Morgan Lewis

alert

eData lawflash

www.morganlewis.com

Court Compels Production of Personal Emails from Company Systems Citing Lack of Reasonable Privacy Expectation

June 9, 2011

On May 23, in *SEC v. Reserve Management Co. Inc.*,[1] the U.S. District Court for the Southern District of New York ruled that an employee does not have a reasonable expectation of privacy with respect to communications with a spouse through an employer's email system. In reaching its decision, the court employed the four-part test from *In re Asia Global Crossing Ltd.*[2] to determine if the employee had a reasonable expectation of privacy. Key to the court's analysis was the presence and actual notice to employees of an email policy that both forbade personal communications and warned employees of possible disclosure of company-controlled email communications.

Background

Reserve Management Co, Inc. (RMCI), under the leadership of its president, Bruce Bent II, managed a money market mutual fund known as the Reserve Primary Fund (Fund). RMCI invested $785 million of the Fund's assets in Lehman Brothers debt. Just days after Lehman Brothers' bankruptcy announcement, the Fund's net asset value dropped to less than $1 per share. In response to RMCI's handling of communications with investors regarding the Fund's vulnerability to Lehman Brothers and its effect on investor assets, the Securities and Exchange Commission (SEC) filed fraud charges against RMCI. During discovery, RMCI withheld approximately 60 emails between Mr. Bent and his wife, asserting the marital communications privilege. The SEC subsequently moved to compel production of these emails.

In determining whether there was a valid marital communications privilege claim, the court found that it was undisputed that the Bents were married and that they intended to convey messages to each other. However what was in dispute was whether their communications were made in confidence.

Privacy of "Personal" Data in the Courts

The question of whether an employee has a privacy interest in "personal" data on company systems has been addressed by many courts in the past decade. Generally, courts have held that content maintained

1. Docket No. 1:09-cv-4346-PGG (S.D.N.Y. May 23, 2011) (*Reserve Management*).

2. 322 B.R. 247 (Bankr. S.D.N.Y. 2005) (*Asia Global Crossing*).

on company-owned systems is the property of the company. However, there have been some notable exceptions. In the *Stengart* case,[3] the Superior Court of New Jersey found that company ownership of a computer was not determinative of whether an employee's otherwise privileged emails were company property. Instead, the court balanced the employer's legitimate business interests against the attorney-client privilege.

Additionally, a growing line of cases affords protection to employees who may reasonably have expected privacy when using company IT systems. In *Asia Global Crossing*, the court set forth a four-factor test to assess the reasonableness of an employee's privacy expectation in personal email transmitted over, and maintained on, a company server. The test poses four questions:

1. Does the company maintain a policy banning personal or other objectionable use?
2. Does the company monitor the use of the employee's computer or email?
3. Do third parties have a right of access to the computer or emails?
4. Did the company notify the employee, or was the employee aware, of the use and monitoring policies?

This test has been adopted by a number of courts faced with the task of determining the reasonableness of privacy expectations. As the *Reserve Management* court pointed out, "the cases in this area tend to be highly fact-specific and the outcomes are largely determined by the particular policy language adopted by the employer."

The Four-Factor Test and RMCI

Applying the four-factor test to determine whether Mr. Bent had a reasonable expectation of privacy in his emails with his wife, the court analyzed whether RMCI maintained a policy regarding personal use of company email. The court rejected RMCI's contention that any policy was merely aspirational, finding that the policy clearly banned personal use of the company email system:

> Employees should limit their use of the e-mail resources to official business. . . . Employees should . . . remove personal and transitory messages from personal inboxes on a regular basis.

Focusing intensely on the policy's language, the court cited prior opinions analyzing obligatory policy language, as well as dictionary definitions. Ultimately, the court determined that RMCI's policy unequivocally banned the personal use of company email, and that Mr. Bent violated this policy by communicating with his wife over RMCI's systems.

