New York Law Journal
TODAY
TECHNOLOGY
Web address: http://www.nylj.com
VOLUME 238—NO. 41 TUESDAY, AUGUST 28, 2007 ALM

# Lines Blur Between Business, Personal Data


H. CHRISTOPHER BOEHNING


DANIEL J. TOAL

• ELECTRONIC DISCOVERY •

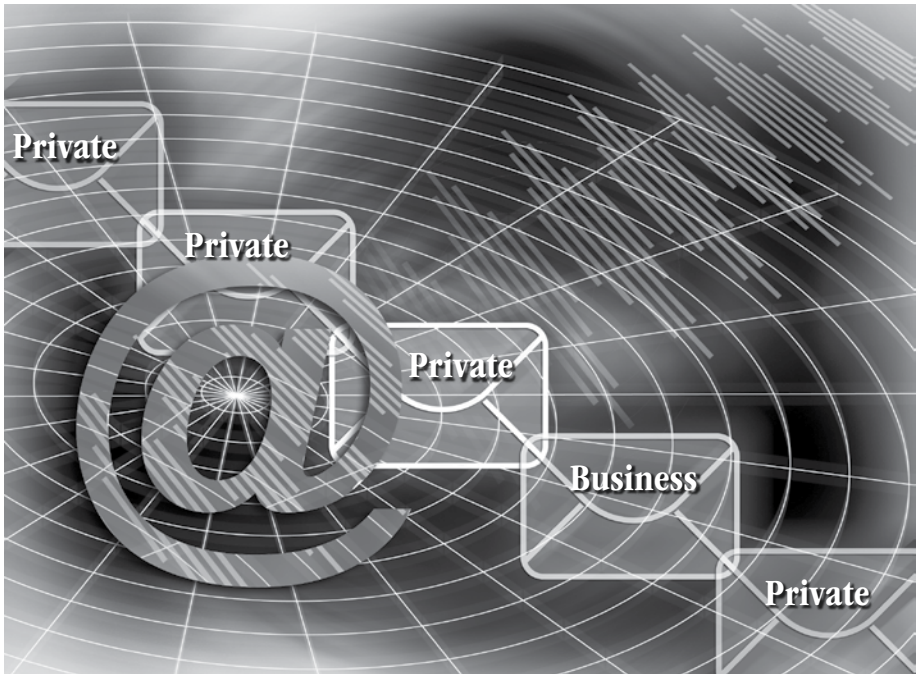
**'Quinby,' 'Ameriwood' and 'Easton' all indicate that businesses may need to consider whether relevant, discoverable information exists on their employees' home computers and personal e-mail accounts, and develop discovery plans tailored to seek and preserve responsive information stored at those location**

**BY H. CHRISTOPHER BOEHNING AND DANIEL J. TOAL**

Recent headlines have highlighted the blurring divide between professional and private e-mail accounts: The White House and its staffers were subjected to criticism and scrutiny for their use of non-governmental e-mail accounts and BlackBerries in connection with official business; New York Governor Eliot Spitzer's aides' personal e-mail accounts have been targeted for communications concerning the investigation into the Senate majority leader; and New Jersey Governor Jon Corzine recently declared that he would stop using e-mail entirely in response to legal requests for private e-mails between the governor and his ex-girlfriend.

The overlap between business and personal e-mail and computer use is not limited to the political arena. An April 2007 survey revealed that 33 percent of employees use personal e-mail accounts at least once or twice weekly for business purposes, and that 17 percent do so daily.[1] Moreover, nearly 16 percent of the survey participants admitted to using their personal e-mail accounts to avoid corporate review or retention of their messages.[2]

As these results indicate, courts and attorneys are likely to face an increasing number of requests for access not only to an employee's business e-mail, but also to any business-related e-mail that may be found in the employee's personal e-mail or stored on the employee's home computer. This reality can raise privacy concerns and questions about whether a subpoena or document




**H. Christopher Boehning** *and* **Daniel J. Toal** *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison LLP.* **John Vagelatos,** *a litigation associate at the firm, and* **Juan A. Ruiz Garcia,** *a visiting foreign attorney at the firm, assisted in the preparation of this article.*

demand to a company should be read to reach the personal e-mail accounts of the company's employees.

