The Stunning Impact of E-Discovery on IT
By Peter S. Vogel

Since more than 95 percent of all information is electronic and it’s estimated that upwards of 97 billion emails are sent each day, it is no wonder that every lawsuit has electronic evidence. All IT shops protect themselves from disaster with the knowledge that every computer will fail, but computer systems are not designed to provide easy access for lawyers and judges.

In today’s world, it is no wonder that every lawsuit has electronic evidence. Unfortunately, for the most part, lawyers and judges do not understand IT or the Internet. As a result, litigation generally misses the mark regarding what is now referred to as “ESI,” or electronically stored information. It is in your best interest to learn more about the legal issues regarding e-discovery to be prepared, since surely everyone reading this article will be impacted in the future, if not already.

Litigation in the United States is controlled by state or federal court systems, or, alternatively, by private arbitrations governed by the rules of the American Arbitration Association — or some other organization, like JAMS, which is a leading private alternative dispute resolution (ADR) provider.

Most people are familiar with the trial system because of television and movies, but are unfamiliar with arbitrations in which the hearing (rather than trial) is conducted by non-judges of one to three panel members (most often lawyers, but sometimes industry experts).

IT has become an integral part of the search for ESI in virtually every lawsuit, but lawyers do not always know what to ask or, even worse, how to interpret the answers received back from IT. So, this article will give some advice about what IT needs to be aware of in order to be prepared.

What Is Discovery?
Generally, after a lawsuit or arbitration is filed, there’s a period of time referred to as “discovery” that extends to just before the trial or hearing. Simply put, this is a time when each party of the suit has a chance to ask questions of the other parties. Each side is entitled to inquire about the claims and defenses, so that when the trial occurs there are no surprises. In fact, if a party withholds information, it may be penalized by losing the trial — or a mistrial may be called by the judge or arbitration panel. The evidence that is collected in discovery is used at the trial or arbitration hearing to prove or disprove specific claims.

There are four primary categories of discovery:
- written questions referred to as “interrogatories”;
- requests for the production of documents and things;
- requests for admissions; and
- oral testimony called “depositions.”

For the most part, there are limits on each category, but since ESI is fundamental to every lawsuit today, it is best to have a basic understanding of each type. Interrogatories, document requests, and requests for admissions usually include definitions, and in today’s world, they mostly detail IT or Internet issues related to the dispute.

The types of discovery requests included in interrogatories regarding ESI can include items such as these: “Describe the procedures for daily backup of the email system”; “When did you start using Google Analytics to measure traffic on your Website?” or “List all employees who had passwords to the Oracle Financial database from January 20, 2003, through May 9, 2005.” Under most procedures, the responding party has 30 days to send its answers or objections to the questions posed, all of which can be challenged for completeness or accuracy.

Document requests may include a request for all emails from certain individuals during a defined time period; all reports from a certain financial system; or copies of correspondence between specific individuals or departments. Under most rules, the guidelines for producing answers to requests state that these documents be produced in their native electronic format rather than in paper, tiff or pdf.

Parties are not required to create items that do not exist, but ESI is different from paper, tiff or pdf, so the ability for IT to respond to these document requests requires an understanding of the issues in the litigation, strategies for your business, and defenses to claims of the other side.

Requests for admissions are exactly that; one side sends the other a series of questions that they either admit are true or deny — for instance, “Admit or deny that all emails sent by Jane Doe were not saved between June 27, 2001, and September 10, 2003”; “Admit or deny that John Doe broke through the firewall and stole financial records on December 6, 2004”; or “Admit or deny that Richard Roe was fired without cause.”
Depositions under most state and federal rules are limited to six or seven hours, during which individuals are asked questions before a court reporter (maybe a video camera as well) with lawyers representing each party present. Questions in depositions can be far-ranging, and the lawyers cannot really coach the deponent (the person who is answering the questions). However, since few lawyers really understand IT, even if they ask IT deponents questions, they may not understand a technical answer, so logical follow-up may not occur. Sometimes lawyers will bring their IT experts to depositions so they can coach the lawyers about probing IT issues. Under the discovery rules, an IT professional can be deposed by a category of “the person or persons most knowledgeable” about lists of things like email, backups, databases, Web sites related to the lawsuit, and the like.

