

Risky Business: E-Mail at Work For Personal Purposes

BY JEREMY R. FEINBERG

Email is a necessary evil in the office. Although it is essential in the workplace for everyday business transactions, and it certainly aids communications in the course of legal representation, e-mail can be Public Enemy Number One when it comes to confidentiality. Relatively minor embarrassments are routine like accidentally e-mailing your grocery list to your work colleagues. Things could be worse, of course as if, by simply clicking your mouse, you accidentally broadcast a very personal note to everyone in your address book. But it does not take much imagination to envision the truly nightmarish scenarios that careless e-mail use can create when more sensitive information is in play.

If you need some real life examples of how e-mail can cause a personal or professional disaster, consider the following, both of which have been featured prominently in news stories and on Internet blogs. These are examples of how ordinary people, sitting at their desks in offices somewhere in the United States, can send an e-mail carelessly and, inadvertently, and very quickly, become objects of discussion around the country.

In 2003, a student from an Ivy League law school who was a summer associate at a prominent New York City law firm prepared a message on his work e-mail, describing his typical day at the firm to a friend. He wrote about how little work he was doing, his two-hour lunches, and how his time in the office was spent socializing and typing personal e-mails. Ben McGrath, OO-5, *THE NEW YORKER* (June 30, 2003) available at http://www.newyorker.com/archive/2003/06/30/030630ta_talk_mcgrath (last visited December 4, 2007). Although the summer associate showed poor judgment to type this e-mail from his work e-mail account in the first place, who could have predicted that by clicking send, he would direct the e-mail not to his friend, but rather, to the many lawyers in the law firm's large underwriting department? *Id.* Yikes! One can only begin to imagine the humiliation, heightened, no doubt, by the aftermath. His firm tasked him with drafting another e-mail from his work account a detailed apology, which included an admission of the implicit reflection such behavior could have on the Firm. *Id.*

A more recent example illustrates a different culprit in misuse of work e-mail: forwarding a message around the office. In 2007, an assistant coach of an NFL team forwarded an e-mail attachment containing a pornographic video from his work e-mail. He had previously received that explicit attachment from a work colleague. When the assistant coach attempted to share (or accidentally shared) the attachment, however, it was sent far more widely to every general manager in the NFL, and even the NFL Commissioner. Ed Bouchett, *Coach Sent Porn E-mail: Steelers Say He Apologized*, *PITTSBURG POST GAZETTE* (May 24, 2007) available at <http://news.cincypost.com/apps/pbcs.dll/article?AID=/20070524/5PT0301/705240332/1035/spt> (last visited December 4, 2007). The coach was made to apologize to the entire NFL and was warned that sending inappropriate e-mails from work e-mail was against club and league policy. *Id.* We all know that in many work environments, the consequences could have been far worse.

Inadvertent transmission of e-mails that shouldn't have been written (or forwarded) from the office in the first place is a concern in itself. Many companies choose to minimize the risks of such behavior by establishing e-mail usage policies prohibiting inappropriate e-mail transmissions and reminding employees that e-mail usage is subject to monitoring and review. But applying these policies to employee e-mails involving sensitive and otherwise confidential communications between the employee and the employee's attorney can have interesting results.

Using E-mail to Communicate with Clients

Throughout the 1990s, as the use of e-mail became increasingly popular, various ethics opinions addressed the risks of using this type of communication with clients. The general consensus, especially by the late 1990s, was that e-mail was generally a safe way to communicate, provided it did not violate the requirements of the Code of Professional Responsibility relating to client confidences. ABCNY Eth. Op. 2000-1; 1998-2.

