Bloomberg BNA

Digital Discovery & e-Evidence®

BNA INSIGHTS

BakerHostetler's James A. Sherer and Jacqlyn Rovine consider whether, to what extent and to what effect a court deciding a motion for spoliation sanctions will examine a challenged-party's efforts to manage its information *before* litigation was reasonably anticipated, and to what extent litigators may be obligated to inform themselves about their clients' information governance efforts vis-à-vis the case at hand.

Past Information Governance May Haunt the Present: The Need for Routine Document Retention/Destruction Policies

BY JAMES A. SHERER AND JACQLYN ROVINE

While case law clearly requires legal holds when litigation is reasonably anticipated, courts have begun to reach further back into parties' histories to examine what the parties did with the information at issue even before legal hold obligations arose.

Most courts have stopped short of censuring parties for past sins not presently before the court; nonetheless, all courts are beginning to consider these behaviors when examining difficult, present-day facts that *are* ripe for determination.

A Hypothetical. Consider the following fact pattern: a court is considering a motion for spoliation sanctions brought against two parties, defendants Alpha and Beta, who both suffered catastrophic data losses prior to producing documents in the case's discovery.

The court confirms that Alpha had good information governance[1] practices: Alpha had created an accountability framework and ensured appropriate behavior in valuing, creating, storing, using, archiving, and deleting the company's information; regularly destroyed data no

[1] *See* Gartner IT Glossary, http://www.gartner.com/IT-Glossary/information/governance (last visited Apr. 15, 2014).

James Sherer is Counsel in BakerHostetler's New York office and co-chairs the Information Governance Team. James focuses on litigation, discovery management processes, records and information governance, data privacy and security, and technology integration issues. He holds an MBA in finance, CIPP/US and CIPM credentials, and is a member of The Sedona Conference® Working Group One on Electronic Document Retention and Production (WG1).

Jacqlyn Rovine is an Associate in BakerHostetler's New York office. She is a commercial litigator, focusing her practice on complex business matters, appellate practice, as well as employment litigation, counseling, and investigations. She also advises clients on information governance, due diligence practices, and performance measurement and audit.

 ISSN 1941-3882

longer needed to meet compliance obligations or in the ordinary course of business; and implemented a legal hold policy that, when anticipating litigation, informed custodians of the need to retain certain data, turned off the automatic deletion features of the document retention policy, and halted the recycling of relevant backup tapes.

Beta, in contrast, had no prior information governance program and no workable legal hold practices. Alpha did ''everything'' and Beta did nothing; regardless, both lost relevant information.

Based on the emerging case law, the parties may be sanctioned for the loss, but the specific sanction applied to each is likely to be different.

Why? Because a party that can point to a comprehensive information governance program—even one that includes an ''extraordinary'' retention/deletion program that deletes e-mails within days of being sent with no record whatsoever—may be in a better position to refute allegations of intentional information destruction in the face of active litigation than a party that failed to implement any proactive information management measures regarding the information at issue.

Courts Accept Information Governance Programs With Legitimate Routine Data Retention/Deletion Policies.

Every organization is facing a massive growth in data, types of data, regulatory scrutiny and privacy/information risks. Organizations are coming to realize that data has to be proactively managed through information governance programs to meet regulatory demands, optimize the value of the information and reduce the risks of noncompliance and leaks.

Key Elements. Among the key elements of an information governance program is a data retention/deletion policy. The United States Supreme Court has allowed that ''[d]ocument retention policies', which are created in part to keep certain information from getting into the hands of others . . . are common in business.''[2] The key for court approval is for such policies to be routine, widely followed, and understood in the context of the organization's other responsibilities.

Two cases brought against EchoStar Communication Corporation illustrate the value in having an ongoing information governance program with a routine data retention/deletion component.

In 2005, the U.S. District Court for the District of Maryland called EchoStar's e-mail/document retention policy ''extraordinary'' because it deleted e-mails from users' 'sent items' folders—completely and without record—after 21 days,[3] yet the court still concluded that ''under normal circumstances, such a policy may be a risky but arguably defensible business practice undeserving of sanctions.''[4]

Several years later, two New York State courts remarked that EchoStar had amended its e-mail/document retention policy, reducing the 21-day deletion cycle to seven days.

While the motion court and First Department focused on EchoStar's failure to halt the automatic deletion function once litigation had been reasonably anticipated, the EchoStar's relatively quick turn-around—but routine—deletion policy was not the problem.[5]

Programs That Incorporate Questionable Data Retention/Deletion Policies Do Not Enjoy Protections.

