

The Metropolitan Corporate Counsel®

www.metrocorpounsel.com

Volume 19, No. 4

© 2011 The Metropolitan Corporate Counsel, Inc.

April 2011

Basic Steps In E-discovery Continued: Legal Hold Policies Where Information Is Within The Company, In A Cloud Or On A Social Media Site

**Mark L. Austrian
and Martin Krolewski**

KELLEY DRYE & WARREN LLP

This is the third in a series of articles providing our thoughts on how to reduce costs and bring some rationality to e-discovery. We have discussed the e-discovery plan, the e-discovery team, ESI systems analysis, record retention policies and triggering event guidelines in prior articles.¹ This article focuses on a critical planning component: legal hold guidelines. This includes legal holds not only on data within the company but also on data held by third parties (cloud computing) and data maintained by a social media service provider.

Legal Hold Guidelines

The legal hold notice is actually the first in a series of concrete steps in the document preservation process. The goal is to have a well-thought-out process without having to construct one under the pressure of actual litigation, when both in-house and outside counsel may be subject to many competing pressures. The guidelines can be constructed as a series of steps. These steps would include

1. determining if a triggering event occurred;
2. analyzing claims and defenses and key

players;

3. developing the legal hold;
4. circulating and confirming the legal hold;
5. monitoring the legal hold;
6. documenting the reasonableness and good faith of the process; and
7. termination of the legal hold.

The process by which a triggering event is determined has been discussed previously. The next step in the process begins with a meeting of the e-discovery team to analyze potential claims and defenses. With these potential issues in mind, the e-discovery team can determine which employees generate, receive or have access to potentially relevant information and/or knowledge of the dispute. This will lead to an analysis of the various locations where this information may reside (including third-party vendors), based upon the company data map and document retention schedules. Information located outside of the United States may create special problems because of data privacy restrictions.² With this information in hand, the company, usually through legal counsel, can construct, circulate an appropriate legal hold notice and work with the IT department to secure relevant ESI from destruction and stop any automatic deletion procedures.

The general structure and content of the legal hold has been described in a number of publications and cases.³ In general, the legal hold should be clearly written, describe (briefly) the dispute, explain the types of information that must be preserved, describe the category of information relevant to the dispute, emphasize that all of the information must be preserved (even if duplicated), set forth how the information will be collected and identify to whom any questions should be addressed. The legal hold might also describe the possible locations of ESI that might not be apparent, such as PDAs, and confirm that even though the ESI may be backed up on enterprise servers, it must still

be maintained on personal computers. The guidelines should contain a form of legal hold that will have to be modified to accommodate the needs of a particular matter. Legal hold notices are generally considered to be privileged but may lose this protection if claims of spoliation are made.⁴

The potential recipients of the legal hold can be placed into three basic categories: individuals with significant involvement in the dispute and/or those who have custody of relevant information; individuals who may have potentially relevant information (potential key players), and individuals who are primarily custodians of documents and have responsibility for overall records management and automatic deletion or destruction practices (IT players). With respect to the first category of individuals (the really key players), there is a suggestion in the case law that the failure to issue a written legal hold to key players constitutes gross negligence.⁵ This rule has not been adopted by any of the circuit courts and, like all e-discovery rules, this admonition may have exceptions. For example, a written hold may alert a custodian of important, but adverse or embarrassing information, to immediately delete the data. Under these circumstances a personal visit that preserves all potentially relevant information would be the better practice. This can be followed with a written legal hold. In any event, in most circumstances this most important class of individuals should be contacted following the written legal hold to insure that they fully understand and are in compliance with the legal hold. It may also be advisable for company compliance personnel to actually conduct the search of the ESI accessible to the key player. The class of key players is not static. Further investigation may reveal that a "potential player" is really a "key player." The corporation may consider circulating a questionnaire to potential key players to determine whether they might fall into the key player category.

Mark L. Austrian is a Litigation Partner at Kelley Drye & Warren. He serves on the Board of the Georgetown Law School's E-discovery Advisory Board, is a Member of the Sedona Conference Working Group on Electronic Document Retention and Production and teaches e-discovery at American University, Washington College of Law. **Martin Krolewski** is an Associate of Kelley Drye and has been active on numerous e-discovery matters.

Please email the authors at maustrian@kelleydrye.com or mkrolewski@kelleydrye.com with questions about this article.

The case law is unclear as to precisely when the legal hold should be issued. It is extremely difficult for a company to prepare properly and issue litigation holds the very first day when, for example, a complaint is filed. It takes time to identify the issues and the key players. However, the corporation should almost always immediately notify the IT players to halt automatic deletion of a broad class of information until a narrower scope of preservation can be developed.

The legal hold process must also be monitored after the initial preservation steps are taken. It may well be that as the litigation develops and agreements are reached with opposing counsel, the scope of the preservation obligations can be reduced, or that issues that were not apparent when the litigation began may become more important as time goes on.

Finally, there is no such thing as perfection in the legal hold process. Despite all of a party's reasonableness and good faith, relevant ESI may be lost. The courts have recognized this reality. However, once it is established that relevant ESI has been destroyed, the burden falls upon the company to defend its conduct in court – in the face of 20/20 hindsight. Thus, as the litigation hold process is put into place, a good business practice is for the company to prepare a memorandum detailing each of the steps taken in the litigation hold process, including the individuals to whom the hold was circulated, the timeframes, the claims and defenses considered, and the location of the ESI searched. There may be instances where the best approach is to contact opposing counsel and negotiate the scope of the legal hold once the parties become more familiar with the necessary information and where it resides. Any such agreements must be in writing.