Federal Rule of Civil Procedure 26(b)(1) allows discovery of any matter relevant to the claims of a party as long as the discovery "appears reasonably calculated to lead to the discovery of admissible evidence," while the recently modified Rule 34(a) allows a party "to inspect, copy, test, or sample any...electronically stored information." Nonetheless, the Advisory Committee for Rule 34(a) anticipated that in our current electronic age, such discovery "may raise issues of confidentiality or privacy."[3] Thus, Rule 34(a) does not entitle a party to "a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances."[4] As a result, courts have been hesitant to allow wholesale access to a parties' personal electronic information.

In *Quinby v. WestLB AG*, Magistrate Judge Henry Pitman of the Southern District of New York quashed two subpoenas seeking such unfettered access to a plaintiff's personal e-mail account through third-party e-mail providers.[5]

Quinby, a former West vice president, had brought a Title VII suit alleging gender discrimination based on disparate treatment in compensation and in connection with her termination. After seeking and receiving document discovery from Quinby and certain third-parties, defendants served two subpoenas on Time Warner Cable of New York City and Road Runner Corporation, plaintiff's personal e-mail providers, which sought all non-privileged e-mails sent to or received by Quinby's personal e-mail account from October 2002 through July 2004, with the exception of attorney-client communications.

Plaintiff objected to the subpoenas primarily on the ground that they were overbroad. Defendant argued that the subpoenas were appropriate because third-party discovery had shown that plaintiff had not produced responsive e-mails from her personal e-mail account.

Magistrate Judge Pitman first noted that "plaintiff's personal e-mail accounts" were presumably "similar to those of most individual's," containing "vast amount[s] of irrelevant material, including 'spam' e-mails, internet purchase orders and confirmations, personal correspondence, confirmations of medical appointments and the whole raft of communications that are now routinely made over the internet." Accordingly, the court found that defendant's subpoenas "entirely ignore the requirement that a discovery request be limited to relevant material."[6]

The defendant argued that broad discovery was appropriate, however, because e-mails produced by third parties established that plaintiff had improperly withheld documents and could not "be trusted to review her own e-mails properly."

After examining the documents produced by the third-parties, the court rejected this argument. Magistrate Judge Pitman found that the third-party e-mails were outside the scope of defendant's document requests, and therefore that defendant had not established any discovery-related misconduct by plaintiff. In the absence of such misconduct, the court quashed the subpoenas as overbroad. Courts have likewise denied wholesale discovery of an adversary's computer hard drives in the absence of a showing of discovery misconduct or that the computer contents go to the central issues in the case.[7]

## Allowing Limited Discovery

When personal e-mails or computers relate to the central issues of the case, however, the courts will balance the need for relevant electronic information located in personal e-mail accounts and computers against the concern of parties in preserving the confidentiality of their personal information.

In *Ameriwood Industries, Inc. v. Liberman*, plaintiff alleged that the defendants, its former employees, had misappropriated trade secrets and confidential business information.[8] Specifically, plaintiff alleged that the "former employees [had] forwarded plaintiff's customer information and other trade secrets from plaintiff's [business] computers to defendants' personal e-mail accounts, presumably for the purpose of using other computers to access and store those files."

Ameriwood sought access to "mirror image" copies of all computers used by the defendants in order to search for responsive information, including deleted files and metadata.[9] Plaintiff also submitted an e-mail obtained from a third party establishing that the defendants, while employed by plaintiff, had used personal e-mail to communicate with plaintiff's customers.

The *Ameriwood* court noted that "[p]laintiff asserts and defendants do not dispute that the e-mail was produced by [the customer] after defendants failed to produce this e-mail in response to discovery requests" and therefore reasoned "that other deleted or active versions of e-mails may yet exist on defendants' computers."

Balancing the defendants' privacy interests against the central role of computers in the suit, the court directed discovery subject to a protective order safeguarding the defendants' privacy concerns: Rather than providing "wholesale" access to the computers to the plaintiff, the court instead directed defendants to provide their computers to an independent expert selected by plaintiff for imaging and recovery of data.

