Recognizing the Risks and Avoiding the Pitfalls of eDiscovery

TIMOTHY CARROLL AND BRUCE RADKE

This article outlines important issues to be aware of when dealing with electronically stored information ("ESI").

As companies increasingly, and sometimes needlessly, store excessive volumes of electronically stored information ("ESI"), preparing for litigation has become more complex and particularly difficult for the information technology (IT) personnel charged with executing legal hold directives. The 2006 amendments to the Federal Rules of Civil Procedure (the "Amended Federal Rules") codified the view that ESI is discoverable and subject to various retention requirements. The Amended Federal Rules require that, early in the litigation, litigants assess their data and confer about issues relating to the discovery of ESI.[1] Because of the breadth of information stored in corporate technology environments and because of potential pitfalls involved in preserving ESI, in-house legal and technology departments must work together and communicate well in order to develop policies that will help them prepare for a Rule 16 "e-conference," as well as admissibility issues that may arise during the litigation.

Timothy Carroll and Bruce Radke are co-chairs of the eDiscovery team and shareholders in the Commercial Litigation Practice Group at Vedder Price P.C. They can be reached at tcarroll@vedderprice.com and bradke@vedderprice.com, respectively.

Published in the November 2008 Privacy & Data Security Law Journal.

This article outlines important issues to be aware of when dealing with ESI. Specifically, this article discusses:

(1) The events that trigger the legal obligation to preserve ESI;

(2) Strategies for implementing a litigation hold protocol in today's technology climate;

(3) Preserving a credible chain of custody;

(4) The evidentiary hurdles that should be considered when preserving ESI;

(5) The importance of taking proactive steps to maintain the integrity of ESI before engaging in litigation; and

(6) When to use an outside expert.

IDENTIFYING TRIGGER EVENTS

The legal obligation to preserve ESI can be triggered before litigation begins.[2] Triggers may include the filing of a complaint, the receipt of a discovery request, the issuance of a preservation order, the service of a subpoena, an investigation by a government or regulatory agency, the request of facts by a third party relating to an incident or dispute, the threat of litigation by an employee or a formal complaint to management by an employee regarding impropriety by the employer.[3] Once this obligation is triggered, a company should initiate its litigation hold protocol. Establishing record retention and litigation hold policies helps avoid charges of data spoliation and internal sabotage. Moreover, parties to litigation have an ethical obligation to safeguard ESI.[4] Failure to institute a litigation hold can result in court sanctions and liability in tort for spoliation of evidence.[5] Credibility is key in electronic discovery, and is bolstered by consistent and reliable record retention and litigation hold policies.

A good litigation hold protocol should at least be designed to prevent charges of spoliation and data destruction, and should demonstrate a good faith effort on the part of the company to comply with its pretrial discovery obligations. This effort should contain strategies for:

(1) Suspending the planned disposition of records;

(2) Notifying all affected employees of the obligation to refrain from disposing relevant evidence;

(3) Implementing specific steps for preserving backup tapes, archived e-mails and other sources of live data;

(4) Monitoring compliance with the legal hold directive; and

(5) Rescinding the hold once the obligation expires.

To prevent miscommunication and confusion, the legal department should be the one to decide when the obligation to preserve ESI is triggered and when to initiate the company's legal hold protocol.

GOOD COMMUNICATION BETWEEN LEGAL AND IT IS CRITICAL

One of the most critical tasks in-house counsel undertakes when handling ESI is to communicate early and often with the IT department. Representatives from both functions should know where and how high-risk ESI resides within the company. Working as a team, they should make decisions early in the litigation so that relevant ESI is collected properly and that legal holds are extended to all repositories of potentially relevant ESI. Even before a preservation obligation arises, the team should have an understanding of the company's records environment. Otherwise, technology and/or forensic consultants, working without an understanding of their clients' records environment, may be over- or underinclusive in applying key word searches when asked to assist in collecting and subsequently producing ESI. In these cases, either too much or not enough data is collected, impacting the preparation efforts and increasing the risk that a repository was missed.[6]

Larger companies or high-volume litigants may also want to form a legal-hold task force to evaluate the status of litigation and the preservation, collection, and production of ESI. The task force should analyze what information has been preserved, who has access to the ESI, and, if litigation is anticipated, whether legal holds are being followed. A com-

pany's good-faith and reasonable efforts to preserve ESI are a necessary step in defending against claims of spoliation. Accordingly, preparing self-serving minutes and recording compliance with established procedures are ways to accomplish this.

