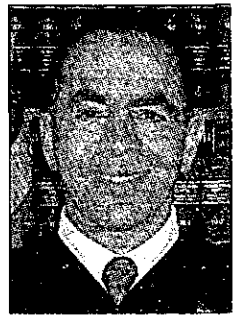
Electronic Communications and the Ethical Obligation to Preserve Confidentiality

In NY Eth. Op. 842, 2010 WL 3961389 (September 2010), the New York State Bar Association Committee on Professional Ethics observed that "[t]he obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must also take reasonable care to affirmatively protect a client's confidential information."



Kenneth L. Gartner

Opinion 842 continues, "[n]ot only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using ... electronic means of communication ... should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege."

In *Scott v. Beth Israel Medical Center, Inc.*, 17 Misc.2d 934 (Sup. Ct., N.Y. Co. 2007) (Ramos, J.), the plaintiff sued for the alleged breach of an agreement to pay the plaintiff $14 million in severance pay if his termination was "without cause." Defense counsel sent a letter to plaintiff's counsel providing notification that the defendant was in possession, on the defendant's servers, of e-mail correspondence between the plaintiff and plaintiff's counsel pertaining to the dispute. The letter stated that the defendant believed that any potential privilege attached to the communications had been waived by plaintiff's use of defendant's e-mail system.

In denying plaintiff's motion for a protective order, the court observed that the defendant had a policy, of which plaintiff was on notice, stating that "[e]mployees have no personal privacy right in any material created, received, saved or sent using [the defendant's] communication or computer systems. The [defendant] reserves the right to access and disclose such material at any time without prior notice."

Even though the defendant acknowledged that it had never in fact monitored the plaintiff's (or any other employee's) e-mails, the defendant retained the right to do so. The court found that "the effect of an employer e-mail policy, such as that of [the defendant], is to have the employer looking over your shoulder each time you send an e-mail. In other words, the otherwise privileged communication between [the plaintiff and his lawyers] would not have been made in confidence because of the [defendant's e-mail] policy."

In *Willis v. Willis*, 79 A.D.3d 1029 (2nd Dept. 2010), the Appellate Division affirmed an order compelling the

See CONFIDENTIALITY, Page 15

CONFIDENTIALITY ...

Continued From Page 3

plaintiff to produce emails she had sent to her lawyers. The Appellate Division observed that the plaintiff's children had access to the email account. Relying in part upon *Scott*, the Appellate Division held that "[u]nder these circumstances, it cannot be said that the plaintiff had 'a reasonable expectation of confidentiality' in the e-mail communications between herself and her attorneys, which communications were freely accessible by third parties." Compare, *Parnes v. Parnes*, 80 A.D.3d 948 (3d Dept. 2011) (husband leaving a note containing the user name and password of his personal email account where wife could find it did not constitute waiver of the privilege as to email communications with his attorney using that account).

In *People v. Klapper*, 28 Misc.3d 225 (Crim. Ct., N.Y. Co. 2010) (Whiten, J.), the court dismissed a criminal charge of Unauthorized Use of a Computer against an employer. The employer installed a keystroke recorder on the complainant employee's assigned workplace computer, and then used the information to access the employee's personal e-mail account. The court, citing *Scott*, held that the employee's use of the workplace computer had so compromised the employee's expectation of privacy as to make the pleading of "unauthorized" access to the private email account insufficient. "An employee who sends an email ... from a work computer sends an email 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 or 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."

Ironically, *Scott* itself viewed the employer's written email policy, which was not present in *Klapper*, as "critical to the outcome." It was critical because CPLR § 4548 provides that "no communication 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." *Scott* cited Vincent Alexander, Practice Commentaries, McKinney's Cons. Laws of N.Y., Book 7B, CPLR § 4548, for the proposition that without an employer policy such as was present in *Scott*, "when the parties to a privileged relationship communicate by e-mail, they have a reasonable expectation of privacy."

In fact, in *Stengart v. Loving Care Agency*, 201 N.J. 300 (2010), the Supreme Court of New Jersey distinguished *Scott*, and determined that an employee's use of a company laptop to access a personal, password-protected, web-based e-mail account possessed a sufficiently reasonable expectation of privacy as to preserve the otherwise privileged character of communications. *Cf., Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F.Supp.2d 548 (S.D.N.Y. 2008) (Koeltl, J.) (former employer obtained former employee's username and password for his Hotmail account when the information was left stored on the employer's computers, and then used this information to access, read, and print the former employee's e-mails. In precluding use of the e-mails, the court determined that the employer's e-mail policy "could not apply to e-mails on systems maintained by outside entities such as Microsoft or Google," *i.e.*, which were "located on, and accessed from, third-party communication service provider systems").

As recently summarized by the American Bar Association Standing Committee on Ethics and Professional Responsibility, in Formal Opinion 11-459 (August 4, 2011), "[a] lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client."

Kenneth L. Gartner is a member of Lynn, Gartner, Dunne & Covello, LLP. A former Nassau County District Court Judge, he is a Special Professor of Lawyers' Ethics at Hofstra Law School, and an Adjunct Professor at Touro Law School.