Once the independent expert recovered all of the electronic information from the computers, including deleted files and metadata, the defendants were allowed to review the information and required to produce only the non-privileged and responsive data.[10]

## Failure to Preserve

Failure to preserve and produce potentially relevant e-mails, even if located in a party's personal e-mail account, may result in harsher ramifications than required production of the party's hard drive.

In *Easton Sports, Inc. v. Warrior LaCrosse, Inc.*, the court sanctioned Warrior for its employee's destruction of his personal e-mail account.[11]

Plaintiff Easton brought suit alleging misappropriation of Easton documents by a former employee, Ghassemi. Defendant Warrior had contacted Ghassemi while he was employed by Easton about his potential employment by Warrior. Over the next several months, the employee forwarded several of Easton's business files from his office e-mail account to his personal Yahoo account. After leaving Easton's employ and joining Warrior, Ghassemi downloaded the files to Warrior's computers.

A month after Ghassemi left Easton, the company notified Warrior that it believed Ghassemi had stolen trade secrets. Warrior responded that it would investigate the matter, and soon thereafter amended Ghassemi's offer of employment to direct him not to bring anything from Easton to Warrior. In response to Warrior's investigation, Ghassemi also denied taking any Easton confidential information and executed affidavits to that effect.

Shortly thereafter, Easton served its complaint alleging Ghassemi's misappropriation of Easton documents and the use of Ghassemi's

personal e-mail account to communicate with Warrior. The day after the suit was filed, Ghassemi "canceled his Yahoo account, which resulted in the destruction of Yahoo records concerning his computer use."

During discovery, which included forensic examination of Warrior and Ghassemi's computer hard drives, Warrior "produced documents revealing that two additional Easton file names traceable to Ghassemi's Yahoo account were found on his Warrior hard drive."

The court found that Ghassemi inappropriately accessed Easton's confidential electronic documents, transferred a portion of those files to his personal Yahoo e-mail account, and then later "corruptly terminated his Yahoo computer service contract with the intent to bring about the destruction of any information or data compiled or stored through that service."

Warrior maintained that it did not solicit Ghassemi's wrongful conduct and that it should not be subjected to sanctions. The court found, however, that Warrior "was aware of Ghassemi's abuse of Easton's confidential records, and not the least bit interested in ensuring their preservation on Ghassemi's or Warrior's computer systems."

On Easton's motion for sanctions, the court found that Warrior's efforts "in acting to preserve relevant and discoverable information [were] sufficient to warrant a finding of at least negligence, and to justify the imposition of a sanction." Nonetheless, the court found that Easton had not met its burden to establish a breach of Warrior's discovery obligations severe enough to warrant the striking of their defenses and the imposition of a default judgment. Instead, the magistrate judge recommended that the district court allow Easton to present evidence of Warrior's failure to preserve the electronic data, to issue an instruction to the jury that it may presume that the evidence would have been favorable to Easton, to permit Easton to argue in favor of the negative inference, and to award attorneys' fees and costs.

## Personal Versus Business Use

A recipient of a subpoena or document request has an obligation to locate and produce all responsive documents within its "possession, custody or control." Fed. R. Civ. P. 26(b), 34(a).

*Quinby*, *Ameriwood* and *Easton* all indicate that businesses may need to consider whether such relevant, discoverable information exists on their employees' home computers and personal e-mail accounts, and develop discovery plans tailored to seek and preserve responsive information stored at those locations.

In the absence of such steps, *Easton* indicates that companies may be vulnerable to spoliation charges should their employees delete e-mails, close personal e-mail accounts or erase private hard drives.

This may well come as a surprise to many corporate employees. Employees may opt to use personal e-mail accounts for business purposes as a matter of convenience (e.g., to deal with an issue from vacation or avoid the sometimes time-consuming steps required to log into their work e-mail remotely). But the reality is that doing so may expose the employee's personal e-mail account and home computer to discovery in litigation.

And although *Quinby* tells us that the courts will hesitate before forcing individuals to share the entirety of their personal hard drives and e-mail accounts with legal adversaries, few if any, individuals want their personal e-mail accounts and home computers reviewed by their employers, or their employers' attorneys or "independent" experts as under *Ameriwood*.

