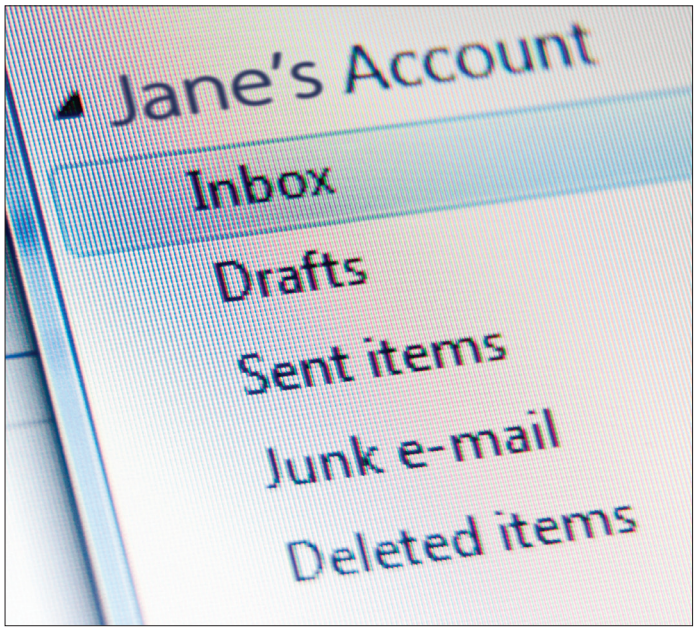
New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
Litigation
An ALM Publication
WWW.NYLJ.COM
MONDAY, SEPTEMBER 9, 2013

Personal Email at Work: What Expectation of Privacy?

BY ROBERT J. JOSSEN AND NEIL A. STEINER

Millions of Americans daily use their work email accounts, computer networks and smartphones to send and receive personal messages. Most do so without seriously considering whether their employers permit or prohibit such non-business and unofficial use of their work accounts, or whether their employers could or do monitor and review such messages and the implications of such a right to monitor. Indeed, given the hours spent at work and the ubiquitous nature of electronic messages as a mode of communication, it would be virtually impossible for many employees not to use their work accounts for personal messages.

In recognition of this reality, many employers now expressly permit limited incidental personal use of employer-provided email accounts and computer hardware (while specifically prohibiting illegal or offensive communications, such as transmitting pornography, engaging in sexual harassment, forwarding junk emails, and installing pirated, copyrighted or unauthorized materials). Most policies also provide that the employer may review messages transmitted through or stored on work accounts and systems, regardless of whether the employer in fact conducts such a review.



A recent decision from the U.S. District Court for the Eastern District of New York, *United States v. Finazzo*,[1] highlights the personal risk that an employee's use of a work email account to send or receive otherwise privileged and confidential communications—for example, with a spouse, personal lawyer, or doctor—will be deemed a waiver of the applicable privilege. *Finazzo* reflects the recent trend of courts finding that the employee has no reasonable expectation of privacy in these circumstances, thereby vitiating any privilege.[2]

This article examines the practical implication of the *Finazzo* decision, from the perspective of both the employee and the employer. We begin by analyzing *Finazzo*, then discuss what an employee should consider in deciding whether to use work email for personal communications, and conclude by addressing the pros and cons of different personal use and privacy policies employers could implement.

Finazzo involved a criminal prosecution, and ultimate conviction, of a former executive of clothing retailer Aéropostale. Christopher Finazzo was charged with participating in a kickback scheme in which he received a portion of the profits on Aéropostale's purchases from South Bay Apparel. The kickback scheme allegedly defrauded Aéropostale by depriving it of the ability to make informed and sound purchasing decisions, and by caus-

ROBERT J. JOSSEN *and* NEIL A. STEINER *are litigation partners at Dechert in New York, where they practice in the white collar and securities litigation group.*

ing it to overpay for goods purchased from South Bay.[3]

The scheme was uncovered during an unrelated internal investigation. The investigating firm discovered an email to Finazzo from his personal trusts and estates attorney that had attached a list of Finazzo's assets for purposes of preparing a will. The schedule of assets showed that Finazzo was a co-owner of South Bay with Douglas Dey, and also co-owned several other companies with Dey, none of which had been disclosed to Aéropostale.[4] Finazzo claimed that (i) he never consented to or encouraged his attorney to send privileged emails to his work account, (ii) he did not know the lawyer was going to send the email to his work account, (iii) he immediately forwarded it to his personal account and deleted it from his work account, and (iv) he instructed his lawyer not to send emails to his work account again.[5] Finazzo therefore argued that the email was privileged and should not have been produced to the government by Aéropostale. He thus sought to have it excluded from evidence in his criminal trial.

