eDiscovery Best Practices: Policies, Protocols and Preservation of Electronically Stored Information

BY ROBERT BROWNSTONE

FENWICK & WEST LLP

Published in the Recorder May 11, 2009 and the Law Technology News May 15, 2009

‹http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202430718101›

Introduction – Catch the Wave

The electronic discovery process entails many hazards that can cause clients and practitioners to wipe-out rather than ride safely to shore.

The 2006 amendments to the Federal Rules of Civil Procedure (FCRP) ‹http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf› were intended to provide guidance to parties navigating eDiscovery. In reality, though, judges, litigants, lawyers and technologists are still struggling to frame the discovery boundaries of a vast, ever-expanding world of electronically stored information (ESI). Thus, every organization must, to a degree, craft its proactive day-to-day information-management and its reactive litigation approach from an eDiscovery standpoint.

Don't panic about embarking on this ride. A legally-defensible ESI process can result from minding the "*Three P's*:" *Policies*, *Protocols* and *Preservation*. If an organization and its counsel follow these practical tips, they can catch eDiscovery's cresting wave.

I. Policies – Proactive Procedures

A proactive records-retention program can enable a much smoother ride once litigation ensues. Once on board, the litigator should inquire into the client's a) records-retention policy and any related policies (including, *e.g.*, employee-separation policy); and b) overall compliance therewith.

A. Defensible Retention Program

Hopefully, the organization frontloaded some effort to achieve efficiencies and information-management benefits from a legally-defensible, systematized approach to records retention and destruction. An organization with a pre-existing program can more quickly access, and assess the pertinent contents of, ESI in a cost-effective way.

B. Compliance With Implemented Retention Program

Substantial compliance with a retention program "in the trenches" can provide a safe harbor once litigation hits. Indeed, a *retention* policy is really a *destruction* policy, "created in part to keep certain information from getting into the hands of others, including the Government." *U.S. v. Arthur Andersen*, 544 U.S. 696, 704 (2005) ‹http://laws.findlaw.com/us/000/04-368.html›. Thus, having an adhered-to policy can serve as a justifiable explanation why responsive information was not retained.

A retention policy can even serve as a shield from sanctions. In *Gippetti v. United Parcel Service, Inc.*, 2008 WL 3264483 (N.D. Cal. Aug. 6, 2008) ‹https://ecf.cand.uscourts.gov/doc1/03504815885› (applying Fed. R. Civ. P. 37(e) ‹http://www.law.cornell.edu/rules/frcp/Rule37.htm›), Plaintiff sought spoliation sanctions, alleging Defendant had inaptly destroyed relevant ESI. At issue for Defendant UPS were Plaintiff's and other employees'/drivers' driving records. *Id.* at 2. Defendant responded that some requested documents had been destroyed as part of a routine retention policy. *Id.* To cope with sheer volume, the policy called for destruction of such records after 37 days. *Id.* at 1. The court relied on the policy's routinized approach when denying the spoliation motion. *Id.* at 2 (finding Defendant had received no notice of litigation before documents destroyed).

II. Protocols – Pre-Existing Plans

In addition to due diligence as to the client's retention policy and compliance thereunder, the litigator should assess the organization's: a) litigation-hold protocols; and b) efforts undertaken since the instant matter was reasonably anticipated.

A. Litigation-Hold Protocol(s) in Place

Including a litigation-hold protocol as part of a retention policy or program is a risk-management boon. The protocol should memorialize actual practices. At a minimum, it should identify someone – likely in Legal – as the point person for:

- assessing whether a hold is warranted;
- maintaining a log of situations that did and did not result in a hold; and
- administering issued holds.

Then, risk insulation can ensue. First, if an opponent (possibly the government) alleges evidence-destruction based on deficiencies in administration of an issued hold, a response can point to an overall defensible protocol followed in the given instance. Second, if an opponent contends a hold should have been issued but was not, one can point to a systematic assessment approach and perhaps a spreadsheet showing how many demands the organization gets annually and how few ripen into litigation. *See Keithley v. Homestore.com,* 2008 U.S. Dist. LEXIS 61741 (N.D. Cal. Aug. 12, 2008) ‹http://pdfserver.amlaw.com/ca/sanctions0815.pdf›, *as clarified by,* 2008 U.S. Dist. LEXIS 70246 (Sep. 16, 2008) ‹https://ecf.cand.uscourts.gov/doc1/03504929726›, where the judge expressed dismay at a litigant's lack of a litigation-hold protocol.

B. Hold-Notice Regime and Follow-Through

Part of the litigation-hold program should be a generic hold notice, explaining ESI's role as a significant discovery source and the importance of suspending ESI deletion. The form notice should also particularize the organization's key ESI repositories.

If the form hold notice meets those goals and is kept up to date, then no one will need to create a process anew each time. The form should not be blindly followed, but rather tailored to each matter, in part because the attorney work-product doctrine only applies if a document were created in "anticipation" of litigation.