In Opinion 1998-2, the New York City Bar Association's Committee on Professional and Judicial Ethics advised that a law firm is not required to encrypt all e-mail messages sent between the firm and its clients which contain confidential information. ABCNY Eth. Op. 1998-2. The opinion further noted, however, that attorneys should exercise different levels of Internet security based on the sensitivity of the information being exchanged and advise clients that e-mail may not be as secure as other forms of communication. *Id.*

The New York State Bar Association's Committee on Professional Ethics, in Opinion 709, went a step further, placing an affirmative obligation on the lawyer to preserve client confidences and secrets by ensuring that the use of e-mail is reasonable under the particular circumstances. NYSBA Op. 709 (1998). The opinion noted that [w]hether the use of e-mail is consistent with the duty [to protect client confidences'] depends on the likelihood of interception, *Id.* at 3, and that a lawyer who uses e-mail to communicate with clients must stay abreast of evolving technology and assess any changes in the likelihood of interception. *Id.* at 5. Thus, if a lawyer is put on notice that an e-mail is at a heightened risk of interception, or if the information being exchanged is highly sensitive, the lawyer should advise the client to use a more secure means of communication. *Id.*

These ethics opinions foreshadow, perhaps, an emerging line of cases from both state and federal courts. These cases address whether an employee's use of the employer's e-mail system to communicate with his own lawyer eviscerates attorney-client privilege and/or work product protection. The decisions, detailed below, make clear that waiver of privilege is a very real possibility enough so that in light of the ethics opinions described above, attorneys may wish to suggest alternate means of communication to their clients in order to keep privilege intact.

Asia Global Crossing

In *In re Asia Global Crossing, Ltd.*, the United States Bankruptcy Court for the Southern District of New York examined whether former officers of a company who had used the company's e-mail to communicate with their private lawyers, had waived applicable privileges and protections covering those communications. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (S.D.N.Y. Banker. 2005) (Bernstein, C.J.) (Asia

Global). In that Chapter 7 bankruptcy proceeding, the Bankruptcy Trustee moved to compel production of e-mails between the former officers of the company and their private attorney that had been left behind on the company's computer system when the former officers left the Company. *Id.* at 253, 255. Citing both attorney-client privilege and work-product protection, the employees refused to turn over e-mails. *Id.* at 253.

The court began its analysis of the motion by stating that use of the e-mail by itself, without more, did not cause a waiver, and that the prevailing view is that lawyers and their clients generally have a reasonable expectation of confidentiality and privacy in e-mail communications. *Id.* at 256. The court even noted that in New York, CPLR 4548 explicitly provides protection to e-mail communications by stating that a privileged communication does not lose its privileged character for the sole reason that it was sent by e-mail or because persons necessary for the delivery or facilitation of the e-mail may have access to its content. *Id.* at 256, citing CPLR 4548.

The court acknowledged a lack of specific case law on the questions before it, and looked for guidance to the case-specific analysis of right to privacy law. *Id.* The court analogized an employee's expectation of privacy in e-mails sent from the work computer and e-mail system, to an employee's expectation of privacy in his office, desk and files, which may be reduced by virtue of office practices, procedures, and regulation. *Id.* at 257, citing *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987).

Relying on right to privacy cases, the Court established a four-factor test to determine whether employees had a reasonable expectation of privacy in their e-mails so as to avoid waiver: (1) whether the company has a policy banning personal or objectionable use, (2) whether the company monitors employees use of computers or e-mail, (3) whether third-parties at the company have the right to access the e-mail, and (4) whether the corporation notifies employees of their monitoring policies. *Id.* at 257.

Applying these factors, the Court ultimately held that under the particular facts at hand, it could not determine as a matter of law that the use of the company's e-mail system had waived attorney-client or work-product privilege as to the e-mails in question. The court noted that there was evidence that the company had access to the e-mails, and that a corporate e-mail policy existed. But there was also conflicting evidence as to whether the former officers knew of the relevant policies, or if the policies applied only to other parts of the corporate family. *Id.* at 258-261. (The court went on to analyze two other sets of documents, one in hard copy form, others in e-mail form, and resolved issues regarding waiver as to the other documents on different grounds that are not relevant here.)

Scott v. Beth Israel Medical Center

More recently, the Commercial Division of the New York State Supreme Court had occasion to examine similar issues in *Scott v. Beth Israel Medical Center*, 2007 NY Slip Op 27429 (Sup. Ct. N.Y. County October 15, 2007) (Ramos, J.). There, plaintiff employee, a doctor, sought a protective order requiring his employer, a hospital, to return all e-mail correspondence sent between the employee and his attorney from the hospital's e-mail system regarding the employee's plan to sue his employer. *Id.* at 1. The court detailed the hospital's e-mail usage policy, which, as the hospital asserted, was either evidence that the e-mails were never privileged, or a basis to find a waiver of privilege and work product protection. *Id.* at 2-3.

