

The Communication Gap Between IT and Legal: Real-Life Blunders and How to Learn from Their Mistakes.

BY PAT PAT MCCOLLOCH, BILL DETAMORE AND CHRIS KNOX

This article appeared in the July 2007 issue of *E-discovery Advisor magazine*.



The last time the Federal Rules of Civil Procedure were amended to address electronic data, the internet, cell phones and even personal computers did not yet exist. With the recent explosion in Electronically Stored Information or “ESI”, the need to address e-discovery in a modern context was paramount. The Federal Rules finally caught up with the changing times with several new rules addressing ESI that became effective on December 1, 2006. This is not surprising given that most industry studies over the past decade estimate that 95 percent or more of all information resides in an electronic form.

One of the paradigm shifts the new Federal Rules has brought to the discovery phase of litigation is that IT and Legal, two departments with seemingly very different goals, backgrounds, approaches and even language, are now being required to work together as a team. If IT and Legal do not communicate, coordinate and operate in unison, the organization loses control over their information, wastes valuable resources, or even worse, faces sanctions and fines for not properly responding to requests for production. More often than not, the failure of the organization’s technology department to understand how counsel intends to use the requested information; and counsel’s failure to understand the form with which the data can be harvested and programmatically manipulated leads to higher costs and less persuasive evidence at trial.

Let’s face it; IT and Legal have different DNA. They have contrasting backgrounds, training, and terminology. However, as stakeholders in their organization, they must work together to bridge the communication gap wherever possible if they hope to manage the complexities of electronic discovery. When miscommunications occur, they usually result in unnecessary time and expense recreating or organizing information that

already exists within the client’s systems. This information is extremely valuable since it can be manipulated or reused in a variety of ways to support the both ongoing and future legal claims.

To illustrate the why it is critical that IT and Legal speak the same language; we have compiled three true stories:

Unnecessary Effort and a Weaker Argument

An organization is sued for fraudulently inducing customers to buy certain products or services. The plaintiffs’ theories are varied and the alleged deceptions took many forms (inter alia unscrupulous sales representatives, misleading advertising, failing to honor contractual rescission rights). The organization’s sales and marketing units track activities with its customers including advertising campaigns, telephone calls, mailing campaigns, and other contacts with prospective customers. That data exists within CRM and sales automation applications.

Defense counsel would like to present evidence that the allegations asserted by plaintiffs were, even if true, isolated, and certainly not a common business practice. In order to do so, the attorneys meet with the technology staff supporting these applications and request certain information to rebut the plaintiff’s claims. The supportive IT staff (under direct orders from the CIO to provide highest priority support, “whatever information the lawyers ask for, make sure they get it”) dedicates resources to customize reports for the lawyers and provides those reports containing all of the requested information in the format requested by counsel. Trial counsel takes those reports, and manually enters certain information into a database application created especially for the litigation in connection with the organization’s expert.

This resulted in unnecessary labor to manually enter the information as well as a high risk of inaccuracy. Both could have been avoided if the selected data had been exported from the CRM and sales automation applications and imported into counsel's database in an automated way. The client's review of this matter (with someone who understood the data structure of the CRM and sales automation applications and counsel's legal arguments) confirmed that the data could have been collected and organized with some minor programming at a savings of \$140,000. Moreover, there was other information that could have supported the defense theories in the case.

Here, because of less than complete understanding between the lawyers and IT (even with the best of intentions), the organization spent more than it should have and developed a less persuasive case

Avoiding a \$12 million IT bill

With the advent of large corporations outsourcing their IT management and support, the risk is potentially magnified even more. The IT vendor typically has goals that are fairly straightforward: Keep the client's systems up and running, and if something goes down bring it back up as soon as possible. These black and white extremes can at times get lost in the greyer world of discovery. In this real example, a Fortune 200 healthcare provider found itself needing to produce emails for ten custodians for a period of 2 years. The company was creating daily back-ups of their 20 separate Microsoft Exchange servers, and their retention policy, combined with various litigation holds, resulted in the existence of roughly 12,500 back-up tapes for their email systems alone. At the time, the company was engaged in a multi-year agreement with a Fortune 100 IT solution provider to handle all IT infrastructures.

