LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An ALM Publication

Volume 18, Number 10 • June 2011

The Backup Tapes Quagmire:
Preservation and Production In White-Collar Matters

By Abraham J. Rein

As night follows day, government "hold" letters and subpoenas in white-collar investigations seek the preservation or production of "backup tapes." Some prosecutors and agents may have a mistaken understanding of backup tapes; some may not understand what production and use actually entail.

Disaster recovery backup tapes (DRBTs) are tape-based media, housing data that is often compressed and heavily encrypted. The tapes are stored offsite, to be used only in the event of a disaster, such as a flood or fire, and are not intended to maintain data for litigation. DRBTs often are very costly to restore and produce, even more so if they house data that was generated with outdated programs or systems that need to be rebuilt.

The Abbott Labs Case

When the Western District of Virginia ordered Abbott Laboratories to comply with a subpoena in a criminal investigation into alleged off-label pharmaceutical marketing, the business community took notice. *In re Subpoenas*, 692 F. Supp. 2d 602 (W.D. Va. 2010) (*Abbot Labs*). Compliance with the subpoena would require Abbott to restore and search six years' worth of e-mail from the company's DRBT archive. Abbott estimated the restoration cost alone at nearly $400,000. The court was unimpressed: "As the court views it, if retrieving the e-mails is as difficult as Abbott conveys, then the fault lies not so much with an overly broad governmental request as it does with Abbott's policy or practice of retaining documents … in a format that shrouds them in practical obscurity." *Id*. at 605.

In the white-collar context, companies are understandably reluctant to litigate document production issues, preferring to begin their relationship with the prosecutor on a collaborative note. As a result, the propriety of government demands for inaccessible DRBTs in white-collar matters has not been fleshed out. This lack of judicial guidance can leave corporate and outside counsel in the dark as to their negotiating leverage even as the parties strive to resolve electronic discovery issues as the courts direct. *See, e.g., United States v. Graham*, 2008 WL 2098044 (S.D. Ohio, May 16, 2008).

Civil Litigation Standards As Guidance in the Business Crimes Context

In recent years, courts considering thorny discovery issues — particularly e-discovery issues — in criminal matters have increasingly turned to civil jurisprudence for guidance. In *United States v. O'Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008), a criminal case, the court looked to the Federal Rules of Civil Procedure (FRCP) for help in deciding a question about the appropriate form of production for electronically stored information, saying "[i]t is foolish to disregard [the FRCP] merely because this is a criminal case." *Id*. at 19. When the District of New Jersey was faced with a case involving spoliation of material stored on the FBI's DRBTs, the court noted the "relatively little criminal case law in the Third Circuit" on the subject, and "consult[ed] the more thoroughly developed civil case law" instead. *United States v. Suarez*, 2010 U.S. Dist. LEXIS 112097, at *22 (D.N.J. Oct. 21, 2010). Similarly, when required to decide whether an investigatory subpoena issued pursuant to 18 U.S.C. § 3486 — the same kind of administrative subpoena used to require Abbott Laboratories to restore its DRBTs — imposed an undue burden, the court consulted the law governing subpoenas issued in civil litigation under Fed. R. Civ. P. 45. *In re Subpoenas Duces Tecum* (*Family Health Care*), 51 F. Supp. 2d 726, 737 (W.D. Va. 1999) (noting that the criminal procedural rule governing subpoenas is, according to the advisory note, "substantially the same" as the civil rule, and consequently applying the jurisprudence developed under the civil rule).

In civil courts, the question of the discoverability of DRBTs has been litigated extensively. Courts and experts generally start from a loose presumption that DRBTs are "not reasonably accessible," making them immune from discovery absent "good cause." *See Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); Fed. R. Civ. P. 26(b)(2)(B). While the resulting body of case law discussing "good cause" is not always clear or consistent, a careful examination of the cases suggests a handful of factors that appear to govern courts' decisions in DRBT cases.

The 'Zubulake Exception'

In what is known as *Zubulake IV*, 220 F.R.D. 212 (S.D.N.Y. 2003), Judge Shira

Abraham J. Rein (arein@postschell.com) specializes in e-discovery issues within the White Collar Defense, Compliance and Risk Management Group at Post & Schell, P.C., Philadelphia.

Scheindlin held that the civil litigant's duty to preserve, "as a general rule, … does not apply to inaccessible backup tapes [DRBTs] (*e.g.*, those typically maintained solely for the purpose of disaster recovery)," with this important exception: "[T]he tapes storing the documents of 'key players' to the … litigation should be preserved if the information contained on those tapes is not otherwise available." *Id.* at 218.

