New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication

TUESDAY, JULY 6, 2010

STATE E-DISCOVERY

Expectations of Privacy In E-Mail Communications

By **Mark A. Berman**

People continue to rely on their belief that the contents of e-mails, like phone calls, are sacrosanct and what is "said" in e-mail communication remains "confidential" to everyone other than the parties to them.

However, that expectation of privacy is breaking down by the day. E-mails should more properly be viewed as a "postcard" or a conversation over a speakerphone, both open and available to a passerby to hear or see, than like a private "confidential," "sealed" letter.[1]

Seeking to ensure that e-mails remain confidential, however, does not take much effort on the part of the sender or recipient. That, no doubt, is why courts are increasingly rejecting arguments seeking to prevent the disclosure and use of putatively confidential e-mails in court proceedings where the e-mail user has done little to maintain its alleged confidentiality.

The recent New York cases discussed below highlight some of the considerations courts are taking into account when deciding whether a party has a realistic expectation of privacy over its e-mail communications. Courts ask, for instance, does a sender leave his or her e-mail account "open" on a computer for others to see or access? Courts also look to whether the e-mail is sent or received via a corporate system or through a personal account; whether the computer used for such communication is owned by an employer or an individual; and whether, when the communication was transmitted, the computer at issue was located in a company's office or at a home?

Further, if an e-mail is sent through a corporate network, courts want to know the company's policy on personal e-mails and, if the policy permits the company to view personal e-mails, does it actuality do so?

As far as security goes, courts inquire whether the computer or e-mail account at issue is password protected or whether any other "security" system has been implemented and, if so, have specific precautions ever been taken when there has been a concern about the security of e-mails.

Courts further look to whether a password has been shared with others and whether the e-mail user is aware that others had access to

BIGSTOCK

view his or her e-mails by whatever means. Courts want to know whether permission has been granted to others (or revoked) to review one's e-mails, and whether it is in writing or oral, or was permission (or revocation) more implicit by, perhaps, manifesting itself through custom or practice.

In *Forward v. Foschi*,[2] defendant sought disqualification of plaintiff's counsel following plaintiff's admission that he intentionally accessed defendant's personal and business e-mail accounts, downloaded e-mails therefrom, and then forwarded e-mails between defendant and her lawyer to his own attorney. Plaintiff admitted that defendant had not authorized him to access her e-mail accounts. Plaintiff's counsel also failed to notify defense counsel or the court that he had been provided with such "privileged" e-mails.

In opposing the disqualification motion, plaintiff asserted that defendant knew he had access to her office and personal e-mail accounts (and failed to object to such access), where she had knowledge that he and other employees knew her password.

Plaintiff asserted that other employees were essentially "looking over [defendant's] shoulder" when she was communicating with her counsel and, accordingly, that defendant waived the attorney-client privilege.

Plaintiff also asserted that, as the system administrator with knowledge of plaintiff's password—a fact known to defendant—he had the right to access e-mail accounts, including defendant's. The court, however, rejected such argument based on CPLR §4548, which explicitly provides that "[n]o communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons *necessary* for the delivery or facilitation of such electronic communication may have access to the content of the communication."[3]

With respect to defendant's personal e-mail account, plaintiff asserted that he found defendant's "gmail" account left "open," which "often" occurred, on an office computer that was shared by others, and it was further asserted that defendant gave her password to employees so they could read her e-mails to her.[4]

As such, plaintiff contended that defendant had no expectation of privacy in such e-mails. The court stated that, in enacting CPLR §4548, the New York Legislature made a "finding that when the parties to a privileged relationship communicate by e-mail, they have a reasonable expectation of privacy," but then noted that, as held by Justice Charles E. Ramos in *Scott v. Beth Israel Med. Ct. Inc.*,[5] "[a]s with any other confidential communication, the holder of the privilege and his or her attorney must protect the privileged communication; otherwise it will be waived. For example, [in the case of] a spouse who sends her spouse a confidential e-mail from her workplace with a business associate looking over her shoulder as she types, the privilege does not attach."[6]

The court found that plaintiff's counsel failed to notify opposing counsel of receipt of such "privileged" e-mails, and that he further failed to seek an *in camera* review of the e-mails based on a good faith belief that the privilege had been waived.

