Employee Use of Company Computers – A Privilege Waiver Mine Field

by Michael F. Urbanski and Timothy E. Kirtner

No one thinks about it. Everyone does it — uses a work computer for personal purposes. Today, employees use work computers to communicate with lawyers, spouses, doctors, or even pastors. Many companies have written policies and on-screen warnings stating that users have no expectation of privacy. What is the legal status of personal information on such computers that would otherwise be subject to a privilege? How have courts addressed no-privacy policies in the context of the broader public policy that protects privileged communications?

Federal courts have addressed the issue of whether communications made on or through employer-owned computers are protected from discovery and use at trial

Federal Decisions

Federal courts have addressed the issue of whether communications made on or through employer-owned computers are protected from discovery and use at trial under the protections of the marital and attorney-client privileges and the work product doctrine.

In *United States v. Etkin*, No. 07-CR-913, 2008 WL 482281 (S.D.N.Y. Feb. 20, 2008), the court held that, in light of the employer's computer use policy, defendant could not claim the marital communications privilege. The defendant moved to preclude introduction at trial of an e-mail that was sent using his government-issued e-mail account, asserting the marital privilege. Each time defendant logged on his computer, however, the screen warned of computer monitoring and notified users that they had no legitimate expectation of privacy. The court was persuaded by the screen warning that any expectation of privacy was "entirely unreasonable" and therefore, the communication was not confidential. *Id.* at *5; *see also Sprenger v. Virginia Tech*, No. 7:07cv502, 2008 WL 2465236 (W.D. Va. June 17, 2008).

The public policy underlying the attorney-client privilege is to encourage "full and frank communication between attorneys and their clients." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). Courts analyzing the confidentiality of e-mails and documents sent from work computers have reached differing conclusions in applying the attorney-client privilege.

For example, in *Long v. Marubeni America Corporation*, No. 05Civ.639, 2006 WL 2998671 (S.D.N.Y Oct. 19, 2006), the court found that the company's electronic communications policy (ECP) rendered any use of the company's computers nonconfidential, and found the attorney-client privilege not to attach and the work product doctrine waived. Unbeknownst to employees, when they used password-protected e-mail accounts, the company's computers "had an automatic administrative function that stored temporary Internet files in a separate folder that was accessible only to authorized [company] employees. Retained within the folder were residual images of the plaintiffs' e-mail messages." 2006 WL 2998671 at *1. The court found such communications not to be confidential because of the breadth of the employer's ECP, which (1) prohibited personal use of company computers; (2) stated that employees had no right of personal privacy in any e-mail or word processing document; and (3) the company had the right to monitor all data on its computer system. *See also Kaufman v. Sunguard Invest. Sys.*, No. 05cv1236, 2006 WL 1307882 (D.N.J. May 10, 2006) (Employee waived attorney-client privilege by communicating with her counsel over employer's e-mail system).

A leading case that reached a contrary conclusion is *In Re Asia Global Crossing Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005). In *Asia Global*, the court laid out four factors to consider in measuring an employee's expectation of privacy in his computer use:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies.

Asia Global, 322 B.R. at 257. Because the employer did not have a formal policy regarding use of computers, the court held that the use of work e-mail to communicate with a personal attorney did not destroy the attorney-client privilege. *Id.* at 261.

Asia Global and *Etkin* both looked toward the Fourth Amendment reasonable expectation of privacy standard to determine the reasonableness of intent that the communication remain confidential. Recognizing that the "question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable," the court in *Asia Global* expressly equated the question to whether there was an objectively reasonable expectation of privacy. *Asia Global*, 322 B.R. at 258.

Many federal cases that involve computers and the Fourth Amendment reasonable expectation of privacy take place in the workplace. In *O'Connor v. Ortega*, 480 U.S. 709 (1987), the Supreme Court held that public employees did have Fourth Amendment rights in their offices, but that their reasonable expectations of privacy could be "reduced by virtue of actual office practices and procedures, or by legitimate regulation." *Id.* at 717. Because of the many different types of public work environments, the Court noted that questions of public employees' reasonable expectations of privacy should be addressed on a case-by-case basis. The Fourth Circuit has held that a public employee had no reasonable expectation of privacy in his Internet use in light of the employer's computer use policy. *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

In two cases similar to *Etkin* involving computers with flash-screen warnings and Fourth Amendment rights, courts held that defendants had no reasonable expectation of privacy in their work computers. *See United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002) (upholding a seizure of a state-owned computer because defendant had no reasonable expectation of privacy in light of flash-screen warning); *United States v. Bailey*, 272 F. Supp. 2d 822 (D. Neb. 2003) (holding that flash-screen warning obviated any defendant reasonable expectation of privacy). *See also Muick v. Glenayre Elecs.*, 280 F.3d 741 (7th Cir. 2002) (notice that laptops were subject to inspection of privacy).