THE IMPORTANCE OF PRESERVING A CHAIN OF CUSTODY IN THE DISCOVERY SETTING

Maintaining a chain of custody and authenticating the evidence presents unique challenges, but these challenges are more acute in the ESI setting. In-house legal and IT teams must therefore understand that when they execute policies to collect, review, and produce ESI, they must maintain a chain of custody relative to their collection of relevant ESI. Chain of custody refers to the document or paper trail detailing the seizure, control, custody, transfer, analysis, and disposal of ESI. To demonstrate the authenticity of ESI in court, and to ultimately have it admitted, the party offering the evidence must show what the evidence was when it was originally gathered and that it has remained unchanged since that time.[7] Each person who had custody of the ESI or accessed it should be able to testify about receiving the information, preserving it, and passing it along to the next person in the chain.

Spoliation risks may arise when too many hands "touch" the ESI. When mistakes are made concerning the chain of custody, the evidence loses credibility and may be deemed inadmissible.[8] In-house counsel must be aware that IT personnel are driven by technological, not legal, considerations. Therefore, they may not properly handle vulnerable data. Many IT departments do not have the experience to handle the job of maintaining a credible chain of custody, and may struggle in implementing in-house eDiscovery tools. The IT department must receive the appropriate training before attempting to secure and maintain the ESI. Forensic experts should be used where doubt is in play.

Metadata, or data about data, is particularly vulnerable to spoliation. It includes information about when the electronic record was created, when it was modified, and the author's identity. However, metadata can easily be overwritten and changed by turning on a computer before prop-

er precautions are taken. Destroying metadata is more likely to occur when the computer is the source of evidence. E-mail is considered more objective and, because it normally exists on servers that are constantly backed up, its metadata is less vulnerable to overwriting. "Taking a quick look" at a source computer can destroy important evidence. Steps should be taken to preserve metadata and the chain of custody. In most cases, the computer should not be turned on. If it is, the user must document everything that is done and at what time. This record will help protect against claims of data spoliation.

A forensically sound copy will also preserve the metadata. Also called hard drive imaging, this copy captures and makes an exact snapshot of the metadata and deleted files. Hard drive imaging is good practice for companies after an employee has been terminated. The IT department should use specialized software, or hire an outside expert, to make a mirror-image copy of the former employee's computer hard drive before the computer is recycled. This preserves evidence in case of future litigation.

EVIDENTIARY HURDLES MUST BE CONSIDERED BY THE IN-HOUSE TEAM

Electronic records must pass through evidentiary hurdles in order to be admissible at trial.[9] In *Lorraine v. Markel*, e-mails were inadmissible because they had not been authenticated.[10] One way to authenticate ESI is by using digital signatures, such as hash marks. Hash marks calculate a unique numerical value, based on the contents of the mirror-image copy.[11] If the metadata is changed in any way (for example, by booting up a computer), the hash marks will also change.[12] By establishing a policy by which hash mark software is utilized, the evidence may be authenticated under Federal Rule of Evidence 901(b)(4) because it is circumstantial evidence of the evidence itself. Hash marks also establish a chain of custody by showing that the examiner did not tamper with the evidence during the investigation. Additionally, certified documents of regularly conducted activity may be self-authenticated under Federal Rule of Evidence 902(11), qualifying record retention and litigation-hold policies

that keep ESI in a consistent manner. Such a document would also be admissible against a hearsay objection as a record of a regularly conducted activity.[13]

PROACTIVE STEPS ARE A MUST

Proactive measures, such as extending records retention policies to ESI and developing litigation hold protocols, should be devised well before litigation. Implementing such measures ensures that, if litigation occurs, the possibility that a "smoking gun" will be found during discovery or that the record will be thrown out at trial is limited.[14]