Records Retention Policies
Because ESI has become fundamental to litigation, companies need to have a records retention policy; otherwise, how can a company explain to a judge why certain ESI was retained or deleted? Clearly, different industries and businesses are subject to state and federal regulations and laws that require retention of records, such as seven years for IRS (Internal Revenue Service) and 50 years for FDA (Food & Drug Administration). So every company needs to analyze what types of records it has and which need to be retained.

When you become aware that a lawsuit may occur, the records retention policy must be changed regarding records relevant to the litigation. The legal term for this is “litigation hold”; however, the rules of evidence have always required potential litigants to save evidence, and if they destroy critical evidence, they lose their case because of the intentional destruction, which is called “spoliation.”

Of course, before ESI became critical, records generally were only paper stored in file cabinets or the desks of the individuals involved in the dispute. Now, ESI is managed and controlled by IT, and as result, IT has a critical role in all litigation. The records retention policy may state that certain accounting records are retained for seven years for tax purposes, but the IT backup procedures will likely have no means to search old backup media to delete old records. Likewise, if the accounting data is part of an SQL database, it is likely that IT would not be inclined to search old records and delete out-of-date information.

Disaster Recovery
Everyone in IT knows that each computer will fail at some time. Every box has components with an MTBF (mean time between failures), so failure or disaster are a fundamental part of the use of IT. Accordingly, IT plans for these failures or disasters by doing routine backup of systems and data to avoid business interruption. As an example, when my office had a flood on the 33rd floor of our building and our data center was shut down, our business was not adversely impacted, since we had good backup procedures already in place.

IT sees backup as a disaster recovery issue; however, judges and lawyers think that copies of ESI are easily available to them since IT does backups regardless of the systems involved. As a result, before litigation — and at least by the point of litigation hold — it is essential that IT and lawyers communicate about what ESI is available, in what format, and for what timeframe.

Pivotal Cases
In 2006, the federal rules of civil procedure (and since then, many state rules as well) were changed to specifically deal with ESI. If you have been reading any reports of trials, you will know that there have been some very high-profile companies that have lost millions of dollars as a result of destruction of emails (Zubulake v. UBS), failing to provide all 14,000 backup tapes of emails during discovery (Coleman v. Morgan Stanley), or hiding more than 41,000 relevant emails (Qualcomm Inc v. Broadcom). All of these cases could have avoided such litigation disaster had the lawyers and IT been communicating.

When evidence has been destroyed (spoliated), a judge or arbitration panel can grant a verdict against the destroying party, fine the party, or issue an adverse inference to the jury. An adverse inference directs the jury to assume that the reason the party destroyed the evidence was that it was adverse to its claims in the lawsuit. Most of the time, juries will accept the judge’s instructions and agree that the evidence destroyed was damaging, which is what happened in the Zubulake and Coleman cases.

In Conclusion
Judges and arbitration panels are having to come to grips with the fact that they have to understand ESI, since every case has some critical evidence that is only electronic. However, only about 5 percent of the cases filed actually go to trial, and most litigation is settled during the discovery process.

Clearly, IT has a role in every lawsuit because of ESI. As a result, the better prepared IT is for litigation, the better things will turn out.

Peter S. Vogel is a trial partner at Gardere Wynne Sewell LLP, where he is Chair of the Electronic Discovery Group and Co-Chair of the Internet, eCommerce and Technology Industry Team. Before practicing law, he was a systems programmer on mainframes, received a masters in computer science, and taught graduate courses in information systems and operations research. His blog covers contemporary technology topics. Vogel can be reached at pvogel@gardere.com.