor information, deciding how to collect the information, and how to make sense of it.

Are there particular considerations for counsel in public sector organizations?

Citizens typically hold government agencies and departments to a higher standard of data protection than private businesses. Also, unlike businesses that focus on what information goes out of the organization, government bodies have to be concerned about both data sent out and data coming in from outside sources. This holds true regardless of the source of the data, whether it is from email, social media, mobile devices, the cloud, or IoT.

Our take: New data sources emerging trends demand increased awareness and understanding of the dimensions they add to discovery

Counsel may not have a direct involvement in how an emerging technology like the IoT, cloud computing and BYOD can improve medical care, a transportation system, an energy grid, or an industrial process. However, legal does have a central role in making sure information from emerging technologies is handled responsibly, legally, and in compliance. By staying abreast of the expanding scope of the these issues and actively participating in decisions around the use of this – and other – emerging technologies, counsel can help the organization be prepared when someone asks about that sensor down by the river.

Contact

For more information, please contact:
Patrick McColloch Director | Deloitte Advisory
Deloitte Discovery
Deloitte Transactions and Business Analytics LLP
pmccolloch@deloitte.com
+1 703 236 3050