The court next addressed the second factor of the *Asia Global Crossing* test—whether the employer monitors the employee email. While stating that the company will not "routinely monitor employee's e-mail and will take reasonable precautions to protect the privacy of e-mail," RMCI's policy further stated that RMCI reserved "the right to access an employee's e-mail for a legitimate business reason . . . or in

---

3. *Marina Stengart v. Loving Care Agency, Inc., et al.*, Docket No. A-3506-08T1 (N.J. Super. Ct. App. Div. June 26, 2009); see the March 31, 2010 Morgan Lewis LawFlash, available online at http://www.morganlewis.com/pubs/XPLF_PersonalEmailAccount_LF_31mar10.pdf.

conjunction with an approved investigation." Because RMCI reserved the right to access email accounts, the court found that RMCI satisfied the second factor of the *Asia Global Crossing* test. Elaborating, the court pointed out that where an employer reserves this right, courts often find the employee has no reasonable expectation of privacy.

The third factor of the *Asia Global Crossing* test asks whether third parties have rights to access employee emails. Once again, the RMCI email policy addressed this, stating:

> Employees are reminded that client/public e-mail communications received by and sent from Reserve are automatically saved regardless of content. Since these communications, like written materials, may be subject to disclosure to regulatory agencies or the courts, you should carefully consider the content of any message you intend to transmit.

The court found that this provision gave clear notice to Mr. Bent that his communications over the company email system were subject to disclosure. In its analysis, the court noted that RMCI operates in the heavily regulated financial sector, and that regulatory action was reasonably foreseeable.

The fourth factor—employer notice and employee awareness of the company use and monitoring policy—was not in contention. The defendants conceded that Mr. Bent was aware of the policy.

Having answered all four questions in the affirmative, Mr. Bent was deemed not to have had a reasonable expectation of privacy in emails he sent or received over RMCI's email system. Consequently, the communications with his wife were deemed not confidential and the marital communications privilege did not apply. Granting the SEC's motion, the court ordered RMCI to produce the withheld emails between Mr. Bent and his wife, which resided on the RMCI email servers and data archives.

Conclusion

This case serves to remind organizations of the importance of email policies and compliance. The commingling of business and private communications can expand the scope of discovery and expose a company to liability for an employee's casual, careless remarks, which the employee may have considered to be private. Even though Mr. Bent believed that his emails with his wife were not business related, and would never be read by anyone else, the court found that this was not a reasonable belief and ordered disclosure.

As in *Stengart*, companies may be at a disadvantage in litigation with an employee or former employee whom the court finds had a reasonable expectation of privacy. In such cases, not only will a company have no right to emails on its own system, but it may also need to sequester any privileged communications identified during discovery and to disclose the discovery to opposing counsel.

The overarching lesson from these cases is that companies should have in place comprehensive, robust computer and email usage policies. Of course, these policies are only effective when they are clearly articulated and publicized. As well as increasing compliance, a formal training program can eliminate questions regarding notice. Finally, companies should strongly consider using an acknowledgement mechanism to demonstrate that employees received, reviewed, and understood the policy.

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis eData attorneys:

New York

Denise E. Backhouse	212.309.6364	dbackhouse@morganlewis.com

Philadelphia

Stephanie A. "Tess" Blair	215.963.5161	sblair@morganlewis.com
Jacquelyn A. Caridad	215.963.5275	jcaridad@morganlewis.com
Tara S. Lawler	215.963.4908	tlawler@morganlewis.com
Scott A. Milner	215.963.5016	smilner@morganlewis.com

San Francisco

Lorraine M. Casto	415.442.1216	lcasto@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 22 offices in the United States, Europe, and Asia, Morgan Lewis provides comprehensive transactional, litigation, labor and employment, regulatory, and intellectual property legal services to clients of all sizes—from global Fortune 100 companies to just-conceived startups—across all major industries. Our international team of attorneys, patent agents, employee benefits advisors, regulatory scientists, and other specialists—nearly 3,000 professionals total—serves clients from locations in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.