Accordingly, the court held that the attorney had violated the "spirit and intent" of the relevant ethical canons.[7] Nevertheless, the court declined to disqualify counsel, in part, because defendant continued to allow plaintiff to access her

MARK A. BERMAN, *a partner at commercial litigation firm Ganfer & Shore, is secretary of the e-discovery committee of the Commercial and Federal Litigation Section of the New York State Bar Association.* ANNE D. TABACK, *a Ganfer & Shore associate, assisted in the preparation of this article.*

communications after a time when she knew that plaintiff was viewing them. The court noted that if defendant was truly concerned about the sanctity of her e-mail communications, she could have taken steps to prevent such access by opening a new account or changing her password.

Further undermining defendant's position is that, as noted by the court, once defendant learned plaintiff was accessing her e-mails, she created bogus e-mails in an attempt to mislead him. The court held that defendant's complicity with the situation militated against her claim of an invasion of privacy, and in favor of finding "consent."

The court found, however, that there had been no waiver of the privilege prior to the date defendant learned that plaintiff had been accessing her e-mail accounts. As a result, the court suppressed all such "privileged" e-mails and, as a sanction for plaintiff accessing defendant's e-mails "outside of the discovery process by engaging in self-help," non-privileged e-mails dated prior to when defendant learned that plaintiff has access to her e-mails were suppressed as well.

Divorce Case

In *Gurevich v. Gurevich*,[8] a matrimonial action, the court held that e-mails a wife "retrieved" from her husband's account were admissible. The wife knew her husband's password and he failed to change it until two years following their separation.

The court noted that, through counsel, plaintiff asserted that her husband never formally rescinded his permission for her to look at his e-mails.[9]

The court noted that CPLR §4506 provides that recorded communications or evidence derived therefrom, which have been obtained by conduct constituting the crime of eavesdropping, as defined by Penal Law §250.05, may not be received as evidence at trial. Penal Law §250.05 provides that, inter alia, a person is guilty of eavesdropping when he unlawfully "intercepts" or "accesses" an electronic communication.

The court, relying on the penal law definitions of "intercept" and "access," noted that this would require an "intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, without the consent of the sender or intended receiver thereof, by means of instrument, device, or equipment."[10]

The court in reviewing the relevant Legislative History noted that the purpose of the statute was to:

> prohibit individuals from intercepting communications going from one person to another, and in this case an email from one person to another. In the case at bar the email was not "in transit," but stored in the e-mail account. Even assuming the husband's facts, as sated, to be true, the wife may have unlawfully retrieved information from a computer; in violation of Penal Law 153.10, but there was no interception and accordingly fails to fall within [the] scope of CPLR 4506 as presently written.[11]

Finding that the e-mails were not "intercepted while in transit," but merely "retrieved" from a computer by a party who knew the password, the court held that the e-mails were admissible at trial, as long as they were not protected by the attorney-client privilege.[12]

Finally, the court noted that there is "no statute that would recognize an 'implied revocation upon service of a divorce action' and bar the use of the email 'stored.'"

Lack of Authorization

In *People v Klapper*,[13] the issue of privacy of e-mail communications is examined in the criminal context. In this case, an employer was charged with the unauthorized use of his own computer, pursuant to Penal Law §156.05, resulting from the employer's installation of keystroke-tracking software and his resultant viewing of an employee's e-mails.

The court dismissed the accusatory instrument finding the allegations insufficient to establish that defendant acted "without authorization." It court held that the accusatory instrument failed to state that defendant, the computer owner, had knowledge of any limited access to the computer or the complainant's e-mail account.

The court noted that there was no allegation that complainant "had installed a security device to prevent unauthorized access or use," and the allegations further demonstrated that defendant had sent e-mails to complainant containing documents from complainant's e-mail account, "support[ing] an inference that defendant did not have notice or at a minimum had a reasonable belief that his access was not prohibited or limited."