WHETHER TO USE AN OUTSIDE EXPERT

In-house counsel should carefully consider the company's internal capabilities before deciding whether to use an outside expert vendor or the IT department.[15] Experts follow standard protocol, and typically apply sound and time-tested methods. As discussed above, not all IT departments are equipped to properly handle ESI. Even if the IT department is experienced, the decision to hire an outside vendor should be made on a case-by-case basis. For example, in a high-cost class action suit, using an outside vendor is sensible because it helps to ensure that the collection and documentation of ESI will not be called into question at court.[16] Additionally, hiring an outside vendor is practical in situations where the company will benefit from independent data preservation (i.e., high-profile claims against management, or a Securities Exchange Commission or Department of Justice investigation).[17] Experts should also be brought in when forensic imaging is necessary. For example, when a case involves the use of a company laptop for illegal purposes, an expert must make a hard drive image and forensically analyze it. All should recognize the risk, however, of putting an internal IT staff member on the witness stand or designating such a person as a corporate designee, relative to providing testimony concerning the company's ESI collection, preservation, and production.

In conclusion, in-house counsel and the IT department need to work together to formulate record retention and litigation hold policies in order

to be well prepared for possible litigation. These policies should acknowledge trigger events before the threat of litigation in order to present authentic and credible ESI at trial. Counsel should decide which litigation triggers will kick-start the litigation-hold policy. Preservation of the chain of custody and the risks involved should also be discussed. Policies must be implemented to make sure that valuable metadata is not overwritten and changed. The IT department should be instructed in how to use software that creates and utilizes hash marks. Finally, counsel should carefully consider the company's capabilities and litigation needs when hiring an outside expert. Each case is unique. Therefore, these policies should be flexible enough to address the idiosyncrasies of each case brought to litigation. These guidelines can help litigation preparation to be more effective and efficient.

NOTES

[1] *See* Fed. R. Civ. P. 26(f).

[2] *See Zubulake v. U.B.S. Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (parties must take affirmative steps to preserve ESI at the outset of litigation or when litigation is reasonably anticipated).

[3] *See Applied Telematics, Inc. v. Sprint Comms. Co.*, No. 94-4603, 1996 U.S. Dist. LEXIS 14053, at *6 (E.D. Penn. Sept. 17, 1996); *Zubulake v. U.B.S. Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004); *Arthur Andersen, LLP v. United States*, 125 S. Ct. 2129, 2131-33 (2005); *Blinzler v. Marriott Int'l, Inc.*, 81 F.3d 1148, 1159 (1st Cir. 1996); *Testa v. Wal-Mart*, 144 F.3d 173, 177 (1st Cir. 1998); *Broccoli v. Echostar Communications Corp.* 229 F.R.D. 506 (D. Md. 2005).

[4] *See Thompson v. U.S. Dep't of Housing & Urban Dev.*, 219 F.R.D. 93, 99-100 (D. Md. 2003) (ethical obligations to safeguard electronic information attaches when litigation is probable or has been commenced).

[5] *See Broccoli, et al. v. EchoStar Commc'n Corp., et al.*, 229 F.R.D. 506, 516-17 (D. Md. 2005) (sanctioned for "indefensible" failure to suspend automatic data destruction).

[6] An underinclusive search can also be an ethical violation. *See Rozier v. Ford Motor Co.*, 573 F.2d 1332, 1341-42 (5th Cir. 1978) (judgment was overturned pursuant to Federal Rule of Civil Procedure 60(b)(3) because

Ford failed to turn over a pertinent electronic record).

[7] *See United States v. Abreu*, 952 F.2d 1458, 1476 (1st Cir. 1992); *Hoover v. Thompson*, 787 F.2d 449, 450 (8th Cir. 1986); *United States v. Briley*, 319 F.3d 360, 363 (8th Cir. 2003).

[8] Interview with David W. Meadows, Director of Disputes & Investigations, Navigant Consulting, Inc., August 11, 2008.

[9] *Lorraine v. Markel Am. Ins. Co.*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007).

[10] *Id.*

[11] John Patzakis, *Maintaining the Digital Chain of Custody*, http://www.infosec.co.uk/files/guidance_software_04_12_03.pdf.

[12] *Id.*

[13] *See* Fed. R. Evid. 803(6).

[14] *See Lorraine v. Markel Am. Ins. Co.*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007) (e-mails were thrown out as inadmissible because they were not authenticated under Federal Rule of Evidence 901).

[15] Interview with David W. Meadows, Director of Disputes & Investigations, Navigant Consulting, Inc., August 11, 2008.

[16] *Id.*

[17] *Id.*