Rambus Inc. commenced a patent infringement action against Infineon, alleging infringement of several patents.[6] In contrast to EchoStar, Rambus had adopted its document policy, resulting in the extensive deletion of material relevant to the case, shortly before and with an eye toward bringing the action against Infineon and other alleged infringers.[7] While Rambus argued that its policy was adopted for ''wholly legitimate business purposes,'' the court disagreed, finding that Rambus's concurrent adoption of its patent litigation strategy and its document retention program ''could not clothe [the deliberate destruction of documents] with propriety.''[8]

The same policy and deletion were challenged in Rambus's cases filed in the Northern District of California[9] and the District Court for Delaware,[10] and a case brought by Samsung against Rambus in the Eastern District of Virginia.[11]

While the Northern District of California found no harm in Rambus's disposal policy, every other court (as well as the Federal Circuit Court of Appeals when vacating the Northern District of California's divergent order)[12] found Rambus's patent infringement claims unenforceable by virtue of Rambus' destruction of relevant information in anticipation of litigation.

The *EchoStar* and *Rambus* cases highlight another important incentive for adopting an information governance program with a routine data retention policy: once those companies had their data retention/deletion policies discussed in open court, their decision-making about data became reputational, and the courts' presumptions followed the companies into future litigation.

This issue—the potential haunting by past information governance sins—is further illustrated by *Porcal v. Ciuffo* and *B.Y.U. v. Pfizer, Inc.*

---

[2] *Arthur Andersen, LLP v. United States*, 544 U.S. 696, 704 (2005).

[3] *Broccoli v. EchoStar Comm. Corp.*, 229 F.R.D. 506, 510 (D. Md. 2005).

[4] *Id.* at 510.

[5] *Voom HD Holdings LLC v. EchoStar Satellite L.L.C.*, 93 A.D.3d 33, 39-40, 939 N.Y.S.2d 321 (1st Dep't 2012); *see also Voom HD Holdings LLC v. Echostar Satellite L.L.C.*, Index No. 600292/08, 2010 NY Slip Op 33759[U], 2010 N.Y. Misc. LEXIS 6711, at *61 (N.Y. Sup. Ct. Nov. 3, 2010).

[6] *Rambus Inc. v. Infineon Technologies*, 220 F.R.D. 264, *motion to compel granted*, 222 F.R.D. 280 (E.D. Va. 2004).

[7] *Id.* at 280, 284.

[8] *Rambus*, 222 F.R.D. at 298.

[9] *Hynix Semiconductor Inc. v. Rambus Inc.*, 591 F. Supp. 2d 1038 (N.D. Cal. Jan. 5, 2006).

[10] *Micron Technology, Inc. v. Rambus Inc.*, 255 F.R.D. 135 (D. Del. Jan. 9, 2009).

[11] *Samsung Elecs. Co. v. Rambus Inc.*, 386 F. Supp. 2d 708 (E.D. Va. Sept. 14, 2005).

[12] *Hynix Semiconductor Inc. v. Rambus Inc.*, 645 F.3d 1336 (D.C. Cir. 2011).

  DDEE ISSN 1941-3882

Courts are Beginning to Consider the Operation of Information Governance Policies Prior to the Case.

In *Porcal*, the defendant-employers had been subject to a wage violation investigation by the Massachusetts Attorney General, which resulted in the Attorney General fining the employer $10,000 for the non-willful failure to comply with a Massachusetts regulation requiring the retention of wage records for up to two years.[13]

When the employee later commenced a civil suit against the employer to recover the unpaid wages, the court learned that the defendants had destroyed the remaining wage records following the conclusion of the Attorney General's investigation.[14]

At first, the court found the recordkeeping requirement ''separate and distinct from the Defendants[']obligation to preserve evidence when litigation was reasonably anticipated.''[15] But after further consideration, the court justified the award of sanctions on defendants' ''considerable past experience . . . that the documents should be retained.''[16]

The plaintiff in *B.Y.U.* similarly asked the court to examine the defendant's duty to preserve documents in the context of ''other sources,'' such as defendant's subsidiary's document retention policies, defendant's document retention policies, defendant's obligations to the federal government, and even defendant's ''litigation with other parties.''[17]

In contrast to *Porcal*, the *B.Y.U.* court declined to examine these additional sources of duty, finding instead that defendant would only be judged according to the duty owed to the plaintiff in the immediate action.[18]

Judicial Scrutiny Will Persist. Regardless of the result, courts will continue scrutinizing how organizations manage their data. This will require challenged parties that rely on their routine data retention/deletion policies to defend against allegations of spoliation to have complied with those policies; the scrutiny will also develop and memorialize organizational reputations regarding information management practices that will live on long after settlement or judgment.