Legal immediately contacted the IT provider and requested the restoration of all 10 custodians' email for the previous 2 years. IT departments are typically set up to handle desktop support as well as network disaster recovery. Naturally, their solution to this request included the restoration of all Microsoft Exchange environments to an online 'live' format so that the 10 individuals' mailboxes could be searched. This approach would have required approximately 500 Terabytes of storage space (500,000 Gigabytes). The resulting quote was \$12.48 million!

There were two vital holes in the communication between Legal and IT. First, Legal simply requested the restoration of the custodian's email. IT personnel can often be quite literal, and heard this request as a need to recreate their live Exchange environment for all 20 Exchange servers. Microsoft Exchange backups contain a backup file (EDB) which can be read and searched without having to recreate the entire Exchange environment. This process enables the restoration of individual mailboxes without the need to restore the entire environment. Due to the decrease in complexity as well as online storage, this approach would cost \$3.1M, or roughly 75% cheaper than the original quote by the IT provider.

In addition to the miscommunication about how the email was to be restored, Legal was unclear of the scope they wished to cover. As mentioned, the company was creating daily backups for all employees. Daily backups on email servers are extremely duplicative. Only added or deleted email would change on the back-ups on a daily basis. At the time, the company was not enforcing any mailbox limitations, so employees had no reason to delete email from their mailbox. Given this scenario, it was possible to sample the backups on a monthly basis instead of daily. An index was provided by IT for the backup tapes and was used to narrow the focus to a small sub-set of tapes. This approach added a very small—but ultimately acceptable—risk that an email sent, received and deleted within the month would be missed but decreased the cost of the project to about \$1.1M, less than 10% of the original quote from the IT provider.

When is a backup not backed up?

Finally, consider the case of a large government agency that was defending itself in a Title VII case. The request for production was quite broad and the universe included all e-mail and other ESI pertaining to the human resources department. The time period in question was long enough that some earlier proprietary e-mail systems had been in use and therefore much of what is known about today's systems such as MS Exchange were not necessarily valid. During the first several attempts by Legal to request backup tapes of the e-mail systems, the IT Department stood firm in its conviction that backups "did not exist". Some members of the legal team who asked this question over the weeks simply attributed this answer to the long timeframe

involved and the proprietary nature of the system. In the opinion of Legal, they had been told that backups did not exist. It was not until the IT Manager was asked the fifth time about this issue when he finally replied “Why would we make backups of the system when every single message that comes in or goes out is automatically copied off line to tape.” In other words, the IT Department was not running a specific “backup tool,” but in fact was saving the data in an even more usable format! However, the legal team had continually asked for “backups” without explaining that their ultimate goal was to know what all old messages existed and therefore potentially needed to be reviewed. In the end, more than 5 million messages were recovered to be potentially analyzed to support the defendant, resulting in a much more comprehensive data collection.

Through these examples, as well as the multitudes of others that continually come to light in the reporting of e-discovery cases, it is clear that miscommunications between Legal and IT can pose a very real danger with potentially high consequences. Risks include not having the proper information to launch a strong defense; increased litigation support expenditures due to inefficiencies and/or errors in collection; as well as sanctions and fines for spoliation or the court concluding that the firm did not undertake collection of ESI in a good faith effort. The good news however is that it does not have to be that way.

By employing the services of a team experienced with the e-discovery process, these landmines can be avoided or at least mitigated. In advance of any litigation (or as early as possible after filing), it's critical to prepare a

discovery management plan, created by a multi-functional discovery management team. The team should have input from the various stakeholders including litigation counsel, support staff, and information technologists to conduct a thorough analysis of the issues. To be most effective, this cross-functional team should:

- ▶ Perform an inventory of all ESI information stores. Know where your e-mail, CRM, Accounting, HR and other important data are stored and how it is managed. This inventory should be conducted under the direction of the E-Discovery Team.
- ▶ Develop standards and procedures for important discovery tasks such as implementing litigation holds, ESI collection and preservation; as well as processing. Documented standards that can be referenced by all of the players can go a long way in avoiding miscommunication between Legal and IT.
- ▶ Communicate clearly and often. Make an effort to understand the language of the other stakeholders. Don't just tell them what you need. Tell them why you need it and how you are going to use the information.

Frequently, both IT and Legal think they are communicating clearly. The challenge is that each person communicates in a way that is unique to their industry, their job function and their prior experience. In other words, one man's “backup” may or may not equal another man's “copy.” The best strategy is to tell the other stakeholder what you need and why.