As soon as he/she is hired, litigation counsel should ascertain what has happened and marshal all writings documenting steps taken. Moving forward it is important for counsel to work with the client to document facts demonstrating compliance.

Producing such documentation, including the actual hold notice, may not ultimately be ordered by the Court. Indeed hold notices are protected under attorney-client privilege and attorney work-product doctrine; and a litigant should not readily waive either protection. A litigant that has effectively implemented a hold may gain credibility with the judge by selectively divulging some underlying details. Moreover, at some point, notices and related memos may have to be produced – and thus become a shield against adversarial attack and/or judicial scrutiny.

If a discovery dispute arises, courts afford varying degrees of protection to the hold notice. At an early stage, one court ordered the responding party to disclose factual information contained in the notice. *In re eBay Seller Antitrust Litigation*, 2007 WL 2852364, at *2 (N.D. Cal. Oct. 2, 2007) (production of names and job titles of 600 employees who received the hold notice) ‹https://ecf.cand.uscourts.gov/doc1/03501816139›. The *eBay* court also acknowledged that details of the responding party's employees' ESI collection and preservation efforts would be fair game not only in the meet-and-confer context, but also in a FRCP 30(b)(6) ‹http://www.law.cornell.edu/rules/frcp/Rule30.htm› deposition notice of a person familiar with those efforts. *Id.* However, the *eBay* Defendant was not required to disclose the actual notice or any of its privileged contents. *Id.*

Other courts have afforded broad content protection once the responding party establishes the notice is likely work-product. *See Gibson v. Ford Motor Co.*, 510 F. Supp. 2d 1116, 1123 (N.D. Ga. 2007) ‹https://ecf.gand.uscourts.gov/doc1/0550934124›, noting that compelled production of the notice or its contents could dissuade other businesses from issuing such instructions. The *Gibson* court reasoned that parties should be encouraged to issue, rather than discouraged from issuing, such directives. *Id.*

As a litigation proceeds, however, higher expectations may kick in when a tenable argument of bad faith arises. The judge may mandate a detailed inquiry into the responding party's retention practices and/or hold process. One well-known opinion, *Rambus, Inc. v. Infineon Technologies AG, Inc*., 222 F.R.D. 280, 288 (E.D. 2004) ‹http://rambus-edva-5-18-04.notlong.com/›, addressed the veil piercing of both attorney-client privilege and work-product protection based on crime/fraud, where Plaintiff had engaged in dubiously timed "shred days."

III. Preservation of Potentially Pertinent ESI

Simply issuing a litigation-hold notice is not nearly enough to satisfy the preservation obligation. Counsel has to navigate various facets of an obligation coined the "*Zubulake* Duty." *See Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y 2004) ("*Zubulake V*") ‹http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/04-05292.PDF›. An attorney has a duty to understand her client's retention program and information-management systems. He/she should communicate with the client to ensure all potential sources of relevant information are parsed out. The client's back-up regime should also be discussed. Also highly advisable is periodically checking back with "key players" who were hold-notice recipients. *Id.* at 433-34, 436, 439.

In civil litigation, a vast body of case-law addresses preservation's flip-side: spoliation, a/k/a destruction of potential evidence. The potential sanctions include: monetary penalties (attorney fees, costs, and/or pay-for- proof sanctions); exclusion of evidence; delay of trial; and, in extreme cases, an adverse inference jury instruction or even dismissal or judgment on the merits.

Among the decisions underscoring the importance of taking the *Zubulake* Duty seriously is *Phoenix Four, Inc. v. Strategic Resources Corp*., 2006 WL 1409413 (S.D.N.Y. May 23, 2006) ‹https://ecf.nysd.uscourts.gov/doc1/12703317469›. There, the court ordered Defendant and its attorneys to each pay over $25,000 for failing to find "hidden server partitions" containing crucial evidence. *Id.* at *9. The court noted that the attorneys had not employed a methodical approach to discover potential sources of information, instead solely relying on their client. *Id.* at *5.

In *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 66932 *4 (S.D. Cal Jan. 7, 2008) ‹http://online.wsj.com/public/resources/documents/qualcomm_doc20080107.pdf›, the attorneys ignored several warning signs indicating their client had failed to adequately search for relevant information. In particular, Qualcomm had not produced emails from key employees who were part of an email distribution list pertaining to key subject matter and had failed to search the emails of individuals listed as most knowledgeable. *Id.* at 10.

Thus, an attorney must execute a plan that actively enables uncovering potential ESI sources and is most likely to ensure that the client engages in comprehensive preservation and collection.

Conclusion

Adhering to systematized proactive and reactive approaches can keep an organization and its counsel upright as they surf the eDiscovery waves.

For additional information, please contact
Robert Brownstone, Director of Law & Technology

at rbrownstone@fenwick.com, 650.335.7912