Courts Disapprove of Litigants Having No Policy Whatsoever.

Returning to the Alpha and Beta fact pattern, the Southern District of California in *Zest IP Holdings, LLC v. Implant Direct Mfg., LLC*, recently considered a motion for spoliation and discovery abuse sanctions where the defendant organizations did not implement a litigation hold or document preservation policy, did not at any time preserve electronic documents, and did not instruct its employees to preserve documents.[19] Instead, the defendants simply had ''a company policy that 'no documents are to be deleted.' ''[20]

Flawed System. Despite defendants' insistence that no documents *were* deleted, it became clear that the defendants had no control over their information: defendants' server failed to record an independent contractor-turned-employee's e-mails, sent to and from a personal AOL e-mail address that she was permitted to use for defendants' work, as well as the president and CEO's e-mails, which he sent and received through six different e-mail accounts.[21]

The defendants' inaction, especially the ''policy'' of not deleting anything, warranted sanctions because ''it [was] obvious that Defendants' document retention policy did not prevent documents from being destroyed.''[22] In determining which sanctions to impose, the *Zest* court considered ''the willfulness of the destructive act and the prejudice suffered by the victim,''[23] finding that the chosen sanctions must be commensurate with the spoliating party's ''motive or degree of fault in destroying the evidence.''[24]

The *Zest* court determined that willfulness, bad faith, or fault was necessary to enter default judgment against the spoliating party, and that a ''conscious disregard'' of discovery obligations was needed to impose an adverse inference jury instruction or preclude the party responsible for destroying evidence from proffering witness testimony based on the destroyed evidence.

Applying this standard, the *Zest* court recommended that the district court read an adverse inference instruction to the jury and impose monetary sanctions in the amount of plaintiffs' attorney fees, as having no information management policy constituted the conscious and/or willful disregard of the duty to preserve and resulted in the wrongful destruction of evidence.[25]

Indeed, the *Zest* court's ability to reach further back into the defendants' history to examine what defendants did with the information at issue *before* legal hold obligations arose permitted the court to consider these sins when examining the difficult, present-day facts that *were* ripe for determination.

Counsel May Be Obligated to Counsel Clients on at Least the Operation of Information Governance Practices.

Aside from the cases which demonstrate that information governance practices and policies are now subjects of discussion before the court, defense counsel in *Zest* should have been aware of how the defendants' information governance ''policy'' intersected with—and would later be argued to constitute—the defendants' legal hold.

---

[13] *Porcal v. Ciuffo*, No. 10-CV-40016, 2011 U.S. Dist. LEXIS 109537, at *3, 3 n.1, 5-6 (D. Mass. Sept. 23, 2011).
[14] *Id.* at *3.
[15] *Id.* at *7.
[16] *Porcal v. Ciuffo*, No. 10-CV-40016, 2011 BL 303846, at *3 (D. Mass. Nov. 21, 2011).
[17] *B.Y.U. v. Pfizer*, 282 F.R.D. 566 at *4 (D. Utah April 16, 2012).
[18] *Id.* at *4-5.
[19] No. 10-CV-0541, 2013 BL 329776, at *2 (S.D. Cal. Nov. 25, 2013).
[20] *Id.*
[21] *Id.* at *2-3, 6.
[22] *Id.* at *6.
[23] *Id.* at *7 (citing *Apple v. Samsung*, 888 F. Supp. 2d 976, 992 (N.D. Cal. 2012)).
[24] *Zest IP Holdings*, 2013 BL 329776, at *7 (citing *Apple*, 888 F. Supp. 2d at 993).
[25] *Zest IP Holdings*, 2013 BL 329776, at *10.

Extending that line of reasoning only slightly, the court's opinion in *Vagenos v. LDG Financial Services, LLC* is instructive for why this maturation of jurisprudence may matter for most practicing litigators.[26]

When considering a sanctions motion relating to spoliation allegations, the court ruminated on the state of technology generally and ''this age of electronic discovery'' specifically.[27] The *Vagenos* court then found that, in the face of these types of technology-oriented challenges, responsibility of counsel to inform the client is ''heightened,'' and the preservation obligation ''runs first to counsel.''[28]

It is not too far a stretch to imagine that the operation of information governance policies would also fall within the ambit of counsel's responsibility, especially if the client relies upon the operation of the policy as part of its legal hold behavior—or, as is frequently the case, the attorney had given advice to the client on proper information governance practices in the first instance.

[26] No. 09-CV-2672, 2009 BL 280813 (E.D.N.Y. Dec. 31, 2009).

[27] *Id.* at *2.

[28] *Id.*

  DDEE ISSN 1941-3882