The Second and Fifth Circuits, however, have held that employees had a reasonable expectation of privacy in office computers. *See United States v. Slanina*, 283 F.3d 670, 676 (5th Cir. 2002) (employer did not have a policy notifying employees that computers were monitored); *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001) (employer only had an anti-theft policy that prohibited use of computers for personal business, and computers were subjected to "infrequent and selective search[es] for maintenance purposes"). The Court of Appeals for the Armed Forces has also held that an employee had a reasonable expectation of privacy in her work computer even though there was a flash screen warning at log-in. *United States v. Long*, 64 M.J. 57, 64 (C.A.A.F. 2006). The court distinguished *Simons* on the basis that the policy in *Simons* was "very specific," restricted use to official business, and notified the user that the system was subject to inspection. *Id.* at 65. The log-on banner in *Long* did not contain a notification that users had no expectation of privacy in use of the system. *Id.* at 65. All these factors added up to a qualification of defendant's privacy expectation in her e-mails, but not an elimination of an objectively reasonable expectation of privacy. *Id.* at 64.

A more nuanced approach was taken by the court in *Curto v. Medical Communications Inc.*, No. 03CV6327, 2006 WL 1318387 (E.D.N.Y. May 15, 2006). There, the court found no waiver of privilege by an employee communicating with her counsel over a company laptop, even though the employer had a policy that prohibited the personal use of computers. The court considered the fact that the employee worked out of her home, communicated with her counsel through a personal AOL account, and attempted to delete the e-mails before returning her computer. Under these circumstances, the court found any disclosure to be inadvertent and not a waiver of privilege.

Likewise, in *Sims v. Lakeside School*, No. C06-1412RSM, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007), the court found an employee manual to be clear that an employee had no reasonable expectation of privacy in e-mails sent over the employer's e-mail accounts. However, the court found that Web-based e-mail communications with plaintiff's spouse or lawyer to be privileged, reasoning that the public policy in favor of confidential communications to trump the provisions

of the employee manual. This aspect of the analysis undertaken by the *Sims* court ought not be underestimated, as it is one of the few opinions that elevates the public policy in favor of preserving privileged communications over an employer's internal computer usage policy.

… it is one of the few opinions that elevates the public policy in favor of preserving privileged communications over an employer's internal computer usage policy.

Selected State Decisions

The Supreme Court of Virginia recently addressed waiver of the attorney-client privilege for information stored on a company computer in *Banks v. Mario Industries of Virginia Inc.*, 274 Va. 438, 650 S.E. 2d 687, 695-96 (2007). In *Banks*, Troy Cook, a manager of a sales division of Mario Industries, made plans to develop a competing business. Prior to Cook's resignation, Cook sought legal advice from his personal lawyer regarding his resignation. Cook prepared a memo for his attorney on a computer owned by Mario. This memo, in which Cook addressed issues concerning Mario, its industry, and his planned resignation and new business, became a key piece of evidence at Mario's civil suit for breach of fiduciary duty.

The Roanoke City Circuit Court admitted the memorandum into evidence over Cook's attorney-client privilege objection. Citing *Clagett v. Commonwealth*, 252 Va. 79, 92, 472 S.E.2d 263, 270 (1996), for the proposition that "the [attorney-client] privilege is waived where the communication takes place under circumstances such that persons outside the privilege can overhear what is said," the Supreme Court of Virginia held the trial court's finding of waiver to be without error. The Court founded its ruling on the fact that Mario's employee handbook provided that there was no expectation of privacy regarding Mario's computers and that Cook created the memorandum on a Mario-owned computer and printed it off before deleting it.

The *Banks* court found the memorandum not to be privileged, notwithstanding the fact that Cook made efforts to delete the memorandum from the Mario computer. The opinion does not reach the question of whether Cook's efforts to delete the memorandum could constitute circumstances under *Clagett* where the communication could not be "overheard." Nor does it reach whether the circumstances of being overheard are impacted by the fact that it took a forensic computer expert to resurrect the memorandum. Waiver is fact specific, and such argument may find resonance in future cases. On the *Banks* facts, therefore, one could argue that waiver of the privilege occurs at the moment the memorandum is typed on a company-owned computer, regardless of whether anyone other than the author saw it or had access to it before it was deleted. The danger, of course, is that waiver of the attorney-client privilege can be broad subject matter waiver. *See United States v. Jones*, 696 F.2d 1069, 1072-73 (4th Cir. 1982).

The issue of an employee's efforts to delete a document was addressed in another case in which an employee went to work in a competing role. In *National Economic Research Associates, Inc. v. Evans*, 21 Mass. Rptr. 337, 2006 WL 2440008 (Mass. Super. 2006), NERA sued David Evans, one of its former consultants, for breach of a non-solicitation agreement following his resignation and subsequent employment with a competitor.