As an initial matter, the court rejected the doctor's argument that CPLR 4548 mandated a holding that the e-mails were privileged. The court reasoned that even if CPLR 4548 ensured that communications should not lose their privileged character solely because they were sent over e-mail, that did not mean that the communications could not lose their privileged status for other reasons, including an employer's e-mail policy. *Id.* at 4.

Turning to the e-mail policy itself, the court noted that both parties had relied heavily on *Asia Global* and recognized the lack of existing New York State authority on point to determine whether the e-mail communications should be disclosed under the circumstances. *Id.* at 4. Accordingly, the court applied the four-factor *Asia Global* test and concluded that because the hospital's e-mail policy prohibited personal use and allowed for employer monitoring, and because the doctor was on notice of these two policies, the doctor's e-mails sent over the hospital's system were never privileged. *Id.* at 4-6.

The court also rejected the doctor's alternative argument that work product protection covered the e-mails. The doctor had asserted that his lawyer's e-mails all contained a notice at the end indicating to any unintended recipient that the contents might be confidential and that unintended recipients should notify the sender if they received the e-mails inadvertently. The court concluded that these standard e-mail notices cannot create a right to confidentiality out of whole cloth, and were not a reasonable precaution to protect [the lawyer's] clients. *Id.* at 6. (Readers of this article should closely read the *Scott* decision to determine its impact, in light of the ethics committee decisions cited above, on how to advise their clients about use of employer e-mail accounts to communicate with their attorneys.)

Variations On A Theme

Asia Global and *Scott* considered similar fact patterns: employees seeking to protect e-mail communications ostensibly sent over the employer's e-mail system through which the employees sought legal advice about matters on which employer and employee were adverse. There are questions, however, not presented by the two fact patterns that take the *Asia Global* and *Scott* scenarios to the next level. What would have happened if either of the parties seeking to uphold the privilege had, instead of using the office's e-mail system, used the Internet at the office to log into their own password-protected personal e-mail accounts on a service such as "gmail" or "hotmail"? Would the situation change if the employer were not adverse to, but either neutral to, or aligned with, the employee? Could a third party suing (or being sued by) the employee in litigation unrelated to the employer seek to pierce the privilege because the e-mails were subject to the employer's e-mail policy? Would the result have been any different?

Obviously there are practical implications here, too. Will subpoenas routinely be sent to employers seeking the production of e-mails that employees might have sent to their personal lawyers relating to litigations that have nothing to do with the employer, on the off-chance that the employee created responsive e-mails on work accounts or over the Internet using work computers? I don't have answers to these questions - and there is currently little or no specific guidance from the courts and ethics committees. But until the courts are presented with an opportunity to speak directly on these issues, there are a few clues available to suggest what might follow.

Private E-mail Accounts

At least one court, without citing or applying the Asia Global factors, has interpreted an employer's broadly-worded e-mail and Internet usage policy to hold that neither attorney-client privilege nor work product protection could shield e-mails from employees to their attorneys, even those created from a private account accessed via the Internet from work. In *Long v. Marubeni America Corp.*, 2006 U.S. Dist. LEXIS 76594 (S.D.N.Y. Oct. 19, 2006) (Fox, M.J.), employees claimed privilege as to e-mails sent from private and password protected e-mail accounts on their work computers, to their attorneys, concerning litigation that they wished to pursue against their employer. These e-mails, unbeknownst to the employees, were stored on the employer's computers in temporary Internet files, in a separate folder that was accessible only to authorized employees of the company. *Id.* at 3.

The employee handbook which one of these employees even helped to prepare, explicitly stated that all communications and information transmitted by, received from, created or stored in [the work computers I automated systems... are company records and company property, and that the company had the right to monitor its automated systems. The employee handbook further stated that employees have no right of personal privacy in any matter stored in, created, received, or sent over the...word processing and / or internet systems provided by the company. *Id.* at 2.