The district court rejected Finazzo's motion in limine to exclude the email. The court first noted that Finazzo had the burden of proving that the email was privileged, including showing that it was made and maintained in confidence. In deciding the motion, the court applied a four-factor test first developed in *In re Asia Global Crossing*.[6] Under this approach, the court evaluates: (1) whether the employer's policies permit or prohibit personal use; (2) whether the company monitors use of the employee's email; (3) whether third parties have a right of access; and (4) whether the company advised the employee or whether the employee was aware of the use and monitoring policies. As a result of this analysis, the court held that Finazzo had waived the attorney-client privilege over the email his lawyer sent to his work account.

Specifically, although there was some dispute whether the policy in effect in 2006 when the email was sent prohibited all personal communications (the 2004 policy) or permitted limited personal use of the work email account (the 2007 policy), both policies warned employees that they "should have no expectation of privacy when using Company Systems."[7] Moreover, between 2002 and 2006 Finazzo repeatedly had affirmed that he had read and was familiar with the company's Employee Handbook, which contained the policy on use of company technology systems. Even though there was no evidence that Aéropostale actually monitored employee emails, the court concluded that Finazzo's acknowledgement of the policies that permitted Aéropostale to review such emails defeated any claim that he had a reasonable expectation of privacy in emails sent from or received in his work email account.

'Finazzo' highlights the **personal risk** that an employee's use of a work email account to send or receive otherwise privileged and confidential communications—for example, with a spouse, personal lawyer, or doctor—will be deemed a **waiver of the applicable privilege**.

Finazzo highlights the precarious choice an employee confronts when deciding between the convenience of using work email account for privileged personal emails and the more cumbersome process of using a personal account or communicating in another fashion, such as by telephone or an in-person meeting. In today's world, there is often an expectation—indeed, almost a societal mandate—that messages must be read and responded to promptly. To have to log in to a personal email account to check for messages may be viewed as a hassle, and will certainly add delay to opening the email and the response time. For many messages that arguably could be privileged, such as routine emails with a spouse about the day, schedules, child coverage and the like, there generally is no concern with using a work account. But for other messages—about unhappiness at work, considerations of job changes, or confidential medical or financial information, as but a few examples—more care needs to be taken.

Unless company policy clearly provides that personal emails from a work account will be maintained in confidence and not monitored or reviewed by company personnel or third parties, an employee must seriously consider the very real risk that privilege will be waived before communicating with a personal lawyer from a work email account—whether about revising a will, matrimonial issues, civil litigation or potential regulatory or criminal investigations. Except for the most innocuous of scheduling emails, the convenience of using a work email account typically will not justify the risk of a privilege waiver. Thus, the best practice for the most sensitive of confidential, privileged discussions often remains a telephone conversation or face-to-face meeting. Indeed, while any privilege waiver should be limited to the actual emails sent or received in the work account, it is possible that frequent use of a work account could lead to claims of a subject matter waiver for all communications with counsel on a particular topic. *Finazzo* also cautions that one must exercise care in giving a work email address to lawyers or other with whom the employee may communicate in confidence on non-business related matters, unless clear instructions are given as to what emails may be sent to the work account.

For the employee's lawyer, sending emails to a client at a work email address may be particularly troubling. Underlying the *Finazzo* decision was the determination that the lawyer's unsolicited sending of a single email to the client at the work address amounted to a waiver of the privilege. *Finazzo* underscores the caution that communications with an employee-client through work email are fraught with risks. A lawyer should explain to the client that work email is not an effective means of communication with counsel and that at most a message "to call" or "I need to discuss an issue" should be the limits of these communications.[8] Moreover, unless the client

has consented to such communications, if an email to the work account results in a privilege waiver, the lawyer may well have exposure under the applicable professional conduct rules.[9] And if the waiver injures the client's case, the lawyer could potentially face a malpractice claim.

For the employer, it may seem obvious to adopt a computer use policy that permits limited personal usage of company accounts, warns employees that emails to or from a work account can be reviewed at any time and therefore the employee should not have an expectation of privacy with respect to any such emails. Anecdotally, this appears to be the most common type of policy currently in force. But it is not that easy.

With the extensive use of email for quick personal communications during the course of the workday, if the employer's policy expressly provides that personal emails on a work account are not confidential, it may hurt morale among employees who believe that their employer should respect their privacy. In addition, some employees may instead shift to using personal email accounts for such messages. That will require constant checking of personal email accounts from work computers—or if such access is not permitted, from personal smartphones—which can be a time-consuming, productivity-reducing distraction.