While still employed at NERA, Evans communicated with his personal lawyer concerning his departure and start of work for his new employer. Many of these communications were conducted by e-mail, with Evans sending and receiving e-mails from his personal, password protected e-mail account with Yahoo rather than his NERA e-mail address. Evans frequently used the laptop issued to him by NERA to communicate with his lawyer via the Internet. As in *Long*, Evans's e-mails with his lawyer left a trail on his computer.

Before Evans left NERA, he deleted personal computer files and ran a defragmentation program, which he understood would prevent recovery of the deleted personal files. Evans did not, however, delete his e-mails from his Yahoo account as he had no idea that they were stored on his work laptop. After Evans left, NERA hired a computer forensic expert who was able to retrieve the communications between Evans and his lawyer.

NERA argued that the attorney-client privilege did not apply to these e-mails, and, even if it did, Evans waived the privilege. NERA contended that its policies made it clear that any e-mails sent over company computers could not be considered confidential. NERA's policy contained admoni-

tions that personal use of e-mails should be kept to a minimum; that computer resources are property of the company; that any information sent over such resources may be reviewed; and that e-mails are not confidential and may be routinely read by the company. As such, NERA argued that Evans's communications with his lawyer were not made in confidence.

The court agreed with NERA that the warnings in the employee manual rendered nonconfidential any e-mails sent via the company e-mail address and network.[1] The court disagreed, however, that a reasonable person would have known that the hard disk of a computer makes a screen shot of all it sees — including password protected Internet e-mail accounts — and stores it in a temporary file. The court found such communications to be privileged.

The court found further that Evans had not waived the privilege. He had taken adequate steps to protect the confidentiality of his communications with his lawyer by using his private password protected e-mail account, he did not store these e-mails on his work computer, and he attempted to delete all personal data off of his work laptop. The Massachusetts court practically rationalized its holding by concluding that:

> If NERA's position were to prevail, it would be extremely difficult for company employees who travel on business to engage in privileged e-mail conversations with their attorneys. If they used the company laptop to send or receive any e-mails, the e-mails would not be privileged because the "screen shot" temporary file could be accessed by the company. If they used the hotel computer to avoid this risk, the communication would still not be privileged because the hotel could access the temporary file on its computer. Pragmatically, a traveling employee could have privileged e-mail conversations with his attorney only by bringing two computers on the trip — the company's and his own.

2006 WL 2440008 at *5. At the end of the day, the specific holding in *NERA*, like the federal decisions of *Curto* and *Sims*, was fairly narrow and specific: the court in *NERA* concluded that there was no privilege waiver for an employee's attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password protected e-mail account over the Internet.

Conclusions and More Questions

How does one begin to rationalize such apparently divergent decisions? Certainly, one way to do so is to recognize that the facts of each case dictate the outcome. For example, use of a company e-mail account and server or word processing program to communicate with one's spouse or lawyer is fraught with danger, particularly where the employee is on notice of the employer's policy that such information is owned by the company and that he has no expectation of privacy, and particularly in the context of employee-versus-employer litigation. The case for waiver is even clearer where employers expressly prohibit personal use of work computer systems. On the other hand, using a personal, password-protected e-mail account that bypasses the employer's server or taking steps to delete a document created on an employer's computer system may give rise to the argument that there was no waiver of a privileged communication. In litigating issues of privilege waiver in this electronic age, parties and courts need to be mindful of the balance that must be struck between the public policy that protects certain confidential communications and the private rights of employers who own computer hardware and software over which employees conduct both the employers' and their own personal business.[2] ■

Endnotes:

1 To that extent, the *NERA* opinion also is consistent with a New York decision in *Scott v. Beth Israel Medical Center Inc.*, 17 Misc. 3d 934, 847 N.Y.S.2d 436 (2007). There the court found that plaintiff doctor, who had sued his former employer for breach of his employment contract, waived the attorney-client privilege as to e-mails sent to his counsel using his employee e-mail address and sent over the employing hospital's server. Applying the *Asia Global* test, the court found that the hospital's computer use policy stated that its computers were for business purposes only, the hospital's policy allowed it to access any information on its system and Scott had both actual and constructive notice of this policy. As such, the court found that Scott's e-mails were not confidential communications protected by the attorney-client privilege and that any work product protection was waived by Scott's use of the hospital e-mail system in the face of the hospital's computer policy.

2 Finally, it is worth noting that the civil cases discussed above concern disputes between employees and employers. Should the *Banks* decision and

Company Computers continued on page 57

Company Computers
continued from page 43

others like it apply outside of this context? Suppose, for example, that an employee drafts a memo to his divorce attorney on the company computer and then deletes it. Further, suppose that a lawyer for the employee's wife subpoenaed the employee's computer records from his employer. Setting aside for the moment questions about what steps the employer might or is obligated to take in response to the subpoena, has the employee waived the attorney-client privilege by typing the memo on the company computer? Following *Banks*, the answer would seem to be yes. Under the "reasonable expectation" of privacy standard employed by the federal courts, however, the opposite result may be reached.