The "*Zubulake* exception" to the general rule that DRBTs are immune from discovery — allowing production when they house data that is: 1) generated by "key players"; and 2) not otherwise available — remains the most common fact pattern in cases where DRBTs are ordered produced, although those decisions frequently do not expressly cite *Zubulake*. In *Abbott Labs*, for example, the subpoena sought the e-mails of three key individuals; to the extent those e-mails were stored on more accessible media, the DRBTs were not implicated. But as to otherwise unavailable e-mails generated by those individuals, the court ordered them produced from DRBTs. *See also DeGeer v. Gillis*, 2010 WL 5096563, 2010 U.S. Dist. LEXIS 129745 (N.D. Ill. Dec. 8, 2010).

Pre-Existing Legal Duty

In cases where the responding party has a legal duty running to the data on the DRBTs independent of the discovery issue before the court, and that data is otherwise unavailable, the general rule that DRBTs are off-limits may be ignored. When, for example, the data housed on the DRBTs is subject to a duty to preserve in other litigation, courts have little patience for an argument that the information has since become inaccessible by virtue of being archived. The decision in *Abbott Labs* turned in part on this factor, as did that in *California ex rel. Fowler v. Caremark Rx*, 2010 Cal. App. Unpub. LEXIS 8087 (Cal. App. Oct. 13, 2010). Similarly, where the responding party has a statutory or regulatory duty to preserve records, the accessibility (or the lack thereof) of the media on which the records are stored will generally be treated as irrelevant. In *In Re Deutsche Bank Securities Inc.*, No. 3-10957, 55 S.E.C. 1248 (2002), the SEC asked the respondent to produce certain e-mails that SEC regulations required it to preserve. When the respondent could not produce the e-mails because they were maintained on DRBTs and "[r]espondents had inadequate systems or procedures to ensure the retention of such back-ups … and/or to maintain such data in a readily accessible manner," each respondent was fined $1.65 million. *See also In Re J.P. Morgan Securities Inc.*, No. 3-11828, 2005 SEC LEXIS 339 (Feb. 14, 2005).

Discovery Failures

When the conduct of the responding party appears to have fallen short of other discovery-related obligations — a failure to timely institute a litigation hold, for example, or apparent discovery-related misrepresentations to the court — the court will more likely order DRBTs produced. In the recent case of *Green v. Blitz U.S.A.*, 2011 U.S. Dist. LEXIS 20353 (E.D. Tex. Mar. 1, 2011), the defendant was sanctioned heavily, in part for its failure to preserve data on DRBTs. The DRBT-related failure had been accompanied by a series of seemingly egregious missteps, including specific instructions to employees to delete all of their e-mail, despite ongoing litigation. *See also Kipperman v. Onex Corp.*, 2009 WL 1473708 (N.D.Ga., May 27, 2009).

Credible Evidence of Burden

Finally, and possibly most significantly, in nearly every recent decision declining to order production of DRBT material, the responding party has introduced some credible, unique facts to demonstrate the associated burden. Such evidence, usually in the form of declarations, estimates from vendors and other similar material, appears to be a crucial factor in exempting DRBTs from production. In *Johnson v. Neiman*, 2010 U.S. Dist. LEXIS 110496 (E.D. Mo. Oct. 18, 2010), for example, the defendant submitted the affidavit of a state Information and Technology Services Division officer, demonstrating that the requested DRBTs would cost upwards of $1 million to restore. This was enough for the court to decline to compel production. *See also Major Tours, Inc. v. Colorel*, 2010 U.S. Dist. LEXIS 62948 (D.N.J. June 22, 2010).

Conclusion

It behooves both parties to narrow government requests for documents, using defensible criteria. For the corporation, narrower requests mean less expense and exposure; for the government it means avoiding a document dump.

Counsel and IT personnel should prepare for narrowing negotiations as early as practicable — even before receiving the document request or subpoena, if possible — by ensuring and documenting that the four factors described above weigh in their favor. The burden associated with producing DRBT material should be carefully documented. If necessary, outside counsel should be consulted on these issues and ensure that other e-discovery-related obligations are followed closely.

There may be no clear rules controlling the government's access to DRBTs in white collar matters, but armed with careful preparation, documentation, and a clear understanding of electronic discovery principles, companies have a chance of avoiding the burden and expense of producing DRBTs in such situations.