In light of this blurring of the lines between business and personal electronic information, employers may well wish to consider steps to educate their personnel on the risks of mixing business and personal e-mail use.

For example, companies should consider educating their employees through employee handbooks, notices, meetings, and regularly scheduled reminders that using home computers and personal e-mail accounts for business may well require those computers and e-mails to be reviewed for responsive information if there is litigation. And employers may wish to discourage their employees from using private e-mail accounts to conduct business.

Because education may not be 100 percent effective in the event of litigation, employers should take appropriate steps to preserve, gather and provide responsive information to counsel regardless of location. Issue litigation holds to employees as soon as litigation is anticipated, and explicitly advise employees that such holds extend to business electronic information stored in their personal e-mail accounts or home computers.

1. "New Survey Reveals One-Third of Employees Use Personal E-mail Once or Twice a Week for Business Purposes; Nearly 60% Use Personal E-mail at Work When E-mail Is Down," AP Alert - Bus. (Market Wire), April 16, 2007.
2. Id.
3. Fed. R. Civ. P. 34 advisory committee note on 2006 amendments.
4. Id.
5. No. 04 Civ. 7406 WHP HBP, 2006 WL 59521 (S.D.N.Y. Jan. 11, 2006).
6. See also *Etzion v. Etzion*, 7 Misc.3d 940, 944, 796 N.Y.S.2d 844, 846-47 (N.Y. Sup. 2005) (holding that "[p]ersonal e-mails between [d]efendant and third parties, unrelated to any business matter, are also not discoverable").
7. See *Calyon v. Mizuho Securities USA*, No. 07CIV02241RODF, 2007 WL 1468889, at *5 (S.D.N.Y. May 18, 2007) (denying wholesale access to defendants' personal computers containing non-relevant "personal information related to taxes, personal finances and investments, family members' social security numbers, and data related to the business or charity activities of their spouses" where there was no evidence of "failure by the defendants to conduct a thorough forensic search of their computers, or to produce any and all relevant documents, files, metadata, and even hidden data fragments" requested); *Hedenburg v. Aramark Am. Food Servs.*, No. C06-5267 RBL, 2007 WL 162716, at *2 (W.D. Wash. Jan. 17, 2007) (denying discovery of hard drives to review e-mails and internet postings, where "the central claims in the case are wholly unrelated to the contents of plaintiff's computer" and plaintiff represented "that she has made a diligent search for her computer files" containing relevant information); *Balfour Beatty Rail, Inc. v. Vaccarello*, No. 3:06-cv-551-J-20MCR, 2007 WL 169628, at *3 (M.D. Fl. Jan. 18, 2007) (denying discovery of the defendants' hard drives where the plaintiff "does not provide any information regarding what it seeks to discover from the hard drives nor does it make any contention that [d]efendants have failed to provide requested information contained on these hard drives").
8. No. 4:06CV524-DJS, 2006 WL 3825291 (E.D.Mo. Dec. 27, 2006).
9. "A mirror image is an exact duplicate of the entire hard drive, and includes all the scattered clusters of the active and deleted files and the slack and free space." Id. at *1, n. 3.
10. See also *Corporate Healthcare Financing, Inc v. Breedlove*, No. 13-C-06-65007, 2006 WL 2400073 (Md.Cir. Ct. Apr. 19, 2006) (granting limited discovery concerning five e-mails sent from defendant's business e-mail account to his personal e-mail account); *Ball v. Versar, Inc.*, No. IP 01-0531-C H/K, 2005 WL 4881102 (S.D.Ind. Sep. 23, 2005) (granting access to plaintiff's work and home computers, and directing the production of e-mails received or drafted by plaintiff, where plaintiff had not preserved discoverable e-mails). But see *Heartland Surgical Spec. Hosp., LLC, v. Mid-West Div., Inc.*, No. 05-2164-MLB-DWB, 2007 U.S. Dist. LEXIS 53217, at *44-47 (D.Kan. July 20, 2007) (balancing the burden of non-parties searching their non-business e-mail accounts "against the likelihood that such searches would recover few, if any, additional documents not already produced" and denying motion to compel).
11. No. 05-72031, 2006 WL 2811261 (E.D.Mich. Sep. 28, 2006).