> It does not take much to protect confidential e-mails from being used by others in court, but precautions must be taken seriously or one risks having damaging messages used against him.

In addressing the lack of authorization, the court found:

> Whereas, some may view e-mails as tantamount to a postal letter which is afforded some level of privacy, this court finds, in general, e-mails are more akin to a postcard, as they are less secure and can easily be viewed by a passerby. Moreover, e-mails are easily intercepted, since the technology of receiving an e-mail message from the sender, requires travel through a network, firewall, and service provider before reaching its final destination, which may have its own network, service provider, and firewall. An employee who sends an email, be it personal or work related, from a work computer sends an e-mail that will travel through an employer's central computer, which is commonly stored on the employer's server even after it is received and read. Once stored on the server, an employer can easily scan or read all stored emails and data. The same holds true once the email reaches its destination, as it travels through the internet via an internet service provider. Accordingly, this process diminishes an individual's expectation of privacy in e-mail communications.[14]

In reaching its conclusion, the court relied on the legislative intent, which was to criminalize computer intrusions only where there existed "sufficiently set forth protections or policies to avoid unauthorized access" and noted the absence of allegations in the accusatory instrument that defendant "circumvented a security device or password or that complainant had installed any security protections to prevent the defendant's authorization or access to the computer or email account."[15]

1. *People v. Klapper*, __N.Y.S.2d__, 2010 WL 1704796, at *5 (Crim. Ct. N.Y. Co. April 28, 2010).
2. 27 Misc. 3d 1224(A), 2010 WL 1980838 (Sup. Ct. West. Co. May 18, 2010).
3. Id. (emphasis added); see N.Y. C.P.L.R. §4548 (McKinney 2010).
4. *Forward*, 2010 WL 1980838, at *12.
5. 17 Misc. 3d 934, 847 N.Y.S.2d 436 (Sup. Ct. N.Y. Co. 2007).
6. *Forward*, 2010 WL 1980838, at *12 (quoting Scott, 17 Misc. 3d at 938, 847 N.Y.S.2d at 440). See Mark A. Berman, "Changes in Laws on Electronically Stored Information, NYLJ, Feb. 14, 2008, discussing the *Scott* case. In Scott, defendant hospital had a policy that its computer and e-mail systems were the property of the hospital and could only be used for business purposes; all information or documents created, sent or saved on the hospital's computer were property of the hospital; and that no hospital employee had a personal privacy right in such materials.
7. *Forward*, 2010 WL 1980838, at *14 (citing *MNT Sales LLC v. Acme Television Holdings LLC*, NYLJ, April 20, 2010 at 42, col. 5 ("if there is a legal dispute before a tribunal and the receiving attorney believes in good faith that the communication appropriately may be retained and used, the receiving attorney may submit the communication for in camera consideration *by the tribunal as to its disposition*") (quoting Formal Opinion 2003-04 of the Committee on Professional and Judicial Ethics of the New York City Bar) (emphasis in original)).
8. 24 Misc. 3d 808, 886 N.Y.S.2d 558 (Sup. Ct. Kings Co. May 5, 2009).
9. Id., at 809, 886 N.Y.S.2d at 559.
10. Id., at 810-11, 886 N.Y.S.2d at 560. See Penal Law §§250.05, 250.00(6).
11. Id., at 813, 886 N.Y.S.2d at 561-62.
12. Id., 24 Misc. 2d at 813, 886 N.Y.S.2d at 562.
13. __N.Y.S.2d__, 2010 WL 1704796.
14. Id., at *5 (citing *Scott*, 17 Misc. 3d at 939, 847 N.Y.S.2d at 44, and noting there that the court held that "an employer's 'no personal use' e-mail policy, combined with the employer's stated policy allowing e-mail monitoring, diminished any reasonable expectation of privacy an employee may have regarding computer services").
15. *Klapper*, 2010 WL 1704796, at *5-*6.

Ganfer & Shore, LLP
360 Lexington Avenue
New York, New York 10017
212.922.9250
mberman@ganfershore.com