Likewise, if company policy makes it likely that personal emails using an employee's work email account are not privileged, the company may find itself the recipient of nonparty subpoenas in various litigations involving the personal affairs of its employees, in the hope that litigants will discover otherwise privileged emails that lose their protection because they are on the company's servers.[10] That may prove expensive and annoying to the company, as well as further affect the morale of employees who believe this an unfair invasion of their privacy. Moreover, in some circumstances—such as an employee consulting with personal counsel about whether a particular company practice is legal—it may be in the company's interest for the employee to be able to assert privilege over the document. In fact the company and the employee may have a common interest with respect to the subject matter that could be harmed in the event the employee was deemed to have waived the privilege over the email. Whether a common interest privilege could protect such a communication remains an interesting question not reached by the *Finazzo* decision.

On the other hand, a company policy that provided employees with a reasonable assurance that personal emails with spouses, lawyers and doctors would remain privileged has problems of its own. First and foremost, if a company undertakes not to monitor or review such emails, it must follow through on such a commitment. A company with such a policy could face claims from its employees if privileged emails are reviewed, inadvertently or otherwise, by network administrators or supervisory personnel. Many employers may be reluctant voluntarily to undertake new and potentially burdensome obligations. As a practical matter, it may not be possible for some employers to implement a system in which personal emails are segregated and not subject to monitoring or review by information technology personnel in the course of system upgrades, routine maintenance and troubleshooting. And employers in some industries may face regulatory prohibitions against, or at a minimum serious questions from regulators about, disclaiming responsibility for monitoring or reviewing certain categories of email communications.

Regardless of the precise policy a company chooses to adopt and implement, it is critically important for the employer to comply with its policy and to communicate clearly and accurately with its employees about the policy. Thus, if the employer adopts a policy that it will not review or access personal emails or a limited subset of personal emails (for example, by permitting employees a secure workspace within their work accounts where privileged personal emails may be stored), it must strictly adhere to that policy. Similarly, if company policy provides that the company in fact monitors and reviews emails, the company should actually do so, lest it potentially find itself liable for failing to uncover improper or criminal activity that it had no duty to discover but for its undertaking to review emails. And, if a company follows the popular current practice of reserving the right to review emails even though it typically does not undertake such a review,[11] it needs to make clear to its employees that they should not have an expectation of privacy if they use their work accounts for personal emails, that such emails therefore may well not be privileged, and that any personal use of the email system is at the employee's own risk.

1. No. 10-CR-457 (RRM) (RML), 2013 WL 619572 (E.D.N.Y. Feb. 19, 2013).

2. See, e.g., *United States v. Hamilton*, 701 F.3d 404 (4th Cir. 2012); *In re Reserve Fund Sec. & Deriv. Litig.*, 275 F.R.D. 154 (S.D.N.Y. 2011). Previously, courts tended to uphold the attorney-client and marital privileges against waiver challenges unless the evidence was clear that the employer repeatedly advised employees that their work computers and email accounts were subject to search by the employer or third parties at any time, such as by a flashing message on the login screen. See, e.g., *United States v. Hatfield*, No. 06-CR-0550 (JS), 2009 WL 3806300 (E.D.N.Y. Nov. 13, 2009) (holding that company chairman and chief executive officer did not waive privilege by using work email for communications with personal counsel, even though policy adopted under his watch gave company the right to monitor work email accounts); *United States v. Etkin*, No. 07-CR-913 (RMK), 2008 WL 482281 (S.D.N.Y. Feb. 20, 2008) (finding waiver of marital privilege where login screen prominently warned that users "have no legitimate expectation of privacy" during any use of New York State Police computer system because any usage could be monitored, recorded or accessed at any time); *In re Asia Global Crossing*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005) (developing four-pronged test for evaluating privilege waiver by personal use of work email, and concluding that no waiver occurred where evidence was inconclusive whether employee was aware of company policy concerning monitoring of emails).

3. *Finazzo*, 2013 WL 619572, at *1.

4. Id.

5. Id. at *10-*11.

6. 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005).

7. *Finazzo*, 2013 WL 619572, at *4-*5.

8. There is obviously a difference when the lawyer represents the entity itself and is communicating with an employee in furtherance of the representation. In such circumstances, the email should be entitled to protection under the entity's attorney-client privilege. See *Upjohn v. United States*, 449 U.S. 383 (1981). The situation in *Finazzo*, of course, was a representation of an employee in his individual capacity. The implications of *Finazzo* are just as important for a lawyer representing the employee in his individual capacity on matters relating to work; these communications also may be denied protection on the rationale that there is no expectation of privacy.

9. See Rule 1.6, N.Y. Rules of Professional Conduct.

10. Judge Joanna Seybert expressed this public policy concern in *Hatfield*. See 2009 WL 3806300, at *10 n.15.

11. Although beyond the scope of this article, we note that such a policy may not pass muster in a regulated industry or with a public company. Compliance and other law enforcement considerations may necessitate that there be periodic review of emails to assure that improper activity is not taking place and is discouraged.

Reprinted with permission from the September 9, 2013 edition of the NEW YORK LAW JOURNAL © 2013 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-09-13-09