In the process of assembling documents for disclosure to the plaintiffs, defendant company discovered several e-mails stored in these folders which, although responsive, appeared to implicate the attorney-client privilege. The court directed defendants to allow plaintiffs to view these files and prepare a privilege log to serve on defendants. Plaintiffs motion seeking to preserve the privilege and work product protection soon followed. *Id.* at 4-5.

After concluding that fifteen e-mails on the privilege log might otherwise have been privileged, the court held that in light of the language in the employee handbook, the confidentiality element did not exist, and the assertion of the attorney-client privilege to safeguard the communication from disclosure was improper. *Id.* at 8. The employees elected to use their work-assigned computers to prosecute their employers and to communicate with their attorney, and because the employees knew or should have known about the company computer use policy, attorney-client privilege did not apply. *Id.* For similar reasons, the court also concluded that the employees had waived any otherwise applicable work product protection. *Id.* at 10.

Marubeni addressed language from a specific e-mail and Internet usage policy. Again, based on the guidance of New York City Bar Opinion 1998-2 and New York State Bar Opinion 709, lawyers should consider whether the Marubeni court's reasoning would be persuasive in the context of a client's employer e-mail policy, when advising the client about whether using the client's own private e-mail address from the office would provide greater protection for the attorney-client communications than using the company's e-mail system.

When Employees and Employers Not Adverse To Each Other

The question whether use of an employer's e-mail system can destroy the privilege when the employer and employee are not adverse to each other also remains to be resolved. Well-established doctrines such as the joint-defense and common-interest privileges might well apply, under appropriate circumstances, if both employer and employee are sued in the same case, are cooperating, or coordinate their legal strategies. See, generally, *Bank Brussels Lambert v. Credit Lyonnais (Suisse) S.A.*, 160 F.R.D. 437, 447

(S.D.N.Y. 1995); *Aetna Cas. & Sur. Co. v. Certain Underwriters at Lloyds*, London, (Sup. Ct. N.Y. Cty. 1998). But suppose the employer and employee are neither adverse nor aligned: the employee has been injured in a car accident unrelated to work and hires a lawyer to help prosecute a lawsuit against the other driver. Would the privilege apply if employee and lawyer communicate via the employer's e-mail?

The employer wouldn't be trying to defeat the privilege (as in *Asia Global and Scott*), but it would have no express reason to preserve it either, as it would in a joint-defense situation. Even when, in the absence of a common-interest or joint-defense arrangement, an attorney-client communication is shared with a party who has every reason to want to maintain the privilege, courts have reached inconsistent conclusions. One state appellate court has held that a mother, injured in a car accident, could speak with her lawyer in the presence of her daughter (who was not a party to the lawsuit) without destroying the privilege. See, *Stroh v. General Motors*, 213 A.D.2d 267 (1st Dept. 1995). By contrast, in one of the many wrinkles in the prosecution of Martha Stewart, a federal court held that Ms. Stewart waived attorney-client privilege when she forwarded to her daughter an e-mail written to her attorney. *United States v. Martha Stewart*, 284 F Supp. 2d 461, 462 (S.D.N.Y. 2003)

In short, and especially in advance of any specific judicial decision addressing e-mails in this context, lawyers should again be careful how they advise their clients to use e-mail as a form of attorney-client communication even if the client is not suing (or being sued by) the client's employer.

Conclusion

Very little good, and as shown by this article, many bad results, can come from using work e-mail for personal reasons. At a minimum, we can all benefit from taking a deep breath, counting to five, and double-checking every e-mail we write before clicking send. But the use of e-mail for attorney-client communications creates significantly more concerns and issues. Lawyers, and their clients, should educate themselves on developing case law, and, consistent with the teachings of the bar association opinions cited above, ensure that they understand and advise their clients about the risks of using work e-mail (or Internet connections) to communicate about personal legal matters.

Jeremy R. Feinberg is the Statewide Special Counsel for Ethics for the New York Unified Court System. He would like to thank his colleagues Rebecca Adams and Laura Smith, for their insight and suggestions that immeasurably improved this article. The views expressed in this article are those of the author only and are not those of the Office of Court Administration or Unified Court System.