Cloud Computing And Social Media Requirements

Today's computing involves an application running through software and accessing data that are both stored within the company. There are now, however, systems where both the application and the data are hosted on a third party's data center (e.g. Google's Gmail). This is often referred to as "cloud computing." Third parties (such as IBM, Amazon and Microsoft) can store this information on massive servers located far away from the company. Similarly, companies are making increasing use of social media as an effective marketing tool, linking groups of users with similar interests and benefiting from the diversity of opinions and observations provided by participants. Social media content can be stored on a company's server (Jive or Social Text) or by a third party, the social media service provider (e.g., Facebook and Twitter). Despite the extensive and growing use of cloud computing and social media,

companies appear to be unprepared for dealing with their e-discovery ramifications. According to a recent Deloitte Forensic Center e-discovery survey,⁶ 62 percent were concerned about e-discovery challenges posed by social media and 53 percent were concerned about e-discovery challenges posed by cloud computing.

Legal hold guidelines must cover the situation where some or all of the company's information is stored by third parties. Counsel must also recognize that companies employ hybrid clouds, where cloud resources are used to protect against unanticipated spikes in demand or for disaster recovery. The potential or actual use of these resources, as well as the potential use of social media service providers, must be considered in the creation of the data map. The relationship between the cloud computing provider and the company is generally governed by a service agreement negotiated with the vendor. While the data is typically within the control of the customer, the possession and custody resides with the service provider. The courts have held that, for e-discovery purposes and FRCP 34(a)(1), the information is within the company's "possession, custody and control."⁷ The courts have not been reluctant to order the production of the contents of social media such as Facebook and MySpace in specific cases. Therefore, social media that is relevant to ongoing litigation must be preserved.⁸ The courts have typically held that a user has the requisite "possession, custody or control" to the extent that the user can access the information on the site.⁹

With cloud computing, the problem arises when the business units negotiating the service agreement fail to consider the issues that may arise within the context of e-discovery.¹⁰ These issues fall within five general categories: management, retention, preservation, collection and production. In many ways, the working relationship between the company and the service provider is analogous to that between the company's business, IT and business units. From the management perspective, the company needs to merge its internal document retention policies and schedules with that of the providers. Decisions will need to be made, for example, on whether to purchase email and instant messaging archiving capabilities, which can help manage document retention and searches. Moreover, it does little good, for example, if the company retains a particular category of records in-house for a certain period of time, but the cloud computing provider uses a different schedule. The company must carefully consider how the legal hold guidelines will be applied to data stored with the cloud computing company, who will pay for implementing the hold, and who can testify that proper preservation techniques were followed. Additional privacy complications may arise if the content is stored outside of

the United States. What is also needed is some intelligence in the form of an application in the cloud itself that can translate a litigation hold request into specific ESI in the cloud.

There is a risk that information held on a social media site may be removed for any number of reasons. Thus, the legal hold requirement may mean downloading the information and retaining it in another format. For example, parties to civil litigation may satisfy discovery requirements relating to their Facebook accounts by producing and authenticating contents of their accounts and by using Facebook's "Download Your Information" tool, accessible through the "Account Settings" drop-down menu.

Care must be taken, however, to capture sufficient data so that it can be authenticated at trial. There are many other unique problems concerning the e-discovery within the context of social media.¹¹

Conclusion

Like it or not, the rules of the road will be constantly changing. The only defensible way to deal with it is a carefully thought-out plan.

¹ Austrian and Krolewski, *Basic Steps in E-discovery: Creating the Team and Knowing When to Pull the Trigger*, The Metropolitan Corporate Counsel (January 2011); *Basic Steps in E-discovery Continued: Knowing Where "Stuff" is and Planning to Retain it*, The Metropolitan Corporate Counsel (March 2011).

² See *Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522 (1987).

³ e.g., Judge Paul W. Grimm, "Suggested Protocol for Discovery of Electronically Stored Information ("ESI"), available at <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf>; The Sedona Conference Commentary on Legal Holds (Sept. 2010); The Sedona Conference® Commentary on Legal Holds (Aug. 2007); *Samsung Elec. Co., Ltd. v. Rambus Inc.*, 439 F. Supp. 2d 524, 565 (E.D. Va. 2006).

⁴ *Major Tours v. Colorel*, 2009 WL 2413631 (D.N.J. 2009).

⁵ *The Pension Comm. of the Univ. of Montreal Pension Plan v. Bank of America Sec., LLC*, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010).

⁶ The Deloitte Forensic Center commissioned the Economist Intelligence Unit to conduct a survey of 337 U.S. IT, legal, risk and compliance professionals in the U.S. regarding the e-discovery challenges facing corporate America in 2009. The complete survey report is available at www.deloitte.com/forensicscenter.

⁷ e.g., *Victor Stanley, Inc.*, *supra* n.14; *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474 (D. Colo. 2007).

⁸ *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. Sept. 21, 2010); *EEOC v. Simply Storage Mgmt., LLC*, 2010 U.S. Dist. LEXIS 52766 (S.D. Ind. May 11, 2010); *Bass v. Miss Porter's School*, 2009 U.S. Dist. LEXIS 99916 (D. Conn. Oct. 27, 2009).

⁹ *Steele Software Sys. Corp. v. DataQuick Info. Sys., Inc.*, 237 F.R.D. 561 (D. Md. 2006).

¹⁰ See generally, Mark L. Austrian and W. Michael Ryan, *Cloud Computing Meets Ediscovery*, *Cyber-space Lawyer* (July 2009).

¹¹ This includes problems involving privacy considerations, ethical considerations, and the impact of the Stored Communications Act of the Electronic Communications Privacy Act, 18 U.S.C. § 2702(a)(1). See *City of Ontario v. Quon*, 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010).