THE DUTY TO PRESERVE ELECTRONICALLY STORED INFORMATION

By Viggo Boserup, Esq., CEDS

As soon as a party is served with a summons and complaint, and sometimes sooner, there arises a duty to preserve evidence, including electronically stored information (ESI). This duty requires both counsel and clients to comply with any litigation hold and monitor ongoing compliance efforts.

Because spoliation – withholding or hiding evidence – goes to the heart of the litigation process and is not unlike perjury, failing to comply with the duty to preserve has serious consequences. Judges have wide discretion in assessing penalties and may impose fines or attorneys' fees. They may also give a spoliation inference instruction to a jury, as Judge Scheindlin did in *Zubulake v. UBS Warburg*: "[i]f you find that [defendant] could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavorable to [defendant]." Many of Judge Scheindlin's holdings in Zubulake have been cited in dozens of other cases and form the foundation for much of the Federal Rules of Civil Procedure adopted in 2006.

Due to the serious consequences of spoliation, counsel and their clients must ensure every effort is made to comply with the duty to preserve.

When Does The Preservation Obligation Arise?

The duty to preserve arises when there is a reasonable anticipation of litigation, such as upon service of a summons, complaint, or preservation demand letter. In Zubulake, supra, the obligation actually arose much earlier. There the court held that the obligation arose when the plaintiff filed her EEOC complaint 2 months prior to even being terminated. The court noted further that the obligation was probably triggered even four months earlier because "almost everyone associated with Zubulake recognized the possibility that she might sue." *Zubulake v. UBS Warburg LLC*. Given the wide discretion demonstrated in Zubulake and other cases citing it, counsel are advised to note the trend in the applicable jurisdiction.

Before All Else: Understand the Client's Information Systems Structure

Given its position as the first phase of any discovery plan and given the serious consequences of a failure to comply with the duty to preserve, it is important to review carefully the discreet steps required to establish a repeatable, defensible process for compliance. The first step for counsel is to make a thorough and comprehensive survey of the client's information technology (IT) systems. At the outset, then, it is critical that IT staff is brought into the picture. IT is generally in the best position to identify relevant repositories through a combination of custodian interviews, feedback, and enterprise search in collaboration with the legal team. IT can perform the required network topology and business process assessment, list key players, preserve in place where appropriate and assist with any other issues associated with putting a preservation repository in place. Counsel must also make a full independent assessment in order to obtain a clear picture of all potential technology issues. This includes the thoughtful selection of team members, including in-house counsel, outside counsel, in-house IT staff, and a point-person or liaison to coordinate all team activities.

Whom to Include

The next step is to determine who has custody of potentially relevant information. Counsel should look to those with some logical relationship to the allegations in the complaint. Documenting this process and approach is important, as the selection of key players will always be subject to scrutiny. While it is important not to omit a key player, it is equally important to restrict the group of individuals to those most likely to have the information requested.

Legal Hold Notice

Having identified the appropriate custodians, the client must issue a legal hold notice requesting that the custodian take reasonable steps to preserve potentially relevant information. There are several requirements for a legal hold notice:

This article was originally published by LAW.COM and is reprinted with their permission.

JAMS®

It must be in everyday English that does not require legal training or background to comprehend.

It must instruct both the individual custodian and the IT staff to suspend any auto-delete or auto-purge policy until the hold notice is lifted.

It should provide examples of potential locations of the information as well as the types of information being sought.

It should explain the potential liability for failure to comply.

It should describe the matter at issue sufficiently to give the reader an idea of the types of information that may be relevant and where such information may reside.

The hold notice must be followed by regular reminders, either monthly or quarterly. In addition, an individual should be designated as a go-to person for any questions.

The legal hold notice must be accompanied with a request to confirm receipt and full understanding of it, as well as a request to acknowledge willingness to comply through a method that can be tracked (usually email). In addition, the client must maintain a tracking system for all holds across all matters for any single entity.

What Kinds of Information May Be Discoverable

Discovery will seek all information that is potentially relevant to the claims and defenses in the action. They would include the following:

Email

Documents

Instant messages

Spreadsheets

Databases

Graphics

Audio recordings

Video recordings

Text messages

Voice mails

Pictures

Where Is the Information Located

In addition to work computers, personal computers, servers, smartphones, and tablets, the information may be located on devices or in places requiring special attention. Accessing social media posts might require usernames and passwords.

Since posts may be made on sites such as Facebook by someone other than the owner of the page, it must be determined if the evidence is legitimate. There also may be privacy issues to be resolved.

Information stored in a cloud server deserves special attention to ensure that metadata is preserved and for that the vendor may need to be consulted. Likewise, information stored in the cloud is not necessarily in one location and may exist across an array of hard drives, some of which may be in foreign countries with stricter laws concerning privacy.

Back-up tapes, generally deemed inaccessible when used solely for disaster recovery, may in fact be deemed accessible if actively used for information retrieval. Furthermore, even if used only for disaster recovery, if the producing party can identify the location of relevant data on back-up tapes, and it is not otherwise available, an exception may apply requiring the producing party to obtain the information from that back-up tape.

Conclusion

As the initial step in the implementation of the discovery plan, preservation is absolutely critical. The search for discoverable ESI is limited to the custodians identified in the preservation phase, and the quality and potential responsiveness of the data recovered is only as good as the response of custodians to the legal hold notice. Since information that is not retrieved or that has been deleted for failing to suspend auto-delete functions when required, there is no do-over of the many steps in the preservation phase. Once it is lost, it is lost, and as several of the cases cited have shown, the consequences can be major to both clients and counsel alike. ■

Viggo Boserup, Esq., CEDS, is a JAMS neutral based in Southern California. In addition to more than 20 years as a fulltime mediator and arbitrator, Viggo serves as a special master and referee in a number of cases involving electronic discovery. He is certified as an Electronic Discovery Specialist by the Association of Certified Electronic Discovery Specialists (ACEDS). He can be reached at vboserup@jamsadr.com or for more information, please visit www